1992

Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?

Joel R. Reidenberg
Fordham University School of Law, jreidenberg@law.fordham.edu

Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?

Joel R. Reidenberg*

CONTENTS

* Associate Professor of Law, Fordham University School of Law. A.B. Dartmouth 1983; J.D. Columbia 1986; D.E.A. dr. int'l eco. Universite de Paris I (Pantheon-Sorbonne) 1987. I would like to thank Stewart Dresner and the participants in the *Privacy Laws & Business* 4th Annual Data Protection Conference at Cambridge University for the opportunity to present and discuss earlier sections of this article. I am also particularly grateful to Jeffrey P. Cunard, Carl Felsenfeld, Michael M. Martin, Michael P. Malloy, Russell G. Pearce and Steve Thel for their helpful comments on prior drafts. A Fordham University Faculty Research Grant Award supported work on this Article and Jeffrey Ash, Peter Batacan, Lawrence Schneider and Rori Wender ably provided research assistance.

INTRODUCTION

More than twenty years ago, American legal scholars first considered the impact of computerization on privacy.[1] Several years later, the United States Privacy Protection Study Commission, under a congressional mandate, made an extensive study of privacy rights in the emerging information society.[2] The Commission focused on eight sets of record-keeping relationships[3] and found that privacy was not protected satisfactorily from

1. *See* Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969).

2. *See* U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PRIVACY COMM'N].

3. The Commission addressed: (1) the consumer-credit relationship; (2) the depositary relationship; (3) mailing lists; (4) the insurance relationship; (5) the employment relationship; (6) record-keeping in the medical care relationship; (7) investigative reporting agencies; and (8) record-keeping in the education relationship. PRIVACY COMM'N, *supra* note 2, at xiii.

either government or industry intrusions.[4] In the fourteen years following the Commission's study, the actual emergence of an information economy has generated little scholarly analysis of the overall legal framework in the United States for privacy and information processing activities by the business community.[5]

During the 1980s, the dramatic advances in telecommunications and information technology changed the relationship between individuals and corporations with respect to the circulation of personal information.[6] Information technology and networking significantly enhanced the extent of available personal information and eliminated inefficient record-keeping practices that once kept personal information from public scrutiny.[7] The proliferation of computers in the last decade has encouraged extensive gathering and dissemination of personal information through sophisticated data collection techniques,[8]

---

4. *See* PRIVACY COMM'N, *supra* note 2, at 1-35.

5. Many insightful studies have analyzed rights of privacy and state action in connection with computer-processed personal information. *See, e.g.*, DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA AND THE UNITED STATES (1989). General surveys of privacy rights in the context of computers have been written. *See, e.g.*, WARREN FREEDMAN, THE RIGHT OF PRIVACY IN THE COMPUTER AGE (1987); RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY ¶¶ 12.09-12.13 (1985). *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987) (focusing generally on privacy rights without delineating clearly between the public and private sectors). Recent articles address discrete privacy issues. *See, e.g.*, Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255 (1984) (health information); Robert Kastenmaier et. al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715 (1989) (telecommunications issues); Ben A. Rich, *The Assault on Privacy in Healthcare Decision Making*, 68 DENV. U.L. REV. 1 (1991) (health information); Glen Chatmas Smith, *We've Got Your Number! (Is It Constitutional to Give It Out?) Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145 (1989) (telecommunications and caller identification). Several student notes have addressed particular aspects of private sector rights. *See* Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987) [hereinafter *Graham*]; John A. McLaughlin, Note, *Intrusion upon Informational Seclusion in the Computer Age*, 17 J. MARSHALL L. REV. 831 (1984).

6. Personal information refers to information about identified or identifiable individuals.

7. *See* Oscar H. Gandy, *The Surveillance Society: Information Technology and Bureaucratic Social Control*, 39 J. COMM. 61, 62-63 (1989).

8. *See, e.g.*, David Churbuck, *Computers' New Frontier*, FORBES, Nov. 26, 1990, at 257, 260 (describing how Northwest Airlines collects ticket receipts and stores them on laser disks for future image processing).

corporate outsourcing of data processing,[9] and the establishment of information service providers and clearinghouses.[10] Interconnected computing systems and expanding information processing capabilities have led to rapidly diminished responsibility and accountability for the treatment of personal information; fewer and fewer direct contacts exist between individuals and those holding personal information.[11] Vast quantities of personal information containing greater detail than ever before about an individual's financial status, health status, activities and personal associations are now readily available through commercial information services and list brokers.[12]

These new capabilities and the increased circulation of personal information in the private sector raise significant privacy issues. A 1990 poll taken in the United States by Equifax, one of the major national credit reporting agencies, found that seventy-nine percent of Americans are concerned about privacy and the use of personal information.[13] Americans believe that they have

---

9. *See* Allen R. Grogan & Ron Ben-Yehuda, *Outsourcing Data Processing Operations*, 8 COMPUTER LAW. 1 (Dec. 1991) (assessing risks and benefits of outsourcing arrangements); George Brandon & John K. Halvey, *The Outsourcing Decision: Avoiding Pitfalls*, AM. BANKER, Jan. 15, 1992, at 4, 4-5 (describing corporate outsourcing arrangement).

10. *See* Norman Jonas, *The Hollow Corporation*, BUS. WK., Mar. 3, 1986, at 56, 56-71 (describing new corporate networking strategies); John Markoff, *Business Technology: For Shakespeare, Just Log On*, N.Y. TIMES, July 3, 1991, at D1 (describing new data exchange networks).

11. *See, e.g.*, Gandy, *supra* note 7, at 63-64; John W. Verity, *Rethinking the Computer*, BUS. WK., Nov. 26, 1990, at 116, 116-24 (describing the developments in corporate computer networks).

12. *See infra* notes 29-35. Over the last decade, the ability of the private sector to accumulate, use and sell personal information has increased dramatically. The name-trading business is now estimated to be a $3 billion industry. *See* Jill Smolowe, *Read This!!!!!!*, TIME, Nov. 26, 1990, at 62, 66. Today, from home or office, a laptop computer can be connected to telecommunications networks that provide instant access to databases containing substantial quantities of personal information. Information service networks such as Dialog, Prodigy or CompuServe provide access to tremendous database resources that can include information ranging from resumes of job hunters to bill collection address lists. *See* Claudia H. Deutsch, *Headhunting from a Data Base*, N.Y. TIMES, May 6, 1990, at C25; William M. Bilkely, *Bill Collectors Master Automated Arm-Twisting*, WALL ST. J., Sept. 10, 1990, at B1; Jeffrey Rothfeder, *Is Nothing Private?*, BUS. WK., Sept. 4, 1989, at 74, 74-82.

13. LOUIS HARRIS ASSOCS. & ALAN F. WESTIN, EQUIFAX, INC., THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE, at V (1990) [hereinafter EQUIFAX REPORT]. In addition, several highly publicized incidents during the last year have brought greater attention to privacy issues. These incidents include the abandoned release of a Lotus/Equifax consumer profile database on CD-ROM, the

lost control over personal information.[14] Not surprisingly, privacy and information processing have also generated substantial interest abroad. In many European countries including Austria, France, Germany, Ireland, Luxembourg and the United Kingdom, broad statutes provide a general set of privacy rights applicable to the private sector.[15] Recently, a number of foreign governments have even prohibited the transmission of personal information to countries perceived as ignoring computer privacy concerns.[16]

The thesis of this Article is that the American legal system responds incoherently and incompletely to the privacy issues raised by existing information processing activities in the business community.[17] Part I examines key privacy concerns and the federal and state framework for the legal protection of individual rights. Part II demonstrates that the rights available at the federal level address limited privacy concerns and then in

---

monitoring of electronic mail on the Prodigy information service, regional telephone company proposals to offer caller identification features, and electronic surveillance of employee activities.

14. Seventy-one percent of Americans believe they have lost control over the use and dissemination of personal information and seventy-nine percent believe that privacy is a fundamental right. EQUIFAX REPORT, *supra* note 13, at 7, 11.

15. *See* ADRIANA C.M. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC (1990); A.C. Evans, *European Data Protection Laws*, 29 AM. J. COMP. L. 578 (1981); *Data Protection Roundup*, PRIVACY L. & BUS., July 1991, at 2-7. A recent draft directive on data protection issued on September 13, 1990 by the Commission of the European Communities has also increased attention to privacy protection. *See* Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C277), Com(90)314 Final SYN 287 (Sept. 13, 1990) [hereinafter Draft EC Directive].

16. Because of privacy concerns, Norway, Austria, Germany, and Sweden have each imposed restrictions on international data flows. Commission nationale de l'informatique et des libertés, 10e Rapport au Président de la République et au Parlement, Annexe 9, at 308-09 (1989). France has restricted the transfer of personal information to Italy on privacy grounds. *Id.* at 32-34 (*reprinting* Deliberation No. 89-78 du 11 juillet 1989 relative à la transmission d'informations relatives aux cadres superieurs de la Société Fiat France à la Société Fiat à Turin). France has also prohibited data exports to Belgium, Switzerland and the United States. Interview with Ariane Mole, Attachée Relations Internationales, Direction Juridique, Commission nationale de l'informatique et des libertés, in Paris, France (June 6, 1991). The United Kingdom has also blocked a data transfer to the United States. See SEVENTH REPORT OF THE DATA PROTECTION REGISTRAR, at 33-34 (1991); *First UK Ban on Data Exports is to Named Companies in the USA*, PRIVACY L. & BUS., at 5 (Winter, 1990/91).

17. This article will not address any issues raised by government information processing or government attempts to gain access to information about individuals held in the private sector.

only a few situations. Part III shows that at the state level neither the available common law rights nor the statutory protections apply to the full scope of relevant privacy concerns. Part IV offers suggestions based on comparisons with European legislation for the development of a new legal framework to coherently and completely satisfy privacy concerns for information processing by the business community.

