Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 9 | Issue 2 Article 3

January 1993

Proposal for Federal Legislation Protecting Informational Privacy across the Private Sector

Joshua D. Blackman

A PROPOSAL FOR FEDERAL LEGISLATION PROTECTING INFORMATIONAL PRIVACY ACROSS THE PRIVATE SECTOR

Joshua D. Blackman†

I. INTRODUCTION

Information technology is providing businesses with powerful new marketing tools. Before the computer revolution, direct marketers flooded mailboxes with junk mail for relatively few sales. Now software can pinpoint target groups by comparing mailing lists or by using "point-of-sale"[1] information to identify consumers likely to buy certain products.[2] Similarly, records kept in the computer memory of TRW, Trans Union Corporation and Equifax, Inc. gather the financial minutiae of most (more than 170 million) American adults.[3] From this financial data, mailing lists based on an infinite variety of criteria are created and sold. While consumers have legislative permission to obtain copies of their credit reports

---

† Director, Legal Research Group, Find SVP. New York City; attorney admitted in New York and Connecticut; author of The Legal Researcher's Internet Directory; email address joshb@panix.com.

1. The Chief Executive Officer of Citicorp's Point-of-Sale (POS) Information Services, Jerry Saltzgaber, described the features of a POS system:

> When they join, consumers receive a personalized card with either a mag stripe or a UPC bar code. Then by presenting these cards at the checkout counter consumers automatically get credit for all the store coupons in effect at that time and all purchases are recorded by household.
>
> . . . .
>
> [The database is used] for a wide variety of direct marketing applications, including delivering bar soap samples to competitive brand users, sending disposable diaper coupons and baby food coupons to households with infant children — *inferred from prior purchases* — and targeting the best prospects for magazine subscription acquisition programs.

Data Protection, Computers, and Changing Information Practices, Hearings on H.R. 685 Before the Subcommittee on Government Information, Justice, and Agriculture of the House Committee on Government Operations, 101st Cong., 2nd Sess. 86 (1990) [hereinafter *Hearing Record*] (emphasis supplied).

2. This practice is known in the direct mail industry as "profiling." *Swedes Worry That European Community Membership Will Compromise Databases*, COMPUTERGRAM INT'L, Jan. 10, 1991, *available in* LEXIS, NEXIS World Library, Txtline File.

3. Peter Kerr, *Big Credit Bureau to Let Consumers See Reports Free*, N.Y. TIMES, Oct. 15, 1991, at A1.

"for a reasonable charge,"[4] nothing other than corporate discretion prevents credit reporting agencies from selling those personal records to whomever they choose.

The most intimate personal information regarding nearly every American adult, including age, marital status, salary, home address and phone, medical procedures paid for (or unpaid for), and debts owed, is thereby freely traded, without the authorization of the individual from whom it was collected. Not only does this practice intrude on individual privacy by its unauthorized disclosure of personal data, it also perpetuates an economic imbalance. Private companies with the resources to collect or purchase personal data are presently able to exploit that information virtually free from legislative restraint and gain economically without compensating the people whom that data describes, or protecting them in case damage ensues due to its mishandling.

The 1989 murder of actress Rebecca Schaeffer is an extreme, though illustrative example of the destruction that the lack of informational privacy can cause. Ms. Schaeffer, the co-star of the television series "My Sister Sam," was killed outside her Los Angeles apartment by an obsessed fan who acquired her address from the California Department of Motor Vehicles.[5]

Although governmentally-held personal information is purportedly protected from misuse,[6] no such restrictions on the DMV's distribution of this personal data existed at the time of Ms. Schaeffer's death. The lack of protection for similar records retained in innumerable private sector databases reveals the potential for abuse of the personal information of every citizen.

Consider, for example, what happened to Supreme Court nominee Robert Bork during his confirmation hearings. A Washington D.C. weekly newspaper published a list of the 146 videotapes Bork and his wife had rented over a two year period.[7] Fortunately for Mr. Bork and his wife, their videotape choices were socially inoffen-

4. The Federal Fair Credit Reporting Act § 612, 15 U.S.C. § 1681j (1988).

5. James Harney, *DMV: Registered Driver: License Plate: Confidentiality*, USA TODAY, Mar. 10, 1992, at 3A.

6. The Privacy Act of 1974 provides: "No agency shall disclose any record . . . by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. . . ." 5 U.S.C. § 552a(b) (1988).

Similarly, the Right to Financial Privacy Act of 1978 provides that: "[N]o Government authority may have access to . . . the information contained in the financial records of any customer from a financial institution unless . . . such customer has authorized such disclosure . . . ." 12 U.S.C. § 3402(1) (1988).

7. *Personalities*, WASH. POST, Sept. 26, 1987, at C3.

sive. Had the list included pornography or other provocative material, damage to his career or their marriage may have been great.

In response to that incident, Congress passed the Video Privacy Protection Act,[8] proscribing disclosure of personal data by "videotape service provider[s]."[9] However, there is no similar protection for records about the purchase of magazines, books, music, computer software, mail order merchandise, airline tickets, foods, film developing and the range of consumer goods and services purchased by American citizens.[10] Companies are free to collect and sell this information without restriction or notice to consumers.[11] The following troubling examples illustrate the extensive potential for privacy invasions permitted by the current lack of protections.

> Purchasers of pregnancy-testing kits may receive solicitations from pro- and anti-abortion groups, or from sellers of birth-control products and diaper services. Purchasers of weight-loss products or participants in diet programs may be targeted for promotional offers from sellers of candy, cookies and ice cream, or, conversely, those whose purchases of the latter exceed the average may receive offers for weight-loss products and services. Subscribers to gay and lesbian publications may be targeted by religious and therapeutic organizations or face employment denials, harassment, and even blackmail. Frequent travelers and those with multiple residences may receive solicitations from sellers of home-security products, and such lists would be a boon to sophisticated burglars. A list of tobacco users might be of interest to potential employers and insurance companies. A list of those with credit troubles and excessive indebtedness would certainly be of interest to promoters of scams that promise to help people obtain credit cards or get out of debt. A cynic might even hypothesize that such a list would be used by promoters of alcoholic beverages, sweepstakes advertising, and gambling junkets.[12]

Individuals are also not protected from the errors made by mailing-list merchants. According to Bankcard Holders of

---

8. The Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 1395 (1988) (codified at 18 U.S.C. § 2710 (1988)).

9. 18 U.S.C. § 2710(b)(1). The Act provides: "A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d)." *Id.*

10. *See* 137 CONG. REC. H755, H756 (daily ed. Jan. 29, 1991) [hereinafter Rep. Wise's Introductory Remarks] (statement of Rep. Wise introducing H.R. 685).

11. *Id.*

12. Gary T. Marx, *Privacy and Technology*, WHOLE EARTH REV., Winter 1991, at 90, 92.

America, a consumer advocacy group, thirty-five percent of those who pay to see their own credit reports find that their credit report contains someone else's data.[13]

> [In one such incident,] Michael Riley, a Washington-based Time magazine reporter, jumped at the mail solicitation he received in late 1989 for a pre-approved Citibank visa card. A few weeks later, his wife, Arline, was about to buy a blouse when the cashier told her the card was no good.
>
> When the Rileys checked further with Citibank, they were told that their car had been repossessed, they faced $70,000 in tax liens and that they had filed for bankruptcy. As it turned out, Citibank, which had purchased its credit information from TRW, according to Riley, had confused Michael George Riley with a Michael Gilbert Riley.[14]

Horror stories like this could be avoided if legislation required that data collectors acquire the data subject's consent prior to distributing personal information.

Medical records are similarly unprotected. Health insurers maintain vast databases of patients' medical records, which the insurers claim they keep private.[15] But self-insured employers also have access to such data which they can use to educate or even discipline employees.[16] Only employer discretion, not legislation or regulation, determines how employee medical records are used.[17]

The marketing industry claims that access to such information is vital to the health of their business.[18] The claims are that no harm is done to the consumer by the free dissemination of this information. On the contrary, argue claim marketers, the consumer is able to enjoy greater, focused access to the products she wants and will receive less junk mail if tailored marketing can be achieved via free access to this personal data.[19] But this argument ignores the threats to personal privacy engendered by the unrestricted free trade in personal data.

While large marketing firms may have security measures in place to prevent disclosure of the personal data in their computer

---

13. Daniel Mendel-Black & Evelyn Richards, *Peering Into Private Lives: Computer Lists Now Profile Consumers by their Personal Habits*, WASH. POST, Jan. 20, 1991, at H1, H6.

14. *Id.*

15. Milt Freudenheim, *Software Controls on Health Costs*, N.Y. TIMES, Feb. 18, 1992, at D2.

16. *Id.*

17. *Id.*

18. *See* Mendel-Black & Richards, *supra* note 13, at H6.

19. *See id.*

memories to those who might mishandle that data, smaller companies might not be able to afford such care. Smaller companies also might not have the assets to recompense a consumer damaged by the misuse of her data.

Nonetheless, in order to offer marketing opportunities to small businesses, Lotus Development and Equifax were planning to market a CD-ROM product known as Lotus Marketplace: Households ("Marketplace") in 1991.[20] The Marketplace database cataloged information on 80 million households[21] and 120 million consumers[22] including names, addresses, estimated income, and propensity to buy over 100 consumer product categories.[23] The product was to retail for $695, and was targeted at small businesses.[24] But Marketplace was never released because some 30,000 consumers demanded that their names be removed from the CD-ROM.[25] However, no existing legislation would have prevented its sale. The protection of personal privacy should not depend merely on consumer protests, the timely reporting of a potentially threatening product's release, or the fortuitous decision of company executives.

Protection of personal data in the private sector historically has been provided by legislation tailored to remedy narrowly perceived problems. Congress has passed legislation to protect consumer's informational privacy in the financial,[26] cable television,[27] and the video retailing industries.[28] Such niche legislation, however, does not effectively protect personal privacy across the broad spectrum of situations where it is threatened.

Personal data is also protected by the private sector itself, but only when it serves private sector interests. As noted by the Chief Executive Officer of Citicorp's Point-of-Sale Information Services, Jerry Saltzgaber, "[t]hose of us involved in consumer marketing are the best agents for protecting the consumer's privacy, because if we don't, we won't have a business."[29]

However, there is an inherent conflict of interests when companies serve as both collectors and protectors of personal data. Ar-

20. Jacob Sullum, *Secrets for Sale: Do Strangers with Computers Know Too Much About You?*, REASON, Vol. 23, April 1992, at 29.
21. Mendel-Black & Richards, *supra* note 13, at H1.
22. Sullum, *supra* note 20, at 29.
23. *See* Mendel-Black & Richards, *supra* note 13, at H1.
24. Sullum, *supra* note 20, at 29.
25. *Id.*
26. Right to Financial Privacy Act of 1978 §§ 1101-22, 12 U.S.C. §§ 3401-22 (1988).
27. Cable Communications Policy Act of 1984 § 631, 47 U.S.C. § 551 (1988).
28. Video Privacy Protection Act of 1988 § 2(a)(2), 18 U.S.C. § 2710 (1988).
29. *Hearing Record*, *supra* note 1, at 88.

guably, when a company is threatened by an economic recession, for example, one cannot expect it to put consumers' interests above its own. Nor can it be expected to forego the exploitation of all its assets, including its consumer database, to protect its business interests. Thus personal data is subject to the vagaries of the economy and corporate discretion. Such an insecure system for protecting personal data is inadequate to guarantee informational privacy rights. Individuals need protection from the private sector itself, both from unnecessary collection of personal data and from its unauthorized disclosure.

In an attempt to reconcile the interests of personal privacy and American business development, Representative Robert Wise of West Virginia has proposed the establishment of a Data Protection Board (DPB).[30] Rep. Wise's bill is an idea whose time has come,[31] but the proposed "watchdog"[32] DPB has not been provided with the teeth to accomplish its stated purpose. As proposed, the DPB only has advisory power.[33]

The "Functions of the Board" section of the House bill[34] provides that the DPB shall develop guidelines for use by Federal agencies in implementing the Privacy Protection Act of 1974[35] (the "Privacy Act").[36] In addition, with respect to the Privacy Act, the DPB shall assist federal agencies, publish a guide, issue advisory opinions, investigate compliance, and make recommendations for amending the Freedom of Information Act[37] and the Privacy Act.[38]

Representative Wise has proposed two goals for the DPB: to protect personal privacy and to ensure that American businesses can compete in the European Community.[39] However, neither goal

30. H.R. 685, 102d Cong., 1st Sess. (1991).

31. A Data Protection Board has been proposed in Congress at least twice before. Rep. Wise introduced a bill to establish such a board on November 15, 1989. H.R. 3669, 101st Cong., 1st Sess. (1989). Senator Samuel J. Ervin, Jr. introduced S. 3418 (which was passed to become the Privacy Act of 1974) to create a Federal Privacy Board on May 1, 1974.

In addition, the Computer Security Act of 1987, Pub. L. No. 100-235, § 3(2), 101 Stat. 1724, 1724-25 (codified at 15 U.S.C. § 278g-3(a)(3) (1988)), mandated that the National Institute of Standards and Technology develop "standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems." *Id.*

32. Rep. Wise's Introductory Remarks, *supra* note 10, at H756.

33. H.R. 685 § 2(c)(2)(A).

34. Provision (c) in H.R. 685, "Functions of the Board," would become section 5(c) of the Privacy Act of 1974. H.R. 685 § 2.

35. 5 U.S.C. § 552a (1988). The Privacy Act of 1974 protects individuals from unauthorized disclosures of personal data by the federal government. *Id.*

36. H.R. 685 § 2(c)(1)(A).

37. 5 U.S.C. § 552 (1988).

38. H.R. 685 § 2(c).

39. Rep. Wise's Introductory Remarks, *supra* note 10, at H755-56.

will be well served by a government board charged with merely "guiding," "opining" and "recommending" means of achieving informational privacy. Furthermore, a DPB whose primary legislative guides are the Privacy Act of 1974 and the Freedom of Information Act (which regulate governmentally held personal data) will have little impact on private sector users of consumer data.

The lack of a central U.S. data protection authority (like the DPB) has also left American industry unrepresented when international decisions are made about transborder data use by multinational companies. Furthermore, the data protection legislation of many countries prevents the transfer of personal data to another country in the absence of reciprocal data protection legislation,[40] which ensures that personal data will be as well protected in the transferee country as it was in its native country. The U.S. has no such reciprocal legislation.

The European Commission has issued draft Directives that would preclude transfers of personal data between countries that have not "ensure[d] an adequate level of protection."[41] The Commission may decide that a particular country has adequate personal data protection by reason either of its international commitments or domestic law.[42] Rep. Wise noted that "[a]doption of this Directive [without concomitant legislation in the U.S.] could make it expensive or impossible for American companies that need to transfer personal data to and from Europe to do business. The result could be a loss of jobs, profits, and business opportunities for America."[43]

The conflict between the United States' need for open access to the EC market and the EC's intention to require reciprocal data protection laws poses an economic imperative for the United States. Failure to put adequate data protection laws in place and represent U.S. business interests in this regard may cause U.S. businesses to suffer.[44] American banks, for example, which are prevented from transferring personal account data from Switzerland to New York will find it difficult to compete in the transnational market with Swiss banks which face no such impediment to transferring data.[45]

---

40. *See Hearing Record*, *supra* note 1, at 3.

41. *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data*, art. 24.1, 1990 O.J. (c277) 3,10 [hereinafter *Draft Directive*].

42. *Id.* at 10.

43. Rep. Wise's Introductory Remarks, *supra* note 10, at H756.

44. *Id.*

45. *See id.* Rep. Wise noted in his Opening Statement before the Subcommittee Hear-

The United States is faced with either creating legislation to protect personal data and national business interests, or subjecting American companies to a regulatory apparatus controlled in Brussels, review of American companies' management practices by European bureaucrats and the determination by European courts of American companies' legal liabilities.[46]

Recognizing, at least for argument's sake, that this latter alternative is not workable, the problem is how to balance the privacy concerns of American consumers and the European Commission against the profit-driven needs of American companies. Achieving this balance will ensure a competitive position for U.S. businesses in the E.C., and privacy protection for people.

The solution consistently chosen to resolve related problems by the U.S. government[47] and EC countries[48] is a simple one. Companies can satisfy privacy concerns by merely obtaining permission to use personal data (for purposes other than the purpose for which it was provided) from the source-individual. Business' resistance to adopting this solution on its own is great, due to perceived costs and a perceived loss of autonomy to exploit information.[49] However, such resistance can be neutralized, adherence ensured across the private sector, and reciprocal legislation requirements fulfilled if federal legislation is passed compelling businesses to acquire an individual's authorization prior to disclosing (or otherwise making use of) her personal data.

In order to demonstrate the viability of adopting such legisla-

---

ings on the DPB bill that "[r]ecently, for instance, the French data protection commission stopped Fiat in France from transferring information about its employees to Fiat in Italy." *Hearing Record, supra* note 1, at 3.

46. Rep. Wise's Introductory Remarks, *supra* note 10, at H757.

47. The Privacy Act of 1974 provides: "No agency shall disclose any record . . . except pursuant to a written request by, or with *the prior written consent* of, the individual to whom the record pertains . . . ." 5 U.S.C. § 552a(b) (1988) (emphasis supplied). The Right to Financial Privacy Act of 1978 provides that "no Government authority may have access to . . . the information contained in the financial records of any customer from a financial institution unless . . . *such customer has authorized* such disclosure . . . ." 12 U.S.C. § 3402(1) (1988) (emphasis supplied).

48. The Directives proposed by the European Commission in July 1990 seek to harmonize the data protection laws of EC countries. Most of those countries, however, including Austria, Belgium, France, Germany, Greece, Italy, the Netherlands, Norway, Spain Switzerland and the United Kingdom already have data protection laws which require that stored data be used only for the purposes stated when the data was originally collected. Those same laws provide the data subject with objection, correction and erasure rights regarding personal data. *European Data Protection Survey*, BULL. (Info. Technology Law Group/Eur.) Issue 6, Autumn 1991.

49. Lovella Miles, *Feeling the Draft; European Community's Data Protection Directive*, MARKETING, May 30, 1991, at 16.

tion, this article will examine the legal and policy bases for such a privacy law and will explain why this form of privacy protection will provide benefits to all involved parties, far outweighing any potential harms.

II. BASES FOR PROTECTING INFORMATIONAL PRIVACY

A. *Constitutional Basis for Protecting Informational Privacy*

Although the United States Constitution does not contain the word "privacy," the Supreme Court has recognized various privacy rights based on several of the Amendments. Justice Douglas outlined the "zones of privacy" protected by the Bill of Rights in *Griswold v. Connecticut*.[50]

> The right of association contained in the penumbra of the First Amendment is [a zone of privacy]. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."[51]

Griswold represented the Supreme Court's first recognition of a fundamental privacy right. Douglas' opinion held that Connecticut's anti-contraceptive statute violated the right of marital privacy, a right "older than the Bill of Rights."[52]

However, while the *Griswold* Justices agreed that there was a "right to privacy," they disagreed about the constitutional basis for the right.[53] Eight years later, Justice Blackmun's opinion in *Roe v.*

---

50. 381 U.S. 479, 484 (1965).

51. *Id.*

52. *Id.* at 486.

53. Justice Goldberg attributed the "fundamental personal [privacy] right" to those unenumerated rights retained by the people pursuant to the Ninth Amendment. *Id.* at 486-87.

Justice Harlan applied a traditional due process analysis, holding that the Connecticut statute violated "basic values 'implicit in the concept of ordered liberty'." *Id.* at 500 (citing Palko v. Connecticut, 302 U.S. 319, 325 (1937)).