I. THE WILDERNESS—PRIVACY CONCERNS IN THE INFORMATION ECONOMY AND THE FRAMEWORK FOR LEGAL PROTECTION OF INDIVIDUALS

Over a century ago, Samuel Warren and Louis Brandeis, in one of the most influential legal articles in American history, referred to privacy in the United States as the "right to be let alone."[18] This view reflected, in part, the tradition of individualism in the United States and Warren's wrath at journalistic practices in Boston at the time.[19] Almost one hundred years later, privacy principles applicable to computer processing of personal information were widely recognized around the world as a necessity for an information-based economy.[20] Two important

18. *See* Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 205 (1890). Others have cast the philosophical basis for privacy somewhat differently. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (arguing that the privacy right consists of the complete control by an individual to determine the disclosure of personal information to others); Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964) (reasoning that privacy concerns fundamental human dignity); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968) (taking the position that privacy consists of the right of individuals to define themselves for others); Miller, *supra* note 1, at 1107-08 (arguing that privacy entails the control of the flow of information about individuals); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978) (arguing that privacy has an economic basis).

19. The impetus for this famous article was thought to be Warren's fury at tabloid press reports of his daughter's wedding. William Prosser, *The Right of Privacy*, 48 CAL. L. REV. 383 (1960). *See also* SAMUEL HOFSTADTER & GEORGE HOROWITZ, THE RIGHT OF PRIVACY 17 (1964). Other scholars have speculated that Warren was angered by gossip column reports of his family's social life. *See* Diane Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren's and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 295-96 (1983).

20. *See* Organization for Economic Cooperation & Development, Recommendations of Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1981 I.L.M. 422, O.E.C.D. Doc. No. C(80)58 final [hereinafter OECD Guidelines]; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981 I.L.M. 377, Euro. T.S. No. 108 (Jan. 28, 1981) [hereinafter European Convention].

international organizations, the Organization for Economic Cooperation and Development (O.E.C.D.) and the Council of Europe, each established principles for information processing in the private sector.[21] These principles address the full range of data processing activities—namely, the acquisition, use, storage, transmission and dissemination of personal information.[22] Many foreign countries have adopted legislation comprehensively regulating information processing.[23] In the United States, however, no single source of privacy rights covers each data processing activity. Information privacy rights emerge from a complex web of federal and state laws that have responded to narrowly identified problems, while industry practices afford some additional non-legal protection.

A. Privacy Concerns

In the context of data processing activities by the business community, the term "privacy" encompasses concerns about fair and reasonable information practices as well as confidentiality.[24] A range of obvious and subtle issues arise from each data processing activity.

---

21. *Id.* The OECD Guidelines, *supra* note 20, seek voluntary compliance, while the European Convention, *supra* note 20, has the force of an international treaty.

22. *See* OECD Guidelines, *supra* note 20, art. 7-14; European Convention, *supra* note 20, art. 5-11.

23. *See supra* note 15. These statutes generally follow the Council of Europe convention on data processing. *See* European Convention, *supra* note 20. The European Convention sets forth standards for the protection of personal information that must be enacted into national law by signatory countries. The European Convention addresses data collection and requires that personal information be "obtained and processed fairly and lawfully." *Id.* art. 5a. Personal information may only be stored for specified and legitimate purposes. *Id.* art. 5b. Stored information may not be used for purposes incompatible with those relating to the data collection. *Id.* art. 5b. Personal information that is not needed to serve the purpose of collection may not be gathered or stored. *Id.* art. 5c. Personal information may not be stored longer than is necessary to accomplish the purpose of collection. *Id.* art. 5e. Personal information must be accurate and current. *Id.* art. 5d. Individuals must be able to determine the existence of and gain access to any database containing their personal information. *Id.* art. 8a-b. Individuals also must have a right to correct erroneous personal information and must have a right to erase personal information that by its processing would contravene any of the basic principles. *Id.* art. 8c. The European Convention further prohibits the processing of information revealing racial origin, political opinions, religious or other beliefs, as well as information concerning health, sexual life, or criminal convictions unless special domestic law safeguards are adopted. *Id.* art. 6.

24. *See* PRIVACY COMM'N, *supra* note 2, at 14-21, 501 (elaborating on fair information practices).

Privacy often conjures up fears of "Peeping Toms," computer hackers, and unauthorized disclosures of personal information to third parties.[25] Yet, in the case of data processing, there are obvious concerns about the information-acquisition itself. As with the fear of Peeping Toms, individuals desire notice of the collection of personal information by others and the opportunity to consent to the acquisition of such information.[26] Many organizations gather personal information in rather visible ways with the consent of individuals.[27] However, many individuals are unaware of the myriad of organizations that collect personal information for commercial purposes. These unknown groups and surreptitiously gathered collections of personal information are troubling.[28] Directories exist listing thousands of rental mailing lists available from different companies.[29] Largely unbeknown to the general public, information service companies, for example, collect and disseminate information regarding personal health,[30] insurance claims,[31] and driving records.[32] Computer reservation systems process and retain information re-

25. *See* Miller, *supra* note 1, at 1109-14.

26. *See, e.g.*, OECD Guidelines, *supra* note 20, art. 7; European Convention, *supra* note 20, arts. 5a, 8a; *Public and Corporate Reactions to Privacy: Hearings on Domestic and International Data Protection Issues Before the Subcomm. on Gov't Info., Justice and Agric. of the House Gov't Operations Comm.*, 102nd Cong., 1st Sess. 5 (1991) [hereinafter *Hearings I*] (statement of Professor David Linowes).

27. Credit card holders, for example, know that card issuers necessarily maintain records identifying both the purchases that are made and the particular selling merchant. The Fair Credit Billing Act requires card issuers to provide cardholders with a statement of account. 15 U.S.C. § 1666(a) (1988). *See also* Agreement Between Cardmember and American Express Travel Related Services Co., CD 22024 (Revised Nov. 1989) (obligating cardholders to pay amount stated on monthly statement); American Express Cardholder Summary of Account (showing details of monthly transactions). Telephone users see that telecommunications companies process data identifying the time, place of origin, destination, number called, duration and amount charged for each call. *See, e.g.*, Standard MCI Telecommunications Customer Account Invoice. Credit applications routinely ask for detailed information regarding the applicant's financial history and employment status and request the applicant to authorize an investigation and the release of credit reports. *See* 15 U.S.C. § 1681b(3).

28. *See* Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 GOV'T INFO. Q. 79, 83-84 (1991).

29. Smolowe, *supra* note 12, at 66 (referring to STANDARD RATE & DATA SERVICE, DIRECT MAIL LIST RATES AND DATA, which contains descriptions of over 10,000 commercially available lists).

30. *See Data Protection, Computers, and Changing Information Practices: Hearings Before the Subcomm. of Gov't Information, Justice and Agric. of the House Comm. on Gov't Operations*, 101st Cong., 2nd Sess. 11 (1990) [hereinafter *Hearings II*] (statement of Marc Rotenberg et al., of the Computer Professionals for Social Responsibil-

lating to individual's travel plans, ticket charges (including credit card information), telephone numbers, hotel reservations, and rental car arrangements.[33] Supermarkets in various parts of the country have, through frequent shopper programs, enabled one of the country's largest financial institutions to keep detailed records of individual customer's buying patterns for sale to product manufacturers.[34] Other information service providers make databases available that identify all the alumni of various universities.[35]

While the unknown collection of personal information may be troubling, the unnecessary or excessive acquisition of personal information from individuals is also a privacy concern.[36] Ninety percent of Americans think the collection of excessive personal information is a problem.[37] Often, information may be gathered "because it's there." If an individual has no understanding of the extraneous character of personal information or no opportunity to refuse to disclose such information, personal information may be collected and disseminated when an informed individual

---

ity); Anne McGrath, *The Executive Goldfish Bowl*, FORBES, Feb. 11, 1985, at 154; Gerald Odening, *Protecting Medical Records*, FORBES, Dec. 8, 1980, at 165.

31. For example, two southern companies, Employee Information Services in Louisiana and Industrial Foundation of America in Texas, maintain computer databases of employee personal injury claims. *Hearings II*, *supra* note 30, at 6 (statement of David Czernick, Exec. Dir., Louisiana Consumers League). *See also* David Tuller, *Trying to Avoid an Insurance Debacle*, N.Y. TIMES, Feb. 22, 1987, at C1. The Medical Information Bureau (MIB, Inc.) in Massachusetts even compiles records on life insurance applications and applicants. *See* MIB, INC., A CONSUMER'S GUIDE TO THE MEDICAL INFORMATION BUREAU (1991).

32. Jeffrey Rothfeder, *Looking For A Job? You May Be Out Before You Go In*, BUS. WK., Sept. 24, 1990, at 128.

33. Howard Gold, *Sabre Dancing*, FORBES, Dec. 30, 1985, at 88. The Sabre airline reservation system also includes the entry of home and travel telephone contacts. Travel agencies, airlines, and rental car companies are even fighting over the ownership of this compiled information. *Hearings II*, *supra* note 30, at 2 (statement of Rep. Bob Wise).

34. *Hearings II*, *supra* note 30, at 94-95 (statement of Jerry Saltzgaber, C.E.O., Citicorp Point of Sale Information Services); Lena H. Sun, *Checking Out the Customer's Habits*, WASH. POST, July 9, 1989, at H1.

35. For example, University Pronet is an electronic database located at Stanford University that contains lists of graduates from several universities. *See* Claudia H. Deutsch, *Headhunting from a Data Base*, N.Y. TIMES, May 6, 1990, at C25.

36. *See, e.g.*, OECD Guidelines, *supra* note 20, art. 8; European Convention, *supra* note 20, art. 5c.