Justice White also found that the Connecticut Statute imposed on a Fourteenth Amendment liberty which he defined as "a 'realm of family life which the state cannot enter' without

Wade[54] identified the source of *Griswold's* "right to privacy" as the Due Process Clause of the Fourteenth Amendment.[55]

Douglas' "zones of privacy" were further defined in the Court's decisions following *Griswold*. The Court found that the Due Process Clause's substantive protection for "fundamental" rights safeguards the right to decide to marry,[56] the right to decide to end a pregnancy,[57] and the right of parents to make decisions regarding the education and upbringing of their children.[58]

The series of Supreme Court decisions leading from *Griswold* was narrowed by Justice White's opinion in *Bowers v. Hardwick*[59] to "a fundamental individual right to decide whether or not to beget or bear a child."[60] The *Bowers* Court claimed that "none of the rights announced in [the *Griswold* line of] cases bears any resemblance to the claimed constitutional right of homosexuals to engage in acts of sodomy,"[61] thereby upholding Georgia's anti-sodomy statute. Justice White's opinion shifted the Court's focus and holding away from the right to privacy to the very narrow right to engage in sodomy. Justice Blackmun's dissent acknowledged this shift, reasoning that

> [t]his case is [not] about "a fundamental right to engage in homosexual sodomy". . . . Rather, this case is about "the most comprehensive of rights and the right most valued by civilized men," namely, "the right to be let alone."[62]

By narrowly construing its prior privacy-related holdings, the *Bowers* Court ignored the Due Process basis for the right to privacy as identified in *Roe*. Instead, the Court relied on historical notions of liberty which precluded finding that the right to engage in sodomy was a "fundamental" right.[63]

---

substantial justification." *Id.* at 502 (citing Prince v. Massachusetts, 321 U.S. 158, 166 (1943)).

54. 410 U.S. 113 (1973).

55. *Id.* at 153 ("This right of privacy, whether it be founded in the Fourteenth Amendment's concept of . . . liberty . . . *as we feel it is*, or . . . in the Ninth Amendment . . . is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.") (emphasis supplied).

56. Loving v. Virginia, 388 U.S. 1 (1967).

57. Roe v. Wade, 410 U.S. 113 (1973).

58. Carey v. Population Servs. Int'l, 431 U.S. 678, 708 (1977)(Powell, J., concurring); and Parham v. J.R., 442 U.S. 584 (1979).

59. 478 U.S. 186 (1986).

60. *Id.* at 190.

61. *Id.* at 190-191.

62. *Id.* at 199 (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

63. *Id.* at 192-194.

The Court also constricted the right to privacy in *Paul v. Davis*.[64] That decision denied constitutional protection against the public disclosure by police of the respondent's arrest on a shoplifting charge, even though the respondent had never been convicted.[65] The Court characterized the respondent's claim as defamation, and therefore not within the meaning of either "liberty" or "property" as used in the Due Process Clause.[66]

Justice Rehnquist's majority opinion distinguished "fundamental" privacy rights "relating to marriage, procreation, contraception, family relationships, and child rearing and education" from the right to non-disclosure of personal information.[67] The opinion foreclosed Due Process protection of informational privacy unless unauthorized disclosure threatens the exercise of "fundamental" rights. Rather, Justice Rehnquist suggested the respondent seek relief via his state's tort laws.[68]

In a contrasting opinion issued a year later, *Whalen v. Roe*,[69] Justice Stevens wrote that "[t]he right to collect and use [personal] data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures .... [I]n some circumstances that duty arguably has its roots in the Constitution...."[70] The opinion recognized that the privacy which the Due Process Clause safeguards includes two different types of interests: "the individual interest in avoiding disclosure of personal matters, and... the interest in independence in making certain kinds of important decisions."[71]

Read together, the *Davis* and *Whalen* opinions bear out one commentator's conclusion that "the Supreme Court suffers from a severe case of schizophrenia."[72] Justice Stevens' acknowledgment in *Whalen* of Due Process Clause protection for "disclosure of personal matters" contradicts Justice Rehnquist's denial in *Davis* of the Due Process right to informational privacy. The second right noted by Justice Stevens, however, the right to autonomy in personal decision-making, is consistent with the *Griswold* line of cases, and with

64. 424 U.S. 693 (1976).
65. *Id.*
66. *Id.* at 711-12.
67. *Id.* at 713.
68. *Id.* at 712.
69. 429 U.S. 589 (1977).
70. *Id.* at 605.
71. *Id.* at 599-600.
72. Michael P. Seng, *The Constitution and Informational Privacy, or How So-Called Conservatives Countenance Governmental Intrusion into a Person's Private Affairs*, 18 J. MARSHALL L. REV. 871, 875 (1985).

Davis's protection against unauthorized disclosure when such disclosure threatens the exercise of "fundamental" rights.

This reasoning is bolstered by the Court's decision in *Nixon v. Administrator of General Services.*[73] In that case, the Court held that President Nixon's assertions of informational privacy in his official records were outweighed by a public interest in the documents. The Court's use of a balancing test implies that the Court recognized a Constitutional right to informational privacy. If President Nixon did not have such a right, such balancing by the Court would have been unnecessary.[74]

The Court has also employed a balancing test to weigh "the right of every person 'to be let alone' . . . [against] the right of [businesses] to communicate."[75] In *Rowan v. U.S. Post Office Department,*[76] mailing list brokers brought suit to challenge the constitutionality of a statute[77] which required removal of consumers' names from mailing lists at the consumers' request.[78] The Court found that the statute violated neither the First Amendment's "right to communicate"[79] nor the Due Process Clause.[80] The Court affirmed the consumer's right to control the contents of her mailbox and the use of her name and address because "[t]o hold less would tend to license a form of trespass," and because "[n]othing in the Constitution compels us to listen to or view any unwanted communication."[81] Thus Chief Justice Burger's opinion found the right to privacy, in the context of prohibiting pandering

---

73. 433 U.S. 425 (1977). "One element of privacy has been characterized as 'the individual interest in avoiding disclosure of personal matters. . . .' " *Id.* at 457 (quoting *Whalen,* 429 U.S. at 599).

74. William C. Lindsay, *When Uncle Sam Calls Does Ma Bell Have to Answer?: Recognizing a Constitutional Right to Corporate Informational Privacy,* 18 J. MARSHALL L. REV. 915, 920 (1985).

75. Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 736 (1970).

76. 397 U.S. 728 (1970).

77. Title III of the Postal Revenue and Federal Salary Act of 1967, 39 U.S.C. § 4009 (1964, Supp. IV).

78. 39 U.S.C. § 4009 . . . provides that

> a person who has received by mail "a pandering advertisement which offers for sale matter which the addressee in his sole discretion believes to be erotically arousing or sexually provocative," may request the Postmaster General to issue an order "directing the sender and his agents or assigns to refrain from further mailings to the named addressee." Such order would also require the sender to delete the addressee's name from his mailing lists and would prohibit him from trading in lists from which the deletion has not been made.

397 U.S. at 728.

79. *Id.* at 735.

80. *Id.* at 738.

81. *Id.* at 737.

advertisements in the mails, greater than businesses' right to communicate.

The *Rowan* decision provides a basis for individual control over the exploitation of personal information. The opinion clearly finds that one aspect of commercial solicitation is not necessarily protected under the First Amendment. Despite the limited focus of the statute challenged in *Rowan*, the Court found Congress' intent to be quite broad:

> In operative effect the power of the householder under the statute is unlimited; he may prohibit the mailing of a dry goods catalog because he objects to the contents - or indeed the text of the language touting the merchandise. Congress provided this sweeping power not only to protect privacy but to avoid possible constitutional questions that might arise from vesting the power to make any discretionary evaluation of the material in a governmental official.
>
> In effect, Congress has erected a wall - or more accurately permits a citizen to erect a wall - that no advertiser may penetrate without his acquiescence.[82]

Although the Court has not found informational privacy to be a fundamental right, its decisions support the notion that the individual's right to informational privacy exists, and must be balanced against the public interest.

As new technologies make collection of information about individuals easier and more insidious, the Court will increasingly be faced with decisions whether to allow intrusion into what Justices Warren and Brandeis termed the "inviolate personality" of the private individual.[83] To allow such intrusion will further limit individual liberty, will discourage personal autonomy and will surely usher in an era of "Big Brother," where the individual is unable to contribute to the greater human good for fear of incurring the government's wrath.

Although statutory protection (as urged by this article) is essential to ensure that businesses and individuals know their rights and responsibilities regarding informational privacy, such rights will be secure only if they are Constitutionally protected. One way

---

82. *Id.* at 737-38.

83. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205, 207, 213 (1890). Warren and Brandeis also noted that "[i]f we are correct in this conclusion [the existence of a right to privacy based on an inviolate personality], the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device . . . ." *Id.* at 206.

to overcome the Court's selective application of the right to privacy is to amend the Constitution to acknowledge that its protections apply regardless of the technologies which threaten our freedoms. Professor Laurence H. Tribe has proposed the following 27th Constitutional Amendment to address the threats to the Constitution's core values in the technological age.

> This Constitution's protections for the freedoms of speech, press, petitions, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted, or controlled.[84]

Professor Tribe's proposed Amendment is necessary to guarantee that the values of freedom, privacy and equality protected by the 18th century Bill of Rights continue unfettered. It would be more comforting if the Supreme Court itself were to consistently interpret the terms of the Constitution so that, for example, the right to privacy found in the Due Process Clause applied equally whether one freely provided a personal phone number, or it was acquired without one's permission via Caller I.D. technology.[85]

But the Court's decisions are not so consistent. For example, while *Roe v. Wade*[86] acknowledged a woman's right to choose how she uses her body, *Bowers v. Hardwick*[87] deprived homosexuals of that same right. Though these cases are based on physically-oriented rights, the rights we have in intangible personalty, like our personal information, are no less precious and no less deserving of protection.

In the context of achieving consistency in the protection of fundamental rights across technologies, acceptance of Professor Tribe's proposal is appropriate. But in the context of non-fundamental rights such as informational privacy, it is insufficient. Protection of informational privacy requires legislation tailored to the reality of the marketplace. Such legislation will not merely assert the existence of such rights regardless of technology, but will also satisfy the

---

84. John Markhoff, *Remember Big Brother? Now He's a Company Man*, N.Y. TIMES, Mar. 31, 1991, at E7.

85. Caller I.D. is a technological service provided by telephone companies in 22 states which "allows a subscriber to identify and record the telephone number of an incoming call, and therefore presumably to determine the caller's identity." Anthony Ramirez, *New York State Approves Caller-Identification Service*, N.Y. TIMES, Mar. 12, 1992, at D1.

86. 410 U.S. 113 (1973).

87. 478 U.S. 186 (1986).

commercial need for information in a manner that is fair to the consumer.

B. *Legislative Basis for Protecting Informational Privacy*

If the Supreme Court has stopped short of expressly recognizing the right to informational privacy, Congress has not been so timid. Congress' recognition of privacy rights is manifest in the proliferation of legislation protecting the individual from governmental intrusion[88] and from the exploitation of personal data by private organizations.

For example, the Fair Credit Reporting Act of 1970[89] prohibits consumer reporting agencies from disclosing consumer data except in specified circumstances.[90] The Right to Financial Privacy Act of 1978[91] provides individuals with the right to notice of a request before a financial institution may disclose records to government agencies.[92] The Cable Communications Policy Act of 1984[93] prohibits cable operators from disclosing personal data regarding subscribers without the consent of the subscriber.[94] The Electronic Communications Privacy Act of 1986[95] protects against the unauthorized interception of electronic communications.[96] The Video Privacy Protection Act of 1988[97] protects personal data held by videotape service providers.[98]

These laws clearly express that Congress has perceived the need to protect individual privacy. For example, included among the Congressional findings regarding the Fair Credit Reporting Act (FCRA) is the following:

> There is a need to insure that consumer reporting agencies exercise their grave responsibilities with. . . a respect for the consumer's right to privacy.[99]

---

88. Freedom of Information Act, 5 U.S.C. § 552 (1988); Crime Control Act of 1973 § 812, 42 U.S.C. § 3789g (1988); Privacy Act of 1974 § 3, 5 U.S.C. 552a (1988); Right to Financial Privacy Act of 1978 §§ 1101-22, 12 U.S.C. §§ 3401-22 (1988); Privacy Protection Act of 1980 § 202, 42 U.S.C. § 2000aa-11 to -12 (1988).

89. 15 U.S.C. §§ 1681-81t (1988).

90. 15 U.S.C. § 1681b.

91. 12 U.S.C. §§ 3401-22 (1988).

92. 12 U.S.C. § 3403(a).

93. 47 U.S.C. §§ 521-611 (1988).

94. 47 U.S.C. § 551(c)(1).

95. 18 U.S.C. §§ 2510-21 (1988).

96. 18 U.S.C. § 2511.

97. 18 U.S.C. § 2710 (1988).

98. *Id.*

99. 15 U.S.C. § 1681(a)(4).

Ironically, the FCRA focuses little on privacy, and primarily on the accuracy of information held by consumer reporting agencies. Although it restricts distribution of credit reports to certain "permissible purposes,"[100] it does not prohibit general disclosure of consumer data.[101] Thus, although Congress' intention in enacting the FCRA, and the other legislation noted above, was to protect consumer privacy, these laws fall short of this goal.

Congress has recognized the need for and demonstrated a desire to protect personal privacy and commercial access to information, but has thus far failed to enact legislation that accomplishes both purposes in a comprehensive, effective manner. Satisfaction of Congress' intentions requires a law that establishes privacy standards for all industries to follow, and a mechanism to ensure its enforcement.

C. *Common-Law Basis for Protecting Informational Privacy*

1. Tort

Justice Rehnquist's assertion in *Paul v. Davis*[102] that individuals must look to state tort law to protect their privacy[103] acknowledges that such protection exists. Indeed, the common-law right of privacy has traditionally given rise to a tort action for a violation of that right.

Dean Prosser has identified four generally recognized state tort actions for invasion of privacy:[104] intrusion on physical solitude and seclusion,[105] public disclosure of private facts,[106] false light in the public eye,[107] and appropriation of one's name or likeness.[108] In the context of informational privacy, two of the actions described by Prosser are material: intrusion and public disclosure.

A tortious intrusion of an individual's privacy may stem from the fact that corporations sell personal information without the authorization of the individual from whom it was collected. The initial collecting of information may not constitute an intrusion on the

100. 15 U.S.C. § 1681b.

101. The allowable circumstances for furnishing a consumer report include "a legitimate business need . . . in connection with a business transaction involving the consumer." *Id.* § 1681b(3)(E).

102. 424 U.S. 693 (1976)

103. *See supra* note 68 and accompanying text.

104. WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 804 (4th ed. 1971).

105. *Id.* at 807.

106. *Id.* at 809.

107. *Id.* at 812.

108. *Id.* at 804.

individual. In fact, the individual seeking a magazine subscription, or insurance, or credit may initiate and volunteer information. However, when the collecting corporation sells that information to a third party, it provides the third party with unauthorized access to personal facts regarding the individual and is thereby intruding on the individual.

Prosser notes that this "form of invasion of privacy consists of intrusion upon the [individual's] physical solitude or seclusion."[109] In the context of informational privacy, courts have found a tortious violation of this interest where there was prying into confidential records such as bank records.[110]

Similarly, the selling or leasing of personal data constitutes a public disclosure of private facts. While the sale of a list of consumer data by one company to another may not appear to be "public" disclosure, list brokers sell thousands of lists every year, and such a distribution has been held to be public.[111] Also, consider the Marketplace information product announced in April 1990 by Lotus Development and Equifax, but never released.[112] By offering the names, addresses and consumer habits of 120 million Americans to small businesses, Marketplace assured a wide (public) disclosure of private facts and therefore a tortious invasion of informational privacy.

Despite the seemingly viable claim that the practice of selling mailing lists is an invasion of privacy by intrusion into another's seclusion, most such cases result in findings of nonliability.[113] It appears that courts are very reluctant to find damage to the consumer and resultant liability to the data collector/distributor based on mere unauthorized disclosure of personal information.[114] This result is unjust, but not unexpected, given a legal tradition which provides for tort recovery only when some palpable damage can be shown. The damage which results from an invasion of informational privacy is more commonly in the realm of lost opportunity than in physical or mental suffering. Thus claims based on viola-

109. *Id.* at 807.

110. Brex v. Smith, 146 A. 34 (N.J. Ch. 1929).

111. *See* STANDARD RATE & DATA SERVICE, DIRECT MAIL LIST RATES AND DATA (April 1993); Kerby v. Hal Roach Studios, 127 P.2d 577 (Cal. Ct. App. 1942) (holding the distribution of a letter to a thousand men to be a public distribution).

112. *See supra* notes 20 - 25 and accompanying text.

113. Jeffrey F. Ghent, *Unsolicited Mailing, Distribution, House Call, or Telephone Call as Invasion of Privacy*, 56 A.L.R.3d 457 §§ 8-16 (1974).

114. *Id.*

tions of property rights and, more likely, breach of contract present stronger bases for successful actions.

2. Property

Defining information as property and affording rights to information "owners" makes for a prescient argument. American intellectual property law has historically resisted conferring property rights to the possessor of information.[115] Rather, its goal has been the free circulation of information. Even more significantly, the existing statutory scheme for protecting intangible property does not provide for the essential difference between information and tangible property. Specifically, tangible property decreases in value when it is divided, while information does not.[116]

As the concentration of wealth in information increases, a legal scheme for protecting information rights will emerge of necessity. Property laws have historically developed in response to new definitions of wealth. Such laws will be based on an expanded definition of property which will encompass claims of informational privacy. Until these new laws are written, the copyright and patent schemes provide an exceedingly insufficient model for protection of rights in information.

The Constitutional clause on which the patent and copyright laws are based grants Congress the power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[117] The statutes based on this clause have sought to balance the free dissemination of ideas against the state's interest in encouraging authors and inventors to maintain the "Progress of Science and useful Arts." Thus protection of author's and inventor's rights is limited to providing a financial return on their expressions, (not their ideas) for a limited time only.[118]

In the case of copyright law, authors are granted the exclusive

115. *See* Douglas G. Baird, *Common Law Intellectual Property and the Legacy of International News Service v. Associated Press*, 50 U. CHI. L. REV. 411, 411 (1983) ("That information once published should be presumptively free for all to use is a commonplace of intellectual property law.").

116. Thomas Jefferson wrote of information's unique ability to be infinitely divisible without losing value in 1813: "He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me." 6 WRITINGS OF THOMAS JEFFERSON 180 (H. A. Washington ed., 1857).

117. U.S. CONST. art. I, § 8, cl. 8.

118. Current copyright law provides for rights to last for the life of the author plus 50 years. 17 U.S.C. § 302(a) (1988). Patent rights are granted for 17 years. 35 U.S.C. § 154 (1988).

right to copy, distribute, perform, display and license their creations,[119] thereby protecting the author's right to profit from the work. The information (ideas) contained in the work, however, are essentially public domain material.[120]

In *Feist Publications v. Rural Telephone Service*,[121] the United States Supreme Court asserted that facts are uncopyrightable because they are "discovered" by humans rather than "created."[122] The Copyright Act of 1976 as amended[123] provides that copyright protection does not extend to discoveries, even when embodied in a copyrighted work.[124]

Similarly, patent law grants to the inventor the right to exclude others from making, using and selling a patented invention.[125] Although patents themselves "shall have the attributes of personal property,"[126] the information on which the invention is based is public domain when the patent is granted.[127]

In dramatic contravention of the intellectual property tradition of denying property rights in information, two recent Supreme Court decisions classified information as private property.[128] In *Ruckelshaus v. Monsanto Co.*,[129] the Court held that research data submitted to a federal agency could be considered 'property' within the meaning of the Fifth Amendment to the Constitution.[130] In *Carpenter v. United States*,[131] the Court held that a newspaper "had a property right in keeping confidential and making exclusive use,

119. 17 U.S.C. § 106 (1988).