37. EQUIFAX REPORT, *supra* note 13, at 18. Fifty-seven percent of Americans believe consumers are asked to reveal excessive amounts of personal information. *Id.*

might have refused to make such disclosures.[38] Not surprisingly, executives in industries that amass personal information are particularly sensitive to this concern in their own lives and decline to provide unnecessary personal information in many situations.[39]

Another important concern arising from the collection of personal information is accuracy.[40] Errors may arise from inaccurate collection or recording techniques. Similarly, misleading information may arise from incomplete collections of personal information. Individuals will, therefore, desire access to personal information and the right to have errors or misleading information corrected.[41]

A more subtle concern relates to the uses or collection purposes of gathered personal information.[42] Information disclosed

38. For example, MCI offers a discount to its subscribers for frequently called numbers. To obtain this discount, a subscriber must provide MCI with the name of the person being called and the family relationship. While such personal information is irrelevant for the purposes of the volume discount, MCI does not inform subscribers of the uses that will be made of this information. *See* Letter from MCI, Inc. to the author (Mar. 25, 1991) (in which MCI misleadingly implies that the name of the person called is needed to determine if the individual is an MCI subscriber and makes no mention of the reasons for collecting information about family relationships). Similarly, as part of the bicentennial celebration of the U.S. Constitution, Philip Morris offered to send a free copy of the Bill of Rights to anyone who called a toll-free number. Phillip Morris requested callers to identify their telephone numbers so that the company could search other databases for demographic and lifestyle information about the callers. The telephone number was wholly irrelevant for the purpose of mailing a document. *See* Mary J. Culnan, *Bill of Rights? Or Bill of Goods?*, N.Y. TIMES, Jan. 21, 1990, at E21.

39. *See* EQUIFAX REPORT, *supra* note 13, at 16 (noting that, compared to the general public, a significantly greater percentage of information industry leaders refuse to reveal personal information on various application forms).

40. *See, e.g.*, OECD Guidelines, *supra* note 20, art. 8; European Convention, *supra* note 20, art. 5d; Miller, *supra* note 1, at 1114-19.

41. *See, e.g.*, OECD Guidelines, *supra* note 20, art. 12-13; European Convention, *supra* note 20, art. 8c.

42. *See, e.g.*, OECD Guidelines, *supra* note 20, art. 9-10; European Convention, *supra* note 20, art. 5b. Advances in merge and sort computer software programming coupled with more accessible computing systems make it possible to compile, from previously incompatible sources, astoundingly detailed profiles of individuals, their lives and lifestyles. For example, a software product, MarketPulse, enables businesses to manipulate lists on an IBM mainframe. Random House is testing a database that enables it to send specialized mail order catalogs to customers with specific reading preferences. Other publishers are able to tailor "demographic editions" of books to fit customer interests. David Churbuck, *Smart Mail*, FORBES, Jan. 22, 1990, at 107. TRW, a credit reporting service, has developed a database, Financial Lifestyle Database, and will sell to anyone the name, address, and phone number of individuals

or collected for one purpose may easily have an associated use in an entirely different and undesirable context.[43] Without knowledge of these associated uses or consent to them, individuals may be outraged to discover how much of their lives are exposed to others.[44] It is probably not commonly known that credit card companies develop lifestyle profiles of card holders, that telecommunications companies track users' calling patterns,[45] that product manufacturers track the habits of individual customers,[46] and that credit reporting agencies also assemble data on household composition (such as marital status of occupants) and on legal disputes involving individuals.[47] Point of sale technology with bar code systems for pricing and inventory manage-

---

grouped by income level, credit cardholdings and credit lines. Rothfeder, *supra* note 12, at 81.

43. The debate over telephone caller identification services illustrates this problem. The caller identification service represents a situation in which a telephone number used in connection with call routing is made to function for another purpose, namely identifying the caller to the recipient and matching callers to other personal information. *See* Smith, *supra* note 5, at 150; PRIVACY AND TECHNOLOGY TASK FORCE, FINAL REPORT OF THE PRIVACY AND TECHNOLOGY TASK FORCE SUBMITTED TO SENATOR PATRICK LEAHY 14 (May 28, 1991). The technology offers the possibility for a caller to block the disclosure of the phone number. The real issue in the debate should be the allocation of the costs for each component of the service. *See also* PRIVACY COMM'N, *supra* note 2, at 20-21 (arguing that individuals must have legally enforceable rights of confidentiality to prevent information gathered for one purpose from being disclosed for another unrelated use); Rotenberg, *supra* note 28, at 81 (arguing that associated uses of personal information breach an implied promise).

44. For example, Lotus, the software developer, and Equifax, the credit reporting agency, recently compiled a database on a CD-ROM storage disk, "Marketplace: Households." The database contained information on 120 million U.S. residents. The information included name, address, marital status, income level, and shopping preferences and was to be sold throughout the U.S. last year. John R. Wilke, *Lotus Product Spurs Fears about Privacy*, WALL ST. J., Nov. 13, 1990, at B1, B5. The product was withheld from the market because of objections from consumer groups. Lawrence M. Fisher, *New Data Base Ended by Lotus and Equifax*, N.Y. TIMES, Jan. 24, 1991, at D4. *See also* EQUIFAX REPORT, *supra* note 13, at 69 (noting that 86% of Americans are concerned about the sale of lists containing information regarding personal characteristics).

45. *See* Rothfeder, *supra* note 12, at 76 (citing examples that shows telemarketing companies have access to information about the places that individuals call); Eben Shapiro, *MCI Discounts Expected on Numbers Called Often*, N.Y. TIMES, Mar. 18, 1991, at D4 (MCI billing system will enable MCI to offer discounts to residential customers for a high number of calls to specific telephone numbers).

46. *See* Churbuck, *supra* note 42, at 107 (noting that Kraft General Foods keeps names and addresses of people who redeem newspaper coupons and call toll-free marketing numbers).

47. Rothfeder, *supra* note 12, at 80.

ment and coded check authorization cards also enable supermarkets to monitor customer purchases and match purchases of any intimate item with individual customers.[48] Even less public attention has been paid to the particularly troubling associated uses of personal information that can result from combinations of data from various existing sources. For example, the recently announced billing arrangements between credit card companies and telecommunications carriers now enable the centralization of substantial amounts of potentially sensitive data that could be sorted to identify and track the associations, personal preferences, travels, activities and, in some instances, even the political beliefs of individuals.[49] If individuals knew that such activities would or could take place, they might not disclose some personal information or enter into various transactions.[50]

Finally, the duration of storage of personal information raises additional concerns.[51] Information may be stored beyond the lifecycle of the purpose for which it was collected. Retention beyond such a time suggests that other uses of the personal information are contemplated. In addition, as the personal information ages, it may become obsolete or inaccurate.

The industry traditionally views these privacy issues as not being problematic until specific abuses occur.[52] The business community desires minimal restraints on the flow of personal

48. *See* Sun, *supra* note 34 at H4 (describing how Vons and Citicorp began a pilot test of this kind).

49. AT&T is now a successful issuer of Visa and MasterCard brand credit cards, and American Express offers billing services for telephone calls placed through MCI. Keith Bradsher, *AT&T Strained by a Success*, N.Y. TIMES, Dec. 3, 1990, at D1. The centralized transaction records from these services may reveal tremendously detailed profiles of an individual's life, from the book titles purchased on the credit card reflecting, for example, the individual's political preferences to the people with whom the cardholder associates by telephone.

50. *See Hearings I*, *supra* note 26, at 8 (statement of John Baker, Senior Vice President, Equifax, Inc.); EQUIFAX REPORT, *supra* note 13, at 14-15 (1990) (indicating that a significant percentage of polled individuals revealed that they have not applied for jobs, credit or insurance because they did not want to provide certain personal information).

51. *See, e.g.*, OECD Guidelines, *supra* note 20, art. 8; European Convention, *supra* note 20, art. 5e.

52. *See Hearings I*, *supra* note 26, at 15 (statement of John Baker, Senior Vice President, Equifax); PRIVACY COMM'N, *supra* note 2, at 34 (noting that industry preferred acceptance of voluntary codes rather than mandatory rules).

information to enhance the development of new technological offerings.[53] While business recognizes that privacy must be protected,[54] most companies in information-intensive industries do not have any mechanism to address privacy problems.[55] There is also a disparity between the industry views of privacy issues and those of the general public. For example, direct marketing executives believe that it is proper to screen lists of individuals for income level and credit histories without advance permission from consumers, yet the vast majority of Americans finds the practice unacceptable.[56] Many in industry prefer a wait and see approach to new privacy policies,[57] though advocacy groups think the issues need to be raised presently.[58] The disparity between the industry views and the views of most individuals reflects the inchoate sense that privacy harms can occur incrementally by the increased processing of personal information without established fair information practices and does not require a series of singularly offensive abuses to warrant consideration and review of legal protection. In fact, Americans today are more distrustful of industry than government with respect to the collection and use of personal information.[59]

Because the privacy concerns cover a broad range of issues addressing notice and consent for the collection of information, the unnecessary collection of personal information, data accuracy and access, associated uses of personal information and the duration of storage, an invasion of privacy may occur in the context of any one of the data processing activities. The importance

53. The industry notes that consumers want the benefits of the use of their personal information. *See* EQUIFAX REPORT, *supra* note 13, at 26. *See also* Peter W. Herman & John K. Halvey, *International Flow of Data is Threatened*, AM. BANKER, Sept. 25, 1990, at 12.

54. *See, e.g.*, EQUIFAX REPORT, *supra* note 13, at 77; *Hearings II*, *supra* note 30, at 50-51 (statement of Richard A. Barton, Senior Vice President, Gov't Affairs, Direct Marketing Association, addressing industry self-regulation).

55. *See* EQUIFAX REPORT, *supra* note 13, at 98 (showing that advisory boards and panels dealing with privacy issues are rare among industry groups).

56. *Id.* at 70.

57. Most companies prefer to wait until others in their particular industry develop privacy policies and follow that lead. Substantial minorities of companies would either pioneer new privacy protection policies, or at the other extreme, wait until laws are passed before adopting new policies. *Id.* at 101.

58. *See id.* at 100 (privacy advocacy groups are overwhelmingly considered important to expose abuses, bring lawsuits, and sponsor legislation).

59. *Id.* at VIII.

of these concerns to individuals suggests that legal protection should systematically consider each data processing activity.