120. Section 107 of the Copyright Act provides in pertinent part that "use of a copyrighted work, including such use by reproduction in copies or . . . by any other means . . . for purposes such as criticism, comment, news reporting, teaching . . ., scholarship, or research, *is not an infringement of copyright.*" 17 U.S.C. § 107 (1988) (emphasis supplied).

121. 111 S.Ct. 1282 (1991).

122. *Id.* at 1287.

123. 17 U.S.C. §§ 101-810 (1988).

124. *Id.* § 102(b).

125. *See* 35 U.S.C. § 271 (1988).

126. 35 U.S.C. § 261 (1988).

127. 35 U.S.C. § 113 (1988) provides that: "[t]he applicant shall furnish a drawing where necessary for the *understanding* of the subject matter sought to be patented." (emphasis supplied). 35 U.S.C. § 10 (1988) provides that "[t]he Commissioner may furnish certified copies of specifications and drawings of patents issued by the Patent and Trademark Office, and of other records available either *to the public* or the person applying therefore." (emphasis supplied).

128. For an in-depth analysis of these two cases and the issue of whether property rights may exist in information, *see* Pamela Samuelson, *Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?*, 38 CATH. U. L. REV. 365 (1989).

129. 467 U.S. 986 (1984).

130. *Id.* at 1003.

131. 484 U.S. 19 (1987).

prior to publication," of the contents of a newspaper column.[132]

These two cases are the forerunners of a new concept about the legal status of information, a concept more appropriate to the changes wrought by the use of new technologies. If the informational rights of artificial persons like Monsanto[133] and the Wall Street Journal[134] are protected, it follows that the personal data of human beings is similarly deserving of protection.

Congress has clearly recognized the necessity that digitized information be considered "property." In the Senate Report on the Computer Fraud and Abuse Act of 1986,[135] the Committee on the Judiciary noted that a slew of enforcement problems had arisen in response to criminal conduct related to computers. "Computer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property. For example, computer data may be 'stolen' in the sense that it is copied by an unauthorized user, even though the original data has not been removed or altered in any way."[136] The Committee found that these enforcement problems could be alleviated by recognizing computerized information as property.[137]

Recognition of the need to classify information as property is the first step towards protection of the bundle of rights that give property its value. But that recognition has only begun to creep into the minds of Justices and Congresspeople. Meanwhile, informational privacy is threatened by unregulated data merchants. Therefore, a more ready basis for protection than property law must be considered.

3. Contract

One of the primary tenets of informational privacy is that personal information collected for one purpose may not be disclosed for another purpose without the data subject's consent. The fact that an individual subscribes to a tennis magazine, for example, is not an invitation to tennis equipment manufacturers to mail adver-

132. *Id.* at 25-26. *Carpenter* also references another Supreme Court case that recognizes a property right in information, specifically the news: International News Serv. v. Associated Press, 248 U.S. 215, 236 (1918).

133. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).

134. *See* Carpenter v. United States, 484 U.S. 19 (1987).

135. S. REP. NO. 432, 99th Cong., 2nd Sess. 1, *reprinted in* 1986 U.S.C.C.A.N. 2479.

136. 1986 U.S.C.C.A.N., *supra* note 134, at 2491.

137. *Id.* at 2492 ("The Committee intends S.2281 to affirm the government's recognition of computerized information as property.") The House bill was passed in lieu of the Senate bill after amending its language to contain much of the text of the Senate bill. *Id.* at 2479.

tisements to that individual. The danger is not in the receipt of unwanted mail. Rather, there is danger in societal acceptance of the idea that personal information is not subject to the individual's control. An extreme result of such a system is that total strangers may become privy to sensitive or (in the case of Rebecca Schaeffer)[138] dangerous information.

When a consumer provides information in conjunction with a purchase, there is an implicit contract. In the case of a magazine subscription, the consumer pays a subscription fee and provides a mailing address in order to receive a publication. The contract thus entails an agreement that the consumer's information (her name and address) will be used for the single purpose of delivering magazines.

When the publisher sells its subscription list to a third party, it does so in violation of the subscription "contract," and without the consent of the subscribers. List purchasers receive not only the subscriber's name and address, but also the information that each person on the list subscribed to a particular publication. This information can imply the financial position and social habits of the subscribers.

But even though the sale of mailing lists is common, the consumer is not implicitly consenting to the sale of her address when she purchases a magazine. Publishers seem to recognize this and occasionally provide a disclaimer enabling purchasers to be removed from shared mailing lists upon request.[139] While the presence of such a disclaimer might defeat a breach of contract claim by implying consent, disclaimers do not comprise actual consent, especially when hidden in the fine print, or when absent.

There are several reasons why basing an informational privacy claim on a contract theory could prove difficult. In *Shibley v. Time*,[140] the Ohio Court of Appeals found no invasion of privacy where the subscribers/plaintiffs claimed the publisher's sale of mailing lists amounted to the unconsented sale of individual "personality profiles," resulting in the publisher's unjust enrichment at the subscribers' expense.[141]

The *Shibley* opinion provides two significant reasons why any common law action, including breach of contract, provides a weak tool for pursuing an informational privacy claim. The primary diffi-

138. *See supra* note 5 and accompanying text.
139. *Hearing Record*, *supra* note 1, at 60-73.
140. 341 N.E.2d 337 (Ohio Ct. App. 1975).
141. *Id.*

culty for such a claimant is that the right of informational privacy is not widely recognized.[142] Without a right to privacy, the right of consent regarding that privacy is moot. Secondly, the court noted that "the practice complained of here [the sale of subscription lists] does not constitute an invasion of privacy even if appellants' unsupported assertion that this amounts to the sale of 'personality profiles' is taken as true because these profiles are only used to determine what type of advertisement is to be sent."[143] The court, therefore, implies that the direct marketer's unauthorized used of personal data is permissible.

State courts, therefore, provide no help to the individual damaged by unscrupulous or careless data merchants. The actual damage caused to individuals by privacy violations is hard to show in a courtroom. To argue, as in *Shibley*, that "personality profiles" are being appropriated without compensation to the individual sounds a bit far-fetched. After all, no physical or economic damage is evident. Most people are not even aware that their personal information is being regularly packaged and sold for a profit. Although the common law provides the theoretical support, at least in the tort and contract realms, for finding informational privacy rights, courts can not usurp the legislature's responsibility to write the law necessary to protect informational privacy.

D. *Public Policy Basis for Protecting Informational Privacy*

Perhaps the most obvious and impressive basis for protecting personal data is the direct impact which lack of protection has on people. In the Subcommittee[144] hearing[145] regarding the DPB bill,[146] a number of industry practices which impact on individuals were exposed.[147] These practices make clear that our current poli-

142. *See id.* at 339-40.

143. *Id.* at 339-40.

144. Subcommittee on Government Information, Justice, and Agriculture of the House Committee on Government Operations.

145. The hearing was held on May 16, 1990.

146. *Hearing Record, supra* note 1.

147. Representative Wise notes that it costs more to have an unlisted phone number, thereby causing the consumer to pay for privacy. *Id.* at 161.

Jerry Saltzgaber, Chief Executive Officer of Citicorp's Point-of-Sale (POS) Information Services described a far-reaching consumer database. "Citicorp POS maintains control of all names and addresses of our customers." *Id.* at 89.

David Czernik, Executive Director of the Louisiana Consumers League, described employers' information services which provide data about individuals' work and credit histories to prospective employers. By collecting and selling this information, companies are able to blacklist workers. Even if individuals are aware that these database records exist, it is very difficult for them to access their own records, much less correct errors. *Id.* at 139-160.

cies, which do not broadly regulate private use of personal data, place profit ahead of personal self-determination and commercial freedom before personal privacy rights.

For example, Caller I.D., a service made available through communications technology, has recently been introduced in New York State despite its negative impact on consumers.[148] The service is already available in 22 states and enables subscribers "to identify and record the telephone number of an incoming call, and therefore presumably to determine the callers' identity."[149] Advocates claim the service can be used to deter annoying calls by, for example, obscene callers.[150] But the more likely users of the service are businesses which will collect telephone numbers for commercial purposes, such as the preparation of mailing lists.[151]

There is no legislation to protect the consumer from the onslaught of this technology. Certainly, *Feist*[152] made clear that a telephone number itself, especially when publicly available in a telephone directory, is not protected. But when a woman calls an abortion clinic, and that fact is captured through a Caller I.D. service, her privacy has been violated. There should be a law protecting her informational privacy in such a case.

Although the legal establishment is just beginning to recognize the doctrinal changes that must occur to adapt to new technologies, such awareness is in its earliest stage. Perhaps, though, we can note that there is recognition for the importance of information protection for the economic health of the United States. Intellectual property exports, for example, "are one of the few areas where the United States enjoys a positive balance of trade."[153] In this age when information is a primary asset, when the effective management of information is widely recognized as the linchpin to industrial success,[154] there need to be safeguards to protect the rights of the developers and the possessors of information.

---

148. Anthony Ramirez, *New York State Approves Caller-Identification Service*, N.Y. TIMES, Mar. 12, 1992, at D1.

149. *Id.*

150. *Id.*

151. *Id.*

152. 111 S.Ct. 1282 (1991). *See supra* note 122 and accompanying text for a discussion of this case.

153. Samuelson, *supra* note 129, at 397.

154. Charles E. Cantu, *Privacy*, 7 ST. LOUIS U. PUB. L. REV. 313, 315-16 (1988) (stating that "the dissemination of information [has become] big business").

III. WHY THERE IS A NEED FOR BROAD LEGISLATION PROTECTING INFORMATIONAL PRIVACY

A. *To Protect Individuals*

It is important to recognize that the interests in need of protection relative to the EC's proposed Directives are not merely those of consumers, but also those of American businesses and the U.S. national economy. These interests are interdependent. Although legislation which specifically protects personal data in the private sector may appear to favor consumer interests, it would effectively protect business and national interests as well.

At this point, however, developing technologies appear to be rapidly reducing the power of the individual relative to large organizations. The ability of credit card companies, for example, to identify a cardholder's whereabouts at specific times as on-line card verification occurs[155] clearly demonstrates that the surveillance and intrusive abilities of the private sector are beyond the self-protective abilities of most consumers. The failure of Congress to establish enforceable rights for personal data protection subjects the most intimate aspects of our personal lives to commercial sale. We need to strike the "delicate balance," as described by the Privacy Protection Study Commission[156] in 1977, between industry's right to access and trade in information and the individual's right to maintain confidentiality in and control over her personal records.[157]

Despite agreement that there is a "need" for this legislation, Congress has been reluctant to broadly protect[158] privacy rights in this regard. As noted in the Senate Report on the bill preceding the Privacy Act of 1974:[159]

> [T]he Committee[160] was persuaded to delay a decision on total application [of privacy protection legislation to the private sec-

155. *See* John Markoff, *American Express Goes High-Tech*, N.Y. TIMES, July 31, 1988, § 3, at 1, 6.

156. The Commission was created by the Privacy Act of 1974. Pub. L. No. 93-579, § 5, 88 Stat. 1896, 1905 (1974). The Commission ceased to exist on September 30, 1977. Pub. L. No. 95-38, 91 Stat. 179 (1977).

157. *See* THE PRIVACY PROTECTION STUDY COMMISSION, REPORT ON PERSONAL PRIVACY IN AN INFORMATION SOCIETY 5-6 (1977).

158. As noted earlier, narrow legislation to protect personal data in the private sector has been enacted. *See supra* notes 26-28 and accompanying text. For example, The Video Privacy Protection Act of 1988 § 2(a)(2), 18 U.S.C. § 2710 (1988), protects videotape rental data.

159. S. REP. No. 1183, 93d Cong., 2d Sess. 1, *reprinted in* 1974 U.S.C.C.A.N. 6916 [hereinafter Privacy Act Legislative History].

160. The Government Operations Committee, authors of the Senate Report on S. 3418 which was passed as P.L. 93-579, the Privacy Act of 1974.

> tor] by considerations of time and investigative resources for developing a full hearing record and for drafting the *needed* complex legislative solution for information abuses in the private sector . . . .[161]
>
> . . . .
>
> . . . [T]he decision to authorize . . . a study [on the data banks, automated data processing programs, and information systems of the private sector as well as of regional and other governmental agencies] is based on the Committee deferral at this time of legislation for abuses of privacy, due process, and confidentiality in the private sector, *a need particularly urgent* with the growth of national data banks, application of computer technology, and use of new information management practices.[162]

Acting on the advice of industry lobbyists, Congress has avoided imposing regulations on businesses that will protect the consumer, in favor of protecting business.

> The Committee has been advised by representatives of the Direct Mail Marketing Association and by numerous prominent direct mailers that this practice [of allowing consumers to request list merchants remove their names from mailing lists] creates more profitable lists by allowing for the removal of names of individuals who are unlikely to purchase goods or services from the soliciting organization.
>
> The purpose of this provision is to extend this practice to all organizations and *to expand the protection to all individuals.* It is consistent with the best practice in American industry and with the programs and standards of the Association representing those companies with direct interest in this problem.
>
> The Committee believes such a requirement is a simple and fair one which *will not necessitate a revision of private business procedures.*[163]
>
> Where lists are maintained by private companies, the Committee believes that the decision as to who should be allowed to rent or buy them is a decision best left up to each individual business.[164]

Although the Senate Report suggests an intention to protect individuals, lack of regulation actually frees businesses to manipulate personal data at will. This practice can be dangerous for the individual, as also acknowledged in the Senate report:

Mailing lists constitute such personal information when, for ex-

---

161. Privacy Act Legislative History, *supra* note 160, at 6934 (emphasis supplied).
162. *Id.* at 6954 (emphasis supplied).
163. *Id.* at 6947 (emphasis supplied).
164. *Id.*.

> ample, they represent a group of individuals possessing a certain set of characteristics. *The disclosure of this personal information can be damaging to the individual.*[165]

If it is true, as the Committee believed, "that the decision . . . is best left up to each individual business,"[166] it is counterintuitive to regulate particular businesses as privacy threats arise, which is exactly what Congress has done by regulating the videotape retailing,[167] cable television[168] and credit reporting industries.[169]

This piece-meal approach to personal data protection makes it impossible for an individual to know her privacy rights. In the present legislative scheme, the individual cannot be assured that a given industry is required by law to protect the data she provides. If, for example, one orders videotapes from a mail-order service, one's records would be protected from disclosure.[170] But there is no legislative protection for information provided for the mail-order purchase of lingerie. Such data is exposed to unrestricted exploitation.

The current lack of a single standard of protection not only prevents the individual from effectively protecting herself, but prevents effective monitoring by a Data Protection Board. Enforcing the current legal scheme would require a DPB to oversee only those select industries (*e.g.*, videotape retailing and credit reporting) that are regulated. The majority of businesses remain free to trade in personal data and free of the proposed DPB's oversight.

In 1974, Congress passed comprehensive legislation to protect personal data stored by federal agencies, thereby setting a precedent for a comprehensive private sector law. The central concern of the Privacy Act of 1974[171] "was that information obtained for one purpose may not be used for a different purpose without the individual's consent."[172]

Ironically, though, "the Act allowed disclosure of records for

---

165. *Id.* at 6946 (emphasis supplied).

166. *Id.* at 6947.

167. Video Privacy Protection Act of 1988 § 2(a)(2), 18 U.S.C. § 2710 (1988).

168. Cable Communications Policy Act of 1984 §§ 601-39, 47 U.S.C. §§ 521-611 (1988).

169. The Federal Fair Credit Reporting Act §§ 601-22, 15 U.S.C. §§ 1681-1681t (1988).

170. 18 U.S.C. § 2710(b)(1).

171. 5 U.S.C. § 552a (1988).

172. S. REP. No. 599, 100th Cong., 2nd Sess. 2, *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-2 [hereinafter Video Privacy Protection Act Legislative History]. The Privacy Act "establishes certain minimum information-gathering standards for all agencies to protect the privacy and due process rights of the individual and to assure that surrender of personal information is made with informed *consent* . . . ." Privacy Act Legislative History, *supra* note 160, at 6917 (emphasis supplied); *see also supra* note 6.

'routine uses'[173] compatible with the purposes for which the records were collected."[174] Subsequent broad interpretations of this clause have undercut the very privacy protections embodied in the Act.[175]

The legislative and subsequent history of the Privacy Act of 1974 also make it clear that an enforcement mechanism must be included with the protective measures in order to adequately protect personal data. Although the Senate Report on the Privacy Act of 1974 indicated that a Privacy Protection Commission would be created to enforce the Act,[176] by the time of its passage, the compromised bill did not provide for a Commission. As a result, the Privacy Act,

> in comparison to data protection legislation in other countries . . . is relatively meaningless . . . . The reason is there is nobody in charge of the Privacy Act. There is a small group of people in the Office of Information and Regulatory Affairs at OMB who are supposed to do something to make the Privacy Act meaningful. . . . [T]hey can't even generate annual reports on implementation of the Privacy Act, never mind go about auditing or encouraging compliance or receiving complaints from individuals.[177]

At the 1983 Subcommittee hearings on the Privacy Act of 1974, the testimony by nongovernment witnesses was highly critical of the implementation of the Privacy Act by federal agencies.[178] Ronald Plesser, former general counsel to the Privacy Protection Study Commission,[179] noted that the Act " 'is overly complex, over bureaucratic, and contains really no effective enforcement mechanism. It has become almost totally unavailable to most citizens because of the cumbersome and frustrating nature of its enforcement remedies.' "[180]

Although the Privacy Act of 1974 does provide for civil remedies whenever any government agency fails to comply with the

---

173. 5 U.S.C. § 552a(b)(3).

174. Video Privacy Protection Act Legislative History, *supra* note 173, at 4342-2.

175. *Id.*

176. Privacy Act Legislative History, *supra* note 160, at 6918.

177. *Hearing Record*, *supra* note 1, at 79 (testimony of David H. Flaherty, Professor of History and Law, University of Western Ontario, author of PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989)).

178. *Hearing Record*, *supra* note 1, at 24.

179. The Study Commission was created by the Privacy Act of 1974 to make a "study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information . . . ." Pub. L. No. 93-579, § 5, 88 Stat. 1896, 1906 (1974).

180. *Hearing Record*, *supra* note 1, at 24.

Act,[181] without a body like the Privacy Protection Commission or Data Protection Board charged with enforcing the regulations and without agency management prioritizing the issue, federal agencies express little concern for the privacy interests of those who need protection. As Professor Flaherty described:

> The busy individuals in administrative agencies are already overworked. Moreover, those persons working on welfare issues, for example, remain more concerned about achieving surveillance of target populations than protecting anyone's privacy. Although there are coordinators for the Privacy Act in each federal agency, their role has been very limited.[182]

As Representative Wise has proposed the DPB, it will not be authorized to investigate private sector violations, nor may it regulate the private sector. Rather, the DPB may:

> investigate compliance with [the Privacy Act of 1974], and report on any violation of any provision thereof . . . to an agency, the President, the Attorney General, and the Congress.[183]

The problem with this enforcement provision is that the Privacy Act of 1974 applies only to personal data within the control of federal agencies. It does not apply to private companies which store personal information.