B. *The Existing Framework for Privacy Rights*

The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community. The federal constitution does not address privacy for information transactions wholly within the private sector[60] and state constitutional provisions similarly do not afford rights for private transactions.[61] Instead, legal protection is accorded exclusively through privacy rights created on an ad hoc basis by federal or state legislation or state common law rules.[62] In addition, self-regulatory

60. Although the U.S. Constitution does not contain an express right of privacy, several provisions of the Bill of Rights have been interpreted by the Supreme Court to provide a sphere of privacy protection to individuals against intrusive government activities. *See, e.g.*, Bowers v. Hardwick, 478 U.S. 186 (1986); Roe v. Wade, 410 U.S. 113 (1973); Stanley v. Georgia, 394 U.S. 557 (1969); Griswold v. Connecticut, 381 U.S. 479 (1965). These constitutional decisions have generally arisen in the context of the Fourth Amendment prohibition on unreasonable searches and seizures, the Fifth Amendment bar to self-incrimination and requirement of Due Process, and the Fourteenth Amendment Equal Protection Clause. The Supreme Court, however, has not elaborated a constitutional right of privacy among private-sector actors. Although the First Amendment protections for freedom of speech have been extended to commercial speech, the application of these protections to private information transactions unrelated to advertising or journalism is beyond the scope of this article. *See generally* Miller, *supra* note 1, at 1162-68 (presenting a preliminary exploration of First Amendment issues and information privacy for computer use).

61. A number of state constitutions expressly protect privacy rights. *See, e.g.*, ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. I, § 1 ("All people . . . have inalienable rights. Among these are . . . obtaining safety, happiness, and privacy."). ILL. CONST. art. I, § 6 ("The people shall have the right to be secure . . . against . . . invasions of privacy."). These state constitutional provisions are similar to the federal constitutional rights in that they impose restrictions only on governmental activities. *See, e.g.*, State v. Murphy, 570 P.2d 1070 (Ariz. 1977); Perkey v. Dep't of Motor Vehicles, 721 P.2d 50 (Cal. 1986); Barr v. Kelso-Burnett Co., 478 N.E.2d 1354 (Ill. 1985); Commonwealth v. Kean, 556 A.2d 374 (Pa. Super. Ct. 1989).

These constitutional provisions have not yet been applied to purely private activities. *See* Gerald B. Cope, Note, *Toward a Right of Privacy as a Matter of State Constitutional Law*, 5 FLA. ST. U. L. REV. 631 (1977).

62. Because federal legislative jurisdiction for commercial information processing activities is drawn principally from the Interstate Commerce Clause, U.S. CONST. art. I, § 8, federal law tends to be adopted on a narrow sectoral basis. State legislation and common law may have a broader jurisdictional basis. This multilayered approach

schemes have been adopted by some industries[63] and by various companies.[64] Although these schemes may offer privacy protection, they do not provide enforceable legal rights[65] and do not seem to have permeated the vast majority of information processing entities.[66]

In general, the aggregation of the federal and state rights provides targeted protection for individuals in answer to defined problems. This mosaic approach derives from the traditional American fear of government intervention in private activities and the reluctance to broadly regulate industry. The result of the mosaic is a rather haphazard and unsatisfactory response to each of the privacy concerns.

II. SECTORAL FORTRESSES—FEDERAL RIGHTS OF INFORMATION PRIVACY?

Existing federal legislation only addresses privacy concerns in particular industry contexts.[67] Although each of these industry-specific laws contains detailed obligations, they provide a sphere of protection to isolated concerns for narrowly-identified problems and are incomplete responses to information privacy

---

illustrates the division of power between the federal government and the state governments.

63. *See, e.g., Hearings II, supra* note 30, at 50-51 (statement of Richard A. Barton, Senior Vice President, Gov't Affairs, Direct Marketing Association).

64. *See* AMERICAN EXPRESS, THE AMERICAN EXPRESS CONSUMER PRIVACY PRINCIPLES (1991). American Express and IBM each have internal information codes of conduct.

65. By definition, voluntary compliance codes offer no legal sanctions for infringing practices.

66. *See* EQUIFAX REPORT, *supra* note 13, at XIII (noting that few companies in information processing industries have internal groups monitoring corporate privacy practices).

67. There is no omnibus legislation applicable to the business community although the original proposals for the Privacy Act of 1974 contemplated comprehensive provisions applicable to the private sector. *See* S. REP. NO. 1183, 93rd Cong., 2nd Sess. 14 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6929. At the time, fears of intrusion into privacy concentrated on governmental gathering of information. *Id.* at 6933. *See also* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 576 (3rd Cir. 1980) ("Much of the concern [leading up to the Privacy Act of 1974] has been with governmental accumulation of data . . . ."). The Privacy Act did not include provisions applicable to the private sector. Privacy Act of 1974 § 3, 5 U.S.C. § 552a(a)-(q) (1976). Recently, proposed legislation would have created a federal Data Protection Board. *See* H.R. 3669, 101st Cong., 1st Sess. (1989); H.R. 685, 102nd Cong., 1st Sess. (1991). The Board would not have regulatory authority, but would be charged with developing privacy principles and codes for the private sector.

issues. This ad hoc industry-specific approach leaves many areas of information processing unaddressed such as direct mail industry activities, personnel record-keeping and electronic employee surveillance. This section will first examine the protections of industry-specific laws and then will analyze the gaps.

A. The Ramparts of Protection

Congress has enacted laws applicable to the private sector with respect to financial services,[68] telecommunication services,[69] education records,[70] the workplace,[71] and home entertainment services.[72] The scope of protection accorded by each of these industry-specific laws is generally limited. The full range of issues with respect to data processing activities for personal information, such as fairness in the collection of data, data minimization, data accuracy and permissible use of personal information, are not consistently treated at the federal level.

1. Privacy and Finance

The financial services sector has perhaps the greatest variety of applicable legislation that does not systematically address privacy concerns. The laws focus for the most part on invasive or offensive credit services and the government's ability to access privately held financial records. The Fair Credit Reporting Act of 1970 ("FCRA") sets forth rights for individuals and responsibilities for consumer credit reporting agencies[73] in connection with the preparation and dissemination of personal information in a consumer report bearing on the individual's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living.[74] The FCRA restrictions do not apply to the disclosure of such personal infor-

68. *See infra* notes 73-103 and accompanying text.
69. *See infra* notes 104-13 and accompanying text.
70. *See infra* notes 114-17 and accompanying text.
71. *See infra* notes 118-21 and accompanying text.
72. *See infra* notes 122-33 and accompanying text.
73. A "consumer credit reporting agency" is defined by the FCRA as: "[A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f) (1988).
74. *See* 15 U.S.C.S. §§ 1681-1681t (Law Co-op. 1982 & Supp. 1991).

mation by organizations other than consumer credit reporting agencies.[75]

The FCRA primarily regulates disclosures of personal information and does not generally address the collection of personal information.[76] The statute avoids the issues of notice and consent, except in cases of the collection of personal information during personal interviews.[77] The FCRA ignores the acquisition of unnecessary information. In fact, the expansive categories of regulated personal information ranging from credit worthiness to personal characteristics[78] reflect that excessive personal information may be collected by credit reporting agencies.[79]

The accuracy of personal information is, nevertheless, treated by the FCRA. Credit reporting agencies must follow reasonable procedures to assure accuracy of personal information, though agencies are not held strictly liable for errors.[80] The FCRA also requires that a dispute process be implemented to investigate and correct errors.[81] To promote fairness and accuracy, individuals have a right to be informed of the contents of personal information files and of the names of recipients of credit reports.[82] In practice, however, this right may be extremely difficult to enforce because there is no requirement that credit reporting agencies notify individuals of the existence of files containing personal information or of the procedures to learn of

75. *See* Smith v. First Nat'l Bank, 837 F.2d 1575, 1578 (11th Cir.) (bank disclosing information about bad experience with one customer is not a credit reporting agency within the meaning of the statute), *cert. denied*, 488 U.S. 820 (1988).

76. In Saint Paul Guardian Ins. Co. v. Johnson, 884 F.2d 881 (5th Cir. 1989), the court ruled that personal information collected for credit reporting purposes may only be used in accordance with FCRA, *id.* at 885, but did not address limiting the collections of personal information.

77. 15 U.S.C. § 1681d(a)(1) (stating that investigative consumer report involving data collection through personal interviews may not be procured or prepared without notice to and consent from the consumer).

78. *See id.* § 1681a(d).

79. *See, e.g.*, Rothfeder, *supra*, note 12, at 80 (noting that credit reporting agencies collect information on marital status).

80. 15 U.S.C. § 1681e(b). *See* Bryant v. TRW, Inc., 689 F.2d 72, 77-78 (6th Cir. 1982); Colletti v. Credit Bureau Servs., Inc., 644 F.2d 1148 (5th Cir. 1981).

81. 15 U.S.C. § 1681i.

82. *Id.* § 1681g. Fees for access may be charged. *Id.* § 1681j. These fees currently range from $15 to $20. No fee may be charged if credit was denied on the basis of a credit report. *Id.* Curiously, consumer reporting agencies offer subscriptions for routine notification of inquiries. *What Price Privacy?*, CONSUMER REP., May 1991, at 356, 358.

the contents and uses of those files. And, despite these obligations, recent reports have found that forty-three percent of all personal information files held by the three major credit reporting agencies contain false or misleading information.[83]

A credit reporting agency has substantial latitude to disseminate regulated personal information without an individual's consent. The FCRA generally permits the disclosure of personal information by a credit reporting agency for statutorily specified purposes, namely establishing the individual's eligibility for credit, employment, insurance, or any other legitimate business need.[84] The statutory authority for disclosures related to "legitimate business needs" offers a credit reporting agency broad permission to disseminate personal information.[85] Anyone seeking to obtain a credit report must certify to the credit reporting agency that the use of the personal information is permitted by the FCRA.[86] Disclosures by a credit reporting agency for other uses require the written consent of the individual whose data is involved.[87] As long as there is a statutorily permitted use or consensual disclosure of a credit report, a recipient is not restricted from making associated or secondary uses of the personal information without the individual's consent, including subsequent disseminations.[88] If an adverse decision on credit,

83. *See What Price Privacy?*, CONSUMER REP., May 1991, at 356, 356-60. In one recent case, due to negligent data gathering, credit reports for all the homeowners in Norwich, Vermont were marked as high risks. Michael W. Miller, *Credit Report Firms Face Greater Pressure; Ask Norwich, Vt. Why*, WALL ST. J., Sept. 23, 1991, at A1.