Furthermore, Rep. Wise intends the DPB to be "a resource, a consultant, a watchdog, and a facilitator . . . [, but not a] regulator."[184] His reasoning stems from concern over heavily bureaucratic European registration requirements for databases containing personal data.[185] For example, the European Commission's proposed Directive to protect personal data[186] requires Member States to provide for a public register of public sector files[187] and private sector files[188] where the personal data are likely to be circulated between the Member States. In the early years of the British Data Protection Act of 1984, "the data protection registrar had 292 bags of unopened mail which were simply registrations . . . they happen to have 100 staff to open the mail bags."[189]

However, fears of an unwieldy database registration scheme in

181. 5 U.S.C. § 552a(g) (1988).
182. *Hearing Record, supra* note 1, at 23-24.
183. H.R. 685, 102d Cong., 1st Sess., § 2(c)(2)(B) (1991).
184. Rep. Wise's Introductory Remarks, *supra* note 10, at H756.
185. *Id.*
186. *Draft Directive, supra* note 41.
187. *Id.* at 6.
188. *Id.* at 7.
189. *Hearing Record, supra* note 1, at 8.

the U.S. are unfounded. The draft Directive will not require the U.S. to register databases. Consistent with the purpose behind the Privacy Act of 1974,[190] draft Directive principles require that data not be processed without the consent of the individual, except in specific circumstances.[191] Although Member States will be required to provide for database registration, "third countries"[192] like the U.S. will not be held to such rigid standards. Rather, a third country will be required to "ensure an adequate level of protection," demonstrable by "the international commitments it has entered into or . . . its domestic law."[193] Such a domestic law would likely be acceptable if it is consistent with the principle of acquiring the individual's consent to process personal data.

At present, though, the U.S. has no private sector analog to the Privacy Act of 1974. Without a comprehensive private sector privacy law to enforce, or the ability to regulate the private sector, the DPB's ability to "serve the interests of consumers, of government, and of business"[194] will be extremely limited. In addition, the absence of such private sector regulations will not satisfy the reciprocity requirements of the draft EC Directive.

Similarly, courts cannot be expected to enable consumers to protect themselves without legislation defining the unauthorized disclosure of personal data as a privacy invasion. Although Congress has recognized that "[t]he disclosure of . . . personal information can be damaging to the individual,"[195] courts have not reached similar conclusions. The Ohio Court of Appeals, for example, holds

---

190. *See supra* note 173.

191. *Draft Directive, supra* note 41, at 7. Article 8 provides that:

> 1. The Member States shall provide in their law that, without the consent of the data subject, the recording in a file and any other processing of personal data shall be lawful only if it is effected in accordance with this Directive and if:
>
> (a) the processing is carried out under a contract, or in the context of a quasi-contractual relationship of trust, with the data subject and is necessary for its discharge; or
>
> (b) the data come from sources generally accessible to the public and their processing is intended solely for correspondence purposes; or
>
> (c) the controller of the file is pursuing a legitimate interest, on condition that the interest of the data subject does not prevail.

Id.

192. The draft Directive distinguishes between Member States (of which there are twelve in the European Economic Community (EC): Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, and the United Kingdom) and third countries. *See Draft Directive, supra* note 41, at 6, 10.

193. *Id.* at 10.

194. *Hearing Record, supra* note 1, at 3.

195. Privacy Act Legislative History, *supra* note 160, at 6946.

that "[w]hen a magazine publisher sells subscription lists to direct mail advertisers without the consent of the individual subscribers he does not violate the subscribers' rights of privacy."[196]

Furthermore, courts are a forum for compensating perceived damage. The mailing list business, which comprises only one segment of industry which uses personal data, "exists largely without the knowledge of the people who are providing the profit, the people whose names and personal data keep this wheel turning."[197] In addressing individual grievances, courts are not equipped to address industry-wide violations of privacy rights. Whereas a data protection agency, specifically focused on investigating privacy abuses, advising government and private organizations, and enforcing privacy legislation, can protect the individual without her needing to be aware of the virtually invisible violation of her privacy rights.

Industry spokespeople argue that broad legislation protecting personal data is unnecessary because industrial self-regulatory practices are sufficient to protect consumers.[198] This is simply untrue. As described by Richard A. Barton, the Direct Marketing Association's (DMA) Senior Vice President for Government Affairs, the Association's "flagship program" is the Mail Preference Service, which consists of a list of people who have requested that they not receive direct marketing solicitations (aka junk mail).[199] In DMA parlance, the people on this list have executed their "negative option."[200] But even Congress recognizes that "only some people know about this service, and the distribution of information through lists is so widespread that people who do manage to get off lists through such a service, have no way of controlling what all the other companies do."[201] Furthermore, the very focus of the Association, which is to "give the public every opportunity [to] get off mailing lists,"[202] is self-serving. The focus of consumer privacy protection should be that of the Privacy Act of 1974: "information obtained for one purpose may not be used for a different purpose without the individual's consent."[203] Consumers are not merely

196. Shibley v. Time, 341 N.E.2d 337, 338 (Ohio Ct. App. 1975).

197. Privacy Act Legislative History, *supra* note 160, at 6947 (statement of Senator Hatfield).

198. *See Hearing Record*, *supra* note 1, at 44.

199. *Id.*

200. Nicholas di Talamo, *Private Secrets; European Community Proposals for Data Protection*, DIRECT MARKETING MAG., Vol. 53, April 1991, at 42, 43.

201. Privacy Act Legislative History, *supra* note 160, at 6947.

202. *Hearing Record*, *supra* note 1, at 44 (statement of Richard A. Barton, Senior Vice President, Government Affairs, Direct Marketing Association)

203. Video Privacy Protection Act Legislative History, *supra* note 173, at 4342-2.

concerned with removing names from mailing lists, or receiving less junk mail. The concern is that people should be able to control how and where their personal information is used.

It should not be the consumer's responsibility to remove her name from a list, but rather, it should be industry's obligation to ask the consumer's permission to use her name. The consumer should not be required to execute a "negative option" to stop unwanted mailings, or other use of personal data. Rather the business should be required to acquire a "positive option" from the consumer permitting access to and profit from that individual's name, address, consumer habits, and an infinite variety of other collectable personal information.[204] Unless the individual explicitly provided her name and address for inclusion on a mailing list and her consent for its sale, disclosure of her information would constitute a breach of the implicit contract she agreed to when providing the data for its initial purpose.

Another important function that private sector privacy legislation would serve, then, is to codify the kind of principles and policies which need to be observed to protect privacy and ensure that business standards are clear. An example of these principles and policies is the "Code of Fair Information Practice." A report done by the Secretary's Advisory Committee on Automated Personal Data Systems to the U.S. Department of Health, Education and Welfare recommended the enactment of a Federal Code such as this for all automated personal data systems.[205] The Code involves five principles:

1. There must be no personal data record-keeping whose very existence is secret.
2. There must be a way for a person to find out what information about him is in a record and how it is being used.
3. There must be a way for a person to prevent information about himself that was obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for a person to correct or amend a record of identifiable information about himself.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[206]

204. *See* di Talamo, *supra* note 201, at 43.
205. Privacy Act Legislative History, *supra* note 160, at 6923.
206. *Id.* at 6924.

Another industrial self-regulatory practice, one which does seek to integrate the above principles, is termed the "consensual database."[207] As defined by Equifax, "[t]his is a list of people who have expressed consent to be listed and who also offer information that will be used to target them for different categories of mail."[208] Although Equifax's recently instituted consensual program (called Buyer's Market) satisfies privacy concerns that data not be used for purposes other than for which it was provided, it is marketed to consumers as a for-profit service.[209] While Equifax is clearly seeking to comply with pro-privacy legislation and address the consumer hostility evidenced by the protests over its Marketplace venture with Lotus,[210] it "will profit handsomely if it can charge a premium for its mailing list," and benefits further by charging consumers a $15 fee to participate in Buyer's Market.[211]

Thus Equifax is able to charge consumers for their right to privacy due to the lack of legislative consumer protections.[212] Consensual databases appear to satisfy privacy concerns, but they must be compulsory across the private sector and must guarantee the right to privacy principles to protect against damaging business practices.[213]

B. *To Serve Business Interests*

Broad private sector privacy legislation would protect businesses from financial loss and legal liability by providing guidance in developing policies and procedures for handling personal data. The destruction of Equifax's joint production plans (and associated financial loss) for the Marketplace product[214] is only the most recent example of what can happen when companies are not put on notice of the privacy standards to which they must conform.

The Marketplace disaster is instructive because it demonstrates an intensifying climate of hostility toward marketers who violate

---

207. Mark D. Uehling, *Here Comes the Perfect Mailing List*, AM. DEMOGRAPHICS, Aug. 1991, at 10.

208. *Id.*

209. *Id.*

210. Sullum, *supra* note 20, at 29.

211. Uehling, *supra* note 208, at 10.

212. Similarly, Representative Wise notes that it costs more to have an unlisted phone number, thereby causing the consumer to pay for privacy. *Hearing Record*, *supra* note 1, at 161.

213. Congress noted the importance of such "negative options" in statements relative to the Video Privacy Protection Act. *See* 134 CONG. REC. H10411 (daily ed. Oct. 19, 1988) (statement of Mr. Moorehead).

214. Sullum, *supra* note 20, at 29.

consumer privacy. According to a survey sponsored by Equifax, seventy-six percent of the public feel that the sale of information about income, home ownership and credit history to direct-mail companies is "unacceptable."[215] Rising criticism from Congress, state attorneys general and from consumer and privacy advocates has motivated TRW to offer free credit reports as a "salve for consumers' fears."[216] This growing sense of violation by consumers, also recognized by Representative Wise in his remarks introducing the DPB bill,[217] suggests a potential for consumer legal action against companies perceived to be violating privacy rights. Such liability can be protected against if the private sector moves to protect consumer data from unauthorized disclosure. Legislation which compels such protection would thereby also protect businesses from liability.