84. 15 U.S.C.S. §§ 1681, 1681b (Law Co-op. 1982 and Supp. 1991). *See* Hansen v. Morgan, 582 F.2d 1214 (9th Cir. 1978) (holding that the obtainment of a credit report to investigate political contributions violates FCRA).

85. Courts seek to interpret this as requiring a direct nexus between a transaction for a consumer and the business claiming a legitimate need. *See* Hovater v. Equifax, Inc., 823 F.2d 413 (11th Cir.), *cert. denied*, 484 U.S. 977 (1987). Yet, if there is an insufficient business transaction, the courts may find that the report is outside the jurisdiction of the FCRA. *Id.*

86. 15 U.S.C. § 1681e(a). A reporting agency need only have "reason to believe" that a user has a permissible purpose. *See* Middlebrooks v. Retail Credit Co., 416 F. Supp. 1013 (N.D. Ga. 1976).

87. 15 U.S.C. § 1681b(2). Frequently, individuals will be asked to sign blanket consent statements authorizing inquiry into credit reporting agency files and disclosures of information for any purpose. These consents rarely identify the credit reporting agencies or all the uses to which the personal information will be put.

88. Some courts have, however, indicated that consumer reports should only be used for statutorily permitted purposes. Hansen v. Morgan, 582 F.2d 1214, 1220 (9th

insurance or employment is based on a consumer report, the decision-maker must inform the consumer of the use of the report and identify the source of the report.[89] The user of a credit report need not inform the consumer of any other adverse decision based on the report.

Although the FCRA does not generally restrict the scope of personal information which may be stored or the duration of storage, it does prohibit the dissemination of certain types of obsolete information, such as bankruptcy adjudications more than ten years prior to the report, suits and judgments older than seven years, paid tax liens older than seven years, records of arrests and convictions older than seven years and any other adverse information older than seven years.[90] A significant exception, however, provides that even obsolete information may be disseminated if requested in connection with an employment application for a position with a salary over $20,000, a credit transaction over $50,000 or the underwriting of life insurance over $50,000.[91] In today's economy, this exception can broadly permit the use and disclosure of obsolete information.[92]

Other legislation affecting credit activities and the treatment of personal information includes the Fair Credit Billing Act of 1974 which requires that consumers be furnished with copies of consumer credit transaction records and provides that consumers have rights of error correction.[93] Creditors are restricted from disclosing information about delinquent payments pending error resolution,[94] but are not otherwise prohibited from disclosing transaction records to third parties. The statute al-

---

Cir. 1978) (stating that use of a credit report for purposes not listed in the FCRA might constitute a violation of provisions against false pretenses). The secondary use of personal information contained in a credit report might, however, qualify the user as a credit reporting agency, thus subjecting this usage to the disclosure restrictions of the FCRA. *See* 15 U.S.C. § 1681a(f).

89. 15 U.S.C. § 1681m. *See* Fischl v. General Motors Acceptance Corp., 708 F.2d 143, 149-50 (5th Cir. 1983) (holding that the adverse decision need not be based on derogatory information in the credit report).

90. 15 U.S.C. § 1681c(a).

91. *Id.* § 1681c(b).

92. These dollar thresholds were set in 1970; despite inflation they have not been increased.

93. *See* 15 U.S.C. § 1666.

94. *Id.* § 1666a.

lows consistent state legislation.[95]

Similarly, the Fair Debt Collection Practices Act of 1977 limits the disclosures to third parties of a debtor's financial situation in the context of collection.[96] The Equal Credit Opportunity Act of 1974 limits the use of data relating to sex, race, color, religion, national origin, age or marital status for purposes of unlawful discrimination with respect to the grant of credit.[97] The law does not address the collection or storage of such information. This law further requires that individuals be notified of any reasons for the denial of credit.[98] The reasons must be described with some specificity.[99]

Aside from the credit laws, the Electronic Funds Transfer Act of 1978 ("EFTA") establishes mandatory guidelines for the relationship between consumers and financial institutions in connection with electronic fund transactions.[100] The EFTA sets forth detailed requirements for the collection of specified transaction data, such as time and place of each transaction, and requires disclosures and the provision of periodic account statements to consumers.[101] The EFTA does not restrict the use of transaction information; disclosures of transaction information may be made to third parties. In addition, the EFTA does not prevent financial institutions from gathering unnecessary personal information beyond that required for executing the electronic transactions and the law contains no restriction on the duration of storage of transaction records. The EFTA does, however, consider accuracy issues and obligates financial institutions to establish error-correction procedures.[102]

2. Privacy and Telecommunications

Industry-specific legislation providing limited privacy protection also exists at the federal level for telecommunications services. The Communications Act of 1984 and the Electronic

95. *Id.* § 1666j.
96. 15 U.S.C. §§ 1692b(2), 1692c(b).
97. *Id.* § 1691(a)(1).
98. *Id.* § 1691(d)(2).
99. Fischl v. General Motors Acceptance Corp., 708 F.2d 143, 147-48 (5th Cir. 1983).
100. *See* 15 U.S.C.S. §§ 1693-1693r (Law Co-op. 1982 & Supp. 1991).
101. 15 U.S.C. § 1693d.
102. *Id.* § 1693f.

Communications Privacy Act of 1986 (ECPA) impose criminal sanctions on wiretapping and surveillance activities.[103] These laws seek to protect the confidentiality of communications and generally prohibit the interception of the contents of private communications. They are primarily targeted against government actions. In the event of violations of the ECPA by the government or private parties, an aggrieved individual may seek civil penalties.[104]

Under the ECPA, the contents of a private communication can usually be disclosed by the communications carrier only if one party consents.[105] The contents of stored messages, such as electronic mail, may similarly be disclosed only with the consent of one of the parties.[106] These provisions effectively require notice and consent for the collection of the contents of communications. The statutory definitions of "contents" do not, however, include data identifying details of telecommunications transactions such as telephone numbers, or time, place, and duration of call.[107] In fact, Congress removed language from the Communications Act protecting information about the identities of parties to the communication and the existence of the communication.[108] An electronic communication service provider is even expressly permitted, without notice or subscriber consent, to disclose transaction information concerning the subscriber to any person for any purpose.[109] Thus, the ECPA does not set forth guidelines for the collection of transaction data nor does it limit the uses of transaction data. Under federal law, the use by private parties of pen registers to record outgoing call information and trap and trace devices to record incoming call data is even

103. *See* 18 U.S.C. §§ 2510-2520, 2701-2709 (1988).

104. *Id.* §§ 2520, 2707.

105. *Id.* § 2511(3)(b). The theory was that a communication is not confidential if one party is willing to disclose the contents. *See* Lewellen v. Raff, 843 F.2d 1103, 1115 (8th Cir. 1988). *See also* Simpson v. Simpson, 490 F.2d 803 (5th Cir.) (holding that spouse may even consent to surreptitious recording of other spouse's telephone conversations), *cert. denied*, 419 U.S. 897 (1974). *Contra*, Kempf v. Kempf, 868 F.2d 970 (8th Cir. 1989).

106. 18 U.S.C. § 2702(b). Disclosures without consent may also be made to the extent that they are necessary for the business of the service provider. *Id.*

107. *Id.* § 2510(8).

108. *See* The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 1, 100 Stat. 1848 (1986).

109. 18 U.S.C. § 2703(c)(1)(A). This authorization, however, does not permit disclosure to government agents.

permitted.[110] Companies are increasingly using such technology to collect information on consumers without their knowledge.[111] There are no limitations on the storage of personal information that is legitimately gathered. The ECPA provides separate criminal penalties for the unauthorized access to transaction records and stored electronic communications, such as electronic mail, by anyone other than the service provider, subscriber or communications addressee.[112]

3. Privacy and Education

Educational institutions receiving public funds must protect student records in certain limited ways. The Family Education Rights and Privacy Act of 1974 generally prohibits the disclosure of student records to third parties without prior written consent.[113] The law does not restrict the kind of information that schools may gather or the sources for such information, nor does it limit the duration of storage of personal information contained in student files. The law requires, however, that educational institutions provide students or parents of students with access to certain school records, yet there is no private right of action for a former student to compel access.[114] In some circumstances, this access may be waived in writing.[115] Schools must provide a procedure for students or parents to challenge the accuracy of records and correct or delete misleading or inappropriate data.[116]

---

110. *Id.* § 2511(2)(h). *See also* United States v. New York Tel. Co., 434 U.S. 159, 166 (1977) ("Both the language of the statute and the legislative history establish beyond any doubt that pen registers are not governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§ 2510-2520 (1970 ed. and Supp. V))").

111. *See* Churbuck, *supra* note 42, at 107; Clifford J. Levy, *Help Lines: The Benefits Are Mutual*, N.Y. TIMES, May 14, 1991, at D4; PRIVACY AND TECHNOLOGY TASK FORCE, *supra* note 42, at 13-14.

112. 18 U.S.C. § 2702(a).

113. 20 U.S.C. § 1232g(b)(1) (1988). The statute does not bar the dissemination of student records if obtained from non-school sources. Frasca v. Andrews, 463 F. Supp. 1043, 1050 (E.D.N.Y. 1979). Failure to comply with the Act can result only in a cutoff of federal funds. *See* Student Bar Ass'n Bd. of Governors v. Byrd, 239 S.E.2d 415 (N.C. 1977).

114. 20 U.S.C. § 1232g(a)(1)(A); Girardier v. Webster College, 563 F.2d 1267 (8th Cir. 1977).

115. 20 U.S.C. § 1232g(a)(1)(C).

116. *Id.* § 1232g(a)(2).

4. Privacy and the Workplace

In the field of labor relations, there is little federal protection that addresses privacy concerns. The Equal Employment Opportunity Act prohibits employment discrimination on the basis of an individual's race, color, sex, religion or national origin, and, thus, the use or classification of information relating to these personal characteristics for purposes of unlawful discrimination would be prohibited.[117] These civil rights provisions do not prohibit the collection, storage or treatment of such information; the act only imposes sanctions on the use of this personal information for illegal, discriminatory purposes.[118]

One federal statute, the Employee Polygraph Protection Act of 1988,[119] restricts the collection of information by private sector employers through the use of lie detectors. Although this law addresses data collection, it applies only to the use of a particular technique for the gathering of personal information and not to the type or extent of personal information being gathered. No other federal labor laws address the existing range of other data processing concerns. In fact, recent cases involving electronic surveillance of employee job performance have been quite controversial and have highlighted both the growing sensitivity to privacy concerns and the extremely limited nature of these industry-specific rights.[120]

5. Privacy and Home Entertainment

Finally, two laws apply to the home entertainment industry, particularly cable communication subscription services

---

117. *See* 42 U.S.C. § 2000e (1988). Any legislative action following the current debate over the renewal of civil rights legislation may affect these provisions. However, the civil rights proposals do not contemplate specific provisions targeting information privacy.

118. *Cf.* Fair Housing Act, § 5, 42 U.S.C. §§ 3604-3605 (precluding the use of personal information for unlawful discrimination in real estate sales or leasing).

119. 29 U.S.C. §§ 2001-2009 (1988).

120. *See* Paul Katzeff, *Surveillance Legislation Pending*, NAT'L L.J., Apr. 15, 1991, at 1. *See also* David F. Linowes & Ray C. Spencer, *Privacy: The Workplace Issue of the '90s*, 23 J. MARSHALL L. REV. 591 (1990) (describing privacy issues arising in the workplace); John Lund, *Computerized Work Performance Monitoring and Production Standards: A Review of Labor Law Issues*, 1991 LAB. L.J. 195 (discussing computerized monitoring of employees); Note, *Addressing New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (1991) (arguing that there are no effective privacy rights for employees with respect to surveillance).

and video rental services. These laws focus largely on the disclosure of customer viewing habits. Nevertheless, they provide the unique examples of statutory treatment for each privacy concern.

The Cable Communications Policy Act of 1984 establishes fair practices for the collection of personal information. The act requires that customers be informed of the collection of any personal information as well as the purposes for which it is collected, the anticipated disclosures of such information, the duration of storage, and the procedures for an individual to gain access to the records.[121] Cable systems may not be used to gather personal information without prior consent from the subscriber.[122] The law seeks to accommodate accuracy concerns and provides for rights of access and correction of personal information.[123] Uses of personal information are also regulated; subscriber information, such as viewing habits, may be disclosed to third parties only with the subscriber's consent or for a legitimate business activity related to the provision of service.[124] A mailing list of subscribers may, nonetheless, be disseminated if each subscriber has an opportunity to opt out.[125] The law further prohibits the retention of personal information longer than necessary to accomplish the purposes of collection.[126] Statutory damages are available to aggrieved individuals.[127]

The other law, the Video Privacy Protection Act of 1988,[128] is a criminal law adopted in response to congressional outrage over a newspaper reporter's ability to obtain the list of films rented by Judge Robert Bork at the time of his ill-fated nomination to the Supreme Court. The Act prohibits the disclosure of titles of particular films rented by any customer, though it allows the disclosure of customer names and addresses as well as subject matter interests for direct marketing purposes, provided that

121. 47 U.S.C. § 551(a)(1) (1988). *See* Warner v. American Cablevision of Kansas City, 699 F. Supp. 851 (D. Kan. 1988).

122. 47 U.S.C. § 551(b)(1).

123. *Id.* § 551(d).

124. *Id.* § 551(c)(2). To obtain a valid consent, the cable operator must inform the subscriber specifically of the intended disclosures. *Warner v. American Cablevision*, 699 F. Supp. at 856.

125. 47 U.S.C. § 551(c)(2)(C).

126. *Id.* § 551(e).

127. *Id.* § 551(f).

128. *See* 18 U.S.C. §§ 2710-11 (1988).

the customer has an opportunity to opt out. The disclosure of other personally identifiable information can only be made with the informed, written consent of the individual concerned at the time the disclosure is sought.[129] However, the Act permits disclosures of personal information without consent if such disclosures are in the ordinary course of business for the provision of videotape rental services.[130] This latter exception may prove to be a major loophole. Nevertheless, the Act limits the duration of storage of personal information to one year beyond the date the information is necessary to accomplish the purpose for which it was collected.[131] Civil remedies and statutory damages are available to aggrieved individuals.[132]

B. The Wild Frontier

Rather than provide consistent protection for individuals, the aggregation of these industry-specific rights of information privacy reveals that strikingly limited legal protection is available at the federal level in response to each of the privacy concerns. The statutory rights have been adopted for particular industries in specific contexts and result in haphazard protection for the full variety of concerns.

In assessing the privacy rights for financial services, it is clear that there is no systematic treatment of the existing privacy concerns. The laws seek to address narrow issues for credit services and electronic fund transfers.[133] In these endeavors, the laws do not try to address the full range of privacy concerns; the credit laws ignore serious data collection concerns,[134] use concerns[135] and storage concerns,[136] while the fund transfer law addresses data accuracy concerns only.[137]

As in the financial services sector, the legal rights available

129. *Id.* § 2710(b)(2)(B).
130. *Id.* § 2710(b)(2)(E).
131. *Id.* § 2710(e).
132. *Id.* § 2710(c).
133. *See supra* notes 73-103 and accompanying text. *Cf.* 12 U.S.C. § 3401 (1988) (prohibiting the disclosure of bank account records without consent, but only if the disclosure will be made to a government agent).
134. *See supra* notes 76-79 and accompanying text.
135. *See supra* notes 84-89 and accompanying text.
136. *See supra* notes 90-92 and accompanying text.
137. *See supra* notes 101-02 and accompanying text.

to protect information privacy for telecommunications services are quite detailed in the treatment of narrow problems. The confidentiality of the contents of communications are protected carefully,[138] but existing privacy concerns for other personal information related to such communications are generally ignored.[139] In particular, the failure to address the circulation of transaction information is a notable omission where such information can be matched with additional personal information from different sources to create troubling uses.[140]

With respect to education, federal law targets one form of information use—third party disclosures of personal information[141]—and touches on access and accuracy concerns.[142] Yet, information collection practices, other associated uses of school records, and storage issues are ignored. Similarly, for the workplace, federal protections address the use of certain types of information for illegal discriminatory purposes[143] and target one information collection technique.[144] The other privacy concerns have not been considered in the myriad workplace contexts.

Only in the home entertainment sector has a set of rights been elaborated to deal with each privacy concern for the various information processing activities. These rights are limited to the context of video rental and cable services.

Thus, in none of the federally regulated industries, with the exception of video rental and cable services, has data collection, use, storage and dissemination been systematically addressed. Many industries have been entirely left alone, such as list brokers and direct marketers,[145] and significant privacy concerns might only be addressed at the state level.

---

138. *See supra* notes 104-08.

139. *See supra* notes 108-11 and accompanying text.

140. *See supra* notes 42-50 and accompanying text.

141. *See supra* note 113 and accompanying text.

142. *See supra* notes 114 and 116 and accompanying text.

143. *See supra* notes 117-18 and accompanying text.

144. *See supra* note 119 and accompanying text.

145. A recent federal law on telemarketing has been described as a privacy law, but in fact only regulates nuisance telephone calls by limiting unwanted commercial solicitations that involve pre-recorded messages or automatic dialing equipment. *See* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991).

III. TAMING THE FRONTIER—STATE RIGHTS OF INFORMATION PRIVACY?

Most states provide some protection to individuals for privacy concerns through common law rights and statutory provisions. While the common law rights do not focus on data processing activities and no state has a comprehensive privacy protection statute applicable to commercial information processing, these state rights tend to cover a broader range of privacy concerns than the federal laws. There is, however, little uniformity in the treatment of privacy issues by the different states. The scope of protection and the completeness of protection vary substantially by state. This section will analyze the common law privacy rights, statutory protections and assess the unsatisfied concerns.

A. Common Law Privacy Rights

Since publication in 1890 of the seminal Warren and Brandeis article on privacy,[146] state courts have developed a set of common law torts to protect against invasions of privacy.[147] Four types of actionable invasions are generally recognized: (1) the intrusion upon one's seclusion; (2) the public disclosure of private facts; (3) publicity that places one in a false light; and (4) the misappropriation of one's name or likeness for commercial purposes.[148] Courts in most states have recognized one or more of these privacy invasions[149] and many states have codified

146. Warren & Brandeis, *supra* note 18.

147. *See* Prosser, *supra* note 19. In addition to these rights of privacy, communications made within certain special relationships, such as those between doctor and patient and attorney and client, are protected from disclosure in court and by professional confidentiality obligations. These common law duties restrict professionals from disclosing information about individual clients without the client's consent.

148. *See id.* Prosser used these four categories in his work as reporter for the RESTATEMENT (SECOND) OF TORTS (1977) and courts have regularly adopted these categorizations. *See id.* §§ 652, 652 app.

149. *See* RESTATEMENT (SECOND) OF TORTS § 652A app. reporter's note (1989 & Supp. 1990). *See also* Kelly v. Franco, 391 N.E.2d 54, 57-58 (Ill. App. Ct. 1979) (holding that Illinois protects only against the misappropriation of a person's name or likeness for commercial purposes); Strutner v. Dispatch Printing Co., 442 N.E.2d 129, 134 (Ohio Ct. App. 1982) (holding that Ohio has not adopted false light privacy tort); Kalian v. People Acting Through Community Effort, 408 A.2d 608 (R.I. 1979) (holding that Rhode Island recognizes only limited common law rights of privacy).

at least one aspect in civil or criminal statutes.[150] For many of these states, however, not all of the privacy invasions are actionable. New York, for example, rejects all but the misappropriation claim.[151] Minnesota is even said to reject all four of these rights of privacy.[152]

Because these common law rights evolved largely in response to news-media and advertising cases, there are few decisions that analyze the privacy issues in other contexts. These protections against invasions of privacy may, nevertheless, apply to commercial data processing activities and may offer limited privacy protection.

1. Intrusion Upon Seclusion

Under the right of seclusion, an individual is protected against improper conduct in connection with the gathering of personal information. A violation occurs through the intentional intrusion "upon the solitude or seclusion of another or his private affairs."[153] The conduct must be highly offensive to a reasonable person in order for an individual to be able to qualify for this protection.[154] Although there need not be a physical invasion of one's home or private places,[155] if the personal information is openly visible to the public, there cannot be an intrusion.[156]

---

150. *See, e.g.*, CAL. CIV. CODE § 3344 (West Supp. 1991); FLA. STAT. ANN. § 540.08 (West 1988); KY. REV. STAT. ANN. § 391.170 (Michie/Bobbs-Merrill 1984); MASS. ANN. LAWS ch. 214, § 3A (Law. Co-op. 1986); NEB. REV. STAT. §§ 20-201 to -211 (1987); N.Y. CIV. RIGHTS LAW, §§ 50, 51 (McKinney 1990); OKLA. STAT. ANN. tit. 21, § 839.1 (West 1983); R.I. GEN. LAWS §§ 9-1-28 to 9-1-28.1 (1985); TENN. CODE ANN. §§ 47-25-1103, 47-25-1105 (1988 & Supp. 1990); UTAH CODE ANN. § 45-3-3 (1988); WIS. STAT. ANN. § 895.50(2) (West 1983).

151. *See, e.g.*, Gautier v. Pro-Football, Inc., 107 N.E.2d 485, 487-88 (N.Y. 1952); Anderson v. Strong Memorial Hospital, 531 N.Y.S.2d 735 (N.Y. Sup. Ct. 1988).

152. *See* ROBERT ELLIS SMITH, A COMPILATION OF STATE AND FEDERAL PRIVACY RIGHTS 29 (1988).

153. RESTATEMENT (SECOND) OF TORTS § 652B (1977). *See* Prosser, *supra* note 19, at 389-90.

154. *See* RESTATEMENT (SECOND) OF TORTS § 652B; Prosser, *supra* note 19, at 389-90.

155. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b; Prosser, *supra* note 19, at 390.

156. *See, e.g.*, Ault v. Hustler Magazine, Inc., 860 F.2d 877, 882 (9th Cir. 1988) (holding that when permission granted for taking of photograph, subject matter no longer a private concern and republication will not constitute an intrusion of privacy),

In the context of data processing activities, an invasion of this right can only result from the techniques used to collect personal information. Voluntarily disclosed personal information will be outside the scope of this right.[157] Even if information is not voluntarily revealed, the particular means used to collect personal information must be highly offensive. Surreptitious or secret collections of personal information without notice or consent may be considered harmful by individuals, yet not rise to a sufficiently "objectionable" level to meet the threshold standard.[158] In any event, this right does not address other data protection practices such as the storage, use and disclosure of personal information.

2. Public Disclosure of Private Facts

The common law right against the public disclosure of private facts[159] can cover particular uses of certain types of personal information. This right does not address privacy concerns for data collection or storage. To violate the right, the personal information must not generally be available or visible to the public[160] and the information must relate to one's "private life."[161] In addition, the nature of the disclosure must be highly offensive to a reasonable person and may not be of legitimate concern to the public.[162]

Personal information voluntarily disclosed or available

---

cert. denied, 489 U.S. 1080 (1989). *See also* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c; Prosser, *supra* note 19, at 391.

157. *See* Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978) (holding that search of files containing information about plaintiff's prior insurance history with defendant was not "evidence of objectionable snooping techniques"); Graham, *supra* note 5, at 1413.

158. However, some commentators have argued that any unauthorized access to personal information contained in databases compiled from public sources should be considered objectionable. McLaughlin, *supra* note 5, at 842.

159. *See* RESTATEMENT (SECOND) OF TORTS § 652D; Prosser, *supra* note 19, at 392-98.

160. *See, e.g.*, Gill v. Hearst Publishing Co., 253 P.2d 441 (Cal. 1953) (holding that plaintiff's embrace of his wife did not relate to a private matter because the kiss occurred in a public place).

161. *See* RESTATEMENT (SECOND) OF TORTS § 652D; Prosser, *supra* note 19, at 392-98.

162. *See* RESTATEMENT (SECOND) OF TORTS § 652D; Prosser, *supra* note 19, at 397.

from public sources does not benefit from this protection.[163] As a result, activities such as the preparation and dissemination of intimate personal profiles from disparate public sources of information or public revelations of information would not be actionable. Recovery under this right further requires that there be a dissemination of qualifying personal information to the general public.[164] This is interpreted to mean general distribution to the public such as the circulation of a newspaper and not just circulation of personal information among a closed group of people.[165]

Many commercial data processing activities are unlikely to satisfy the standard of offensiveness, the condition that the personal information relate to non-disclosed matters, or the requirement of general public distribution. These thresholds thus restrict this right significantly even when important privacy concerns are raised by private sector information processing activities.

3. False Light Publicity

The right to be "secure from publicity that places [a] person in a false light before the public"[166] can address one privacy concern raised by data processing activities—the use of inaccurate information.[167] Specifically, this right can provide protection against the dissemination of personal information that is misleading or erroneous.[168] Data processing activities that involve truthful and non-misleading personal information are not covered by this action.

---

163. *See* Gill v. Hearst Publishing Co., 253 P.2d 441 (Cal. 1953).

164. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. a; Prosser, *supra* note 19, at 393.

165. *See, e.g.*, Polin v. Dun & Bradstreet, Inc., 768 F.2d 1204 (10th Cir. 1985) (circulation of credit report to 17 subscribers of reporting service is insufficient publicity to be actionable); Senogles v. Security Benefit Life Ins. Co., 536 P.2d 1358 (Kan. 1975) (holding that insurance company's dissemination of applicant's medical history to a trade association, Medical Information Bureau, not actionable).

166. RESTATEMENT (SECOND) OF TORTS § 652E. *See* Prosser, *supra* note 19, at 398-401.

167. This right is very similar to the common law protection against defamation. *See* Lovgren v. Citizens First Nat'l Bank, 534 N.E.2d 987, 988-91 (Ill. 1989). A discussion of defamation law is beyond the scope of this article.

168. *See, e.g.*, Leverton v. Curtis Pub. Co., 192 F.2d 974 (3rd Cir. 1951) (photograph of non-negligent child used to illustrate article on children's negligence); RESTATEMENT (SECOND) OF TORTS § 652E; Prosser, *supra* note 19, at 398-401.

The false light claim can be made only if there is a wide dissemination of misleading or erroneous personal information. An individual cannot prevail if the disclosure was made in the context of a private communication, even if the dissemination was made to a group of people or business entities.[169] As a result, this action is not likely to be particularly useful for individuals in the context of commercial data processing activities where there is no public offering of inaccurate personal information.

4. Misappropriation of an Individual's Name

A right exists against "one who appropriates to his own use or benefit the name or likeness of another."[170] This protection against the misappropriation of one's name may offer coverage for privacy concerns associated with some commercial data processing activities.[171] The right originally emerged to address unauthorized endorsements in advertisements and commercial uses of photographs of individuals.[172] Yet it is possible that this right could apply to ban certain uses, including dissemination, of personal information for commercial purposes without consent. However, privacy concerns associated with the collection of personal information—notice and consent to data acquisition, unnecessary data compilation, and accuracy of data—and the storage of personal information would be outside the scope of this misappropriation right.

The courts often point out that this right protects narrowly against the appropriation of the value of one's personality[173] and

169. *See Polin v. Dun & Bradstreet*, 768 F.2d 1204 (holding that a communication to 17 business entities does not constitute "publicity"). *See also* RESTATEMENT (SECOND) OF TORTS §§ 652E cmt. a (using the same standard for publicity established in comment a of § 652D for public disclosure of private facts: the communication must be "to the public at large" and not merely a private communication); Graham, *supra* note 5, at 1412.

170. *See* RESTATEMENT (SECOND) OF TORTS § 652C; Prosser, *supra* note 19, at 401-07.

171. *See* Graham, *supra* note 5, at 1412 (arguing that this tort "affords little protection against invasion of information privacy by the misuse of information"); George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 539 (1990) (arguing that the sale of mailing lists is tortious).

172. *See, e.g.*, Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

173. *See, e.g.*, Goodyear Tire & Rubber Co. v. Vandergriff, 184 S.E. 452, 454 (Ga. 1936); Freihofer v. Hearst Corp., 480 N.E.2d 349, 353 (N.Y. 1985); Bartholomew v. Workman, 169 P.2d 1012, 1014 (Okla. 1946). *See also* RESTATEMENT (SECOND) OF

a privilege usually exists for media uses due to federal and state constitutional protections of free expression.[174] If personal information can be considered to invoke an individual's "personality," then the use might be regulated. When the personal information being processed approaches a profile of an individual, it is possible to view commercial uses as an appropriation of one's personality. Although the use of a name and address in itself, for example, might not constitute an appropriation of that individual's personality, if the degree of personal information portrays aspects of the individual's lifestyle (e.g., wine collecting based on a list of all wealthy wine drinkers with an affinity for fine French cognac), the information profile could be considered a reflection of the individual's personality. As such, it might thus be within the scope of this protection. In these instances, the right would restrict the use giving rise to commercial gain rather than the collection or storage of that personal information.

Although reported cases do not seem to address this invasion of privacy in the context of data processing, one old Ohio case gives a confused discussion of the use of a personality profile under the misappropriation theory. In *Shibley v. Time, Inc.*,[175] the Ohio court ruled against a plaintiff who argued that the sale of his name and address as part of a mailing list was an appropriation of a personality profile and, thus, an invasion of privacy. The court relied on the argument that there was no reasonable expectation of privacy in the mailbox and that no misappropriation of Shibley's personality could occur without a display to the public. In general, courts do not require an expectation of privacy or publicity as elements of this invasion of privacy.[176] The *Shibley* court did not, in fact, assess whether the

---

TORTS § 652C cmt. c (stating that the appropriation must be of another's "reputation, prestige, social or commercial standing [or] public interest").

174. *See, e.g.*, Arrington v. New York Times Co., 434 N.E.2d 1319 (N.Y. 1982) (interpreting the New York codification of this common law right), *cert. denied*, 459 U.S. 1146 (1983).

175. 341 N.E.2d 337 (Ohio App. 1975).

176. *See, e.g.*, Coleman v. Ted's Auto Sales, Inc., 227 N.Y.S.2d 693 (N.Y. Sup. Ct.), *aff'd*, 17 A.D.2d 827 (N.Y. App. Div. 1962) (holding that a cause of action arose from defendant's unauthorized use in credit application of plaintiff's name as an associate of business partnership); Griffin v. Harris, Beach, Wilcox, Rubin and Levey, 481 N.Y.S.2d 963 (N.Y. Sup. Ct. 1984) (noting that the unauthorized use in a credit application of an individual's name as a named plaintiff would constitute an invasion of

mailing list reflected Shibley's personality. Significantly, in New York, where this right has been codified, there is some case support prohibiting dealing in photographs that could also apply to mail list brokers.[177]

B. Statutory Protection

In addition to the common law protection against invasions of privacy, most states have enacted some statutory rights that apply to industry.[178] Three approaches can be discerned among

---

privacy under common law, but not under the New York statute because the defendant did not receive an economic benefit as the direct result of the unauthorized use; court distinguishes *Coleman* on the grounds that in that case the circulation of a credit application was an advertisement); *Goodyear v. Vandergriff*, 184 S.E. at 454 (plaintiff's name used without permission to gain access to confidential price quotes); Hinish v. Meier & Frank Co., 113 P.2d 438, 448 (Ore. 1941) (plaintiff's name signed without consent on telegram to governor). *See also* RESTATEMENT (SECOND) OF TORTS § 652C cmt. b, illus. 3-5 (cases in which publication does not occur).

177. *See Arrington v. New York Times*, 434 N.E.2d at 1323-24. This landmark New York Court of Appeals decision supports the view that section 51 of the New York Civil Rights Law (codifying the misappropriation invasion of privacy) should be applicable to sales of name-linked information. Arrington sued the Times for publishing his photograph without his consent. The court held that the Times could not be liable because of the media privilege. But significantly, the court held that the dealer, Contact Press Images, who sold the photograph of Arrington without consent could be liable under section 51.

The court ruled that dealer's liability could exist notwithstanding the Times' right to publish the photograph. *Id.* at 1323-24, and specifically refused a motion for reargument on this point. 454 N.Y.S.2d 75 (N.Y. 1982). The court said that Contact Press Images had commercialized the photograph in furtherance of trade. Although the legislature responded the following year and amended section 51 to protect middlemen who sell photographs to newspapers for publication, dealers in photographs are still subject to liability if the end use of the photograph is prohibited by section 51. *See* 1983 N.Y. Laws 280, *reprinted in* 1983 N.Y. STATE LEGIS. ANNUAL 124 (memorandum of Senator H. Douglas Barclay) ("The purpose of this bill is to correct the inadvertent effect of a 1982 decision of the New York Court of Appeals which could seriously limit the availability of photographs taken by freelance photographers for use by major news organizations.").

Dealing in names presents a situation analogous to that of merchandising photographs. Collecting and selling personal information is very much like acquiring and selling photographs. The statute, as well as the common law tort, proscribes the use of "names" in the same manner that it restricts the use of photographs. As a result, it appears that section 51 could prohibit any use for commercial purposes of the names of individuals without their consent. New York also requires that such consent be in writing. *See* N.Y. CIV. RIGHTS LAW § 51 (McKinney 1990).

178. *See, e.g.*, ALA. CODE §§ 13A-11-30 to -11-37 (1982 & Supp. 1990); CAL. CIV. CODE §§ 990, 1747.8, 3344 (West Supp. 1991); CAL. PENAL CODE § 637.5 (West 1988); CONN. GEN. STAT. ANN. §§ 53-422, 53-450 (West 1985 & Supp. 1991); DEL. CODE ANN. tit. 11, §§ 925, 1335, 1336 (1987 & Supp. 1990); FLA. STAT. ANN.

these statutory rights. At least two states, Massachusetts and Wisconsin, have adopted general rights of privacy,[179] though these rights seem to be viewed only as expressions of the common law torts.[180] A substantial number of states have codified one or more of the four common law invasions of privacy.[181] And many states have enacted industry-specific legislation containing a variety of privacy rights in fields such as financial services,[182] telecommunications,[183] home entertainment and in-

§ 540.08 (West 1988); ILL. ANN. STAT. ch. 17, ¶ 360 (Smith-Hurd 1981 & Supp. 1991); ILL. ANN. STAT. ch. 38, ¶ 87-1 to 87-3 (Smith-Hurd Supp. 1991); KY. REV. STAT. ANN. § 391.170 (Michie/Bobbs-Merrill 1984); ME. REV. STAT. ANN. tit. 17-A, § 511 (West 1983); MASS. ANN. LAWS ch. 214 §§ 1B, 3A (Law. Co-op. 1986); MICH. COMP. LAWS ANN. § 750.539 (West 1991); MINN. STAT. ANN. § 626A (West 1983 & Supp. 1991); NEB. REV. STAT. §§ 20-201 to -211 (1987); N.H. REV. STAT. ANN. § 644.9 (1986); N.H. REV. STAT. ANN. § 359C:1-18 (1984); N.J. STAT. ANN. § 17:16K-3 (West 1984); N.J. STAT. ANN. § 48:5A-54 to -63 (West Supp. 1991); N.M. STAT. ANN. §§ 56-3-1 to 56-3-8 (Michie 1986 & Supp. 1990); N.Y. CIV. RIGHTS LAW §§ 50, 51 (McKinney 1990); N.D. CENT. CODE § 14-02-10 (1981 & Supp. 1989); OKLA. STAT. ANN. tit. 21, §§ 839.1, 839.2 (West 1983); 18 PA. CONS. STAT. ANN, §§ 5701-5775 (1983 & Supp. 1991); R.I. GEN. LAWS ANN. §§ 9-1-28, 9-1-28.1 (Supp. 1990); S.D. CODIFIED LAWS ANN. §§ 22-21-1, 22-21-3 (1988); TENN. CODE ANN. §§ 45-10-104, 47-25-1103, 47-25-1105 (1988 & Supp. 1990); UTAH CODE ANN. §§ 45-3-1 to 45-3-6, 77-23a-1 to 77-23a-16 (1988 & Supp. 1991); VA. CODE ANN. § 8.01-40 (Michie 1984 & Supp. 1991); WIS. STAT. ANN. § 895.50 (West 1983 & Supp. 1991). *See also* SMITH, *supra* note 152.

179. *See* MASS. ANN. LAWS ch. 214, § 1B (Law. Co-op. 1986) ("A person shall have a right against unreasonable, substantial or serious interference with his privacy."); WIS. STAT. ANN. § 895.50(1) (West 1983) ("The right of privacy is recognized in this state.").

180. Massachusetts treats the general right of privacy as a right of protection against the publication of private facts. *See* Bratt v. IBM Corp., 467 N.E.2d 126, 136 (Mass. 1984). However, the standard of publicity is lower than the traditional common law requirement and limited intracorporate circulation of personal information could suffice. Consequently, this right would have slightly broader applications in Massachusetts than the common law action. In Wisconsin, the statute limits the general right to the intrusion, publicity of private facts, and misappropriation torts. *See* WIS. STAT. ANN. § 895.50(2) (West 1983); Zinda v. Louisiana Pac. Corp., 440 N.W.2d 548, 554-55 (Wis. 1989).

181. *See supra* note 150. Text accompanying notes 153-77 provides an analysis of these rights. In states that have not adopted all four of the common law rights, the remaining actions for invasions of privacy are often unavailable. For example, no common law or non-statutory rights of privacy are recognized in New York or Virginia. *See* Anderson v. Strong Memorial Hosp., 531 N.Y.S.2d 735 (N.Y. Sup. Ct. 1988); Falwell v. Penthouse Int'l, Ltd., 521 F. Supp. 1204, 1206-07 (W.D. Va. 1981). Massachusetts has not adopted the false light invasion of privacy. *See* Elm Medical Lab., Inc. v. RKO General, Inc., 532 N.E.2d 675 (Mass. 1989). *But see* UTAH CODE ANN. § 45-3-6 (1988) (The Abuse of Personal Identity Act "does not limit or supersede any causes of action otherwise available to the parties.").

182. *See infra* notes 188-197 and accompanying text.

formation services,[184] employment records,[185] insurance records[186] as well as a few special sets of protection.[187] Like the federal industry-specific laws, each state law generally seeks to resolve a narrow problem within a given industry and does not systematically address all the privacy concerns relating to the acquisition, storage, transmission, use and disclosure of personal information. Analysis of the state industry-specific regulation shows the limited and ad hoc nature of these rights.

1. Personal Information and Financial Services

As at the federal level, statutory protection is also granted by some states against credit reporting activities.[188] Each state with legislation may offer different degrees of protection to individuals in addition to the federal rights.[189] Generally, the state statutes restrict the purposes for which personal information may be disseminated and grant individuals rights of access and rights to challenge the accuracy of stored information. Some of the laws limit the types of information that may be contained in credit files, namely, data relating to race, religion and sexual orientation and limit information that can be stored for indefinite periods of time such as bankruptcy records, information about bad debts, drug or alcohol addictions