Another cost-saving, and liability-avoiding benefit of establishing standard privacy protections is to ensure that businesses can invest with the security and knowledge that they are complying with legal requirements. A broad privacy law would release the private sector from carrying the cost of conforming to patch-work legislation and varying judicial standards of privacy. In the absence of such a standard, technologies appear to be changing the traditional legal definitions of trespass, property, and privacy faster than the government's ability to keep pace. When basic definitional ground rules shift, this threatens the stability on which sound business decisions are based.

The current rapid evolution of technology makes it inevitable that new threats to privacy will continue to arise. Therefore, a broad standard of privacy protection is essential to ensure individual rights, as well as those of business. Justice Brennan noted that:

> [the] [d]evelopment of . . . computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpreta-

215. Uehling, *supra* note 208, at 12.

216. Peter Kerr, *Big Credit Bureau to Let Consumers see Reports Free*, N.Y. TIMES, Oct. 15, 1991, A1. The article notes that "critics have charged that [TRW, the Trans Union Corporation and Equifax Inc.] maintain credit histories riddled with mistakes, sell private data to companies that send out 'junk mail' and make it easy for practically anyone to pull up confidential reports." *Id.*

217. Rep. Wise's Introductory Remarks, *supra* note 10, at H755. ("Americans are greatly concerned about threats to their personal privacy resulting from the increased use of computers to collect, maintain, and manipulate personal information. Seven of ten Americans agree that consumers have lost control over how personal information about them is circulated and used by companies.")

> tions of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[218]

Similarly, legislative clarification of the privacy parameters to which businesses must adhere will not only protect the consumer, but also the businesses which will be on notice of the rights which government will protect.

Marketing industry lobbyists are predictably opposed to the idea of personal data protection. Critics of the European Commission's proposed Data Protection Directives claim that if imposed, the legislation could "leave Europe's electronic sales and marketing machines crippled by legislative arthritis."[219]

But data protection needn't mean governmental registration.[220] It is, however, undeniable that data protection would require businesses to make significant modifications in their information-handling practices.[221] The costs for such modifications are difficult to determine. Although Equifax will spend $10 million to create a consensual database including roughly a quarter of the 80 million people in its files,[222] costs can also be saved when direct marketers target their efforts (via consensual databases, for example) directly to receptive consumers. By polling their listees regularly, marketers can purge uninterested people from their computers, and save mail production and postage costs.[223]

Therein is the rationale for enforcement by the DPB of private sector privacy legislation. The degree of behavior change required to be made by businesses to protect individual liberties and personal privacy is not likely unless compelled by legislation and administrative oversight. Despite the arguments of industry spokespeople like Citicorp's Jerry Saltzgaber that it is in marketers' self-interest to protect consumer privacy,[224] companies have an obligation to stockholders to make money. Protecting privacy is expensive and that cost deters innovation.

C. *To Serve the United States' Interests*

U.S. businesses will benefit from U.S. privacy legislation which

---

218. U.S. v. Miller, 425 U.S. 435, 451-452 (1976) (Brennan, J., dissenting).

219. Louella Miles, *Feeling the Draft; European Community's Data Protection Directive Data Protection*, MARKETING, May 30, 1991, at 16.

220. *See supra* notes 193-94 and accompanying text.

221. *See Hearing Record, supra* note 1, at 35 (testimony of Professor David H. Flaherty).

222. Uehling, *supra* note 208, at 10.

223. *Id.*

224. *Hearing Record, supra* note 1, at 88.

ensures freedom to do business after 1992 throughout the single European market. The reciprocal legislation requirements of the EC's proposed Directive will effectively lock U.S. industries out of business opportunities if adequate U.S. legislation is not in place. Particularly in dealing with international concerns, a data protection board ought to have jurisdiction over private sector information practices. Private companies transfer an enormous amount of personal data across international borders every day.[225] The U.S. economy can ill afford to have that pipeline constricted.

Such U.S. data protection legislation, enacted in tandem with a provision for a privacy enforcement body, will also protect the interests of U.S. businesses by providing for representation in international forums where the international impact of privacy issues are discussed. Although large U.S. corporations can represent their own interests abroad, the concerns of smaller companies and individuals are currently not expressed in international privacy forums. While other countries have set up independent government agencies to represent domestic privacy,[226] the U.S. has no such governmental body. The DPB would serve the purpose of fostering all U.S. privacy interests, including those of all businesses, all citizens and the U.S. Government.[227]

IV. PROPOSED LEGISLATION

The European Commission's proposed Directive[228] provides, *inter alia*, comprehensive provisions for private sector protection of personal data. The following proposed legislative text is a modification of pertinent sections of the Directive. Adoption of legislation modeled on the Directive's principles would not only protect personal and business interests, but would also satisfy the Directive's Article 24 requirement for "adequate" reciprocal legislation.

A. *SHORT TITLE*

This Act may be cited as the "Private Sector Privacy Act" (hereinafter the "Act").

---

225. Taking data relating to air travel as an example, some 27,000 messages are involved in the passenger reservation process for a single 747 flight. Similarly, American Express processes authorizations of a quarter million credit card transactions and for over $10 billion in banking transactions daily. Christopher Millard, *Data Protection and Privacy Considerations in Transnational Distribution: A European Perspective*, THE COMPUTER LAW ASS'N BULL., Vol. 6, No. 1, 1991, at 17 n.1.

226. *See Hearing Record*, *supra* note 1, at 2.

227. *Hearing Record*, *supra* note 1, at 76.

228. *Draft Directive*, *supra* note 41.

B. *DEFINITIONS*

For the purposes of this Act:

1. "Individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;
2. "Personal Data" means any information relating to an identified or identifiable individual;
3. "Data Subject" means the individual(s) described by or relating to personal data;
4. "Personal Data File" (file) means any set of personal data, whether centralized or geographically dispersed, undergoing automated processing or which, although not undergoing processing, are structured and accessible in an organized collection according to specific criteria in such a way as to facilitate their use or combination;
5. "Processing" means the following operations, whether or not performed by automated means: the recording, storage, collection or combination of data, and its alteration, use or communication, including transmission, dissemination, retrieval, blocking and erasure;
6. "Private Sector Personal Data Processor" (PDP) means any natural or legal person or association, including non-profit and for-profit companies, corporations, organizations and entities in so far as they carry on an industrial, commercial, social, civic, political, philosophical, religious, cultural, trade union, sporting or leisure activity who engages in processing of personal data;
7. "Data Protection Board" (DPB) means the independent public authority proposed in HR 685 and further empowered as follows:
   a. The DPB shall monitor the application of the national measures taken pursuant to this Act and perform all the functions that are entrusted to it by this Act.
   b. The DPB shall have investigative powers and effective powers of intervention against the creation and exploitation of files which do not conform with this Act. To that end, it shall have, *inter alia* the power to gather all the information necessary for the performance of its supervisory duties.
   c. Complaints in connection with the protection of individuals in relation to personal data may be lodged with the DPB by any individual.

C. *NON-DISCLOSURE PRINCIPLES*

1. Without the consent of the data subject, the recording in a file and any other private sector processing of personal data

shall be lawful only if it is effected in accordance with this Act and if:

a. the processing is carried out under a contract, or in the context of a quasi-contractual relationship of trust, with the data subject and is necessary for its discharge; or
b. the data comes from sources generally accessible to the public and their processing is intended solely for correspondence purposes.

2. No PDP shall disclose any personal information which is contained in a file by any means of communication to any person, or private or public entity, except pursuant to a written request by, or with the prior written consent of the data subject, unless disclosure of the file would be required for reasons relating to:
   a. national security; or
   b. public safety.

D. *INFORMED CONSENT*

1. Any giving of consent by a data subject to the processing of personal data relating to that data subject within the meaning of this Act shall be valid only if:
   a. the data subject is supplied with the following information:
      i. the purposes of the file and the types of data stored;
      ii. the type of use and the recipients of the personal data contained in the file; and
      iii. the name and address of the PDP;
   b. it is specific and express and specifies the types of data, forms of processing and potential recipients covered by it; and
   c. it may be withdrawn by the data subject at any time without retroactive effect.

E. *RIGHTS OF DATA SUBJECTS*

1. Data subjects shall be granted the following rights:
   a. To oppose, and, for legitimate reasons, cause the cessation of the processing of personal data relating to the data subjects.
   b. To know of the existence of a file and to know its purposes and the identity and place of business of all PDP's with access to that file.
   c. To obtain at reasonable intervals, and without excessive delay or expense, confirmation of whether personal data relating to data subjects are stored in a file, and communication to him of such data in an intelligible form.
   d. To obtain correction, or erasure, of such data, or blocking of access to particular PDPs of such data.

e. To bring a civil action against the PDP if the rights guaranteed in this Act are infringed. Any individual whose personal data has been stored in a file and who suffers damage as a result of processing or of any act incompatible with this Act shall be entitled to compensation from the PDP.

F. *RESPONSIBILITIES OF PDP's*

1. Every PDP must assure the reliability of the personal data held in its files by periodic disclosure to and approval of the data by the data subjects.
2. Every PDP shall take appropriate technical and organizational measures to protect personal data stored in a file or communicated in any way against accidental or unauthorized or unconsented to destruction, or accidental loss and against unauthorized access, modification or other processing.

V. CONCLUSION

In certain hands, personal information can prevent an individual from securing employment or health insurance or from protecting herself from a murderer. Perhaps the greatest danger we face by failing to protect informational privacy is the unreversable weakening of that privacy. By the time the majority recognizes how far technology and commercial interests have intruded on the individual, it may be too late to reclaim her privacy. To prevent such a threat, there is only one viable choice for government to make. Congress must regulate the behavior of data collectors, and thereby prevent discrimination against the subjects of personal data files.

The alternate, dangerous choices for dealing with the personal data issue are either to maintain the status quo, that is to allow those with the resources to collect and store data to profit from and intrude on the privacy of people, or to ban the collection of potentially threatening data altogether. This article has sought to illuminate why regulation of private sector use of personal data is essential to protect against damage to people, and the national economy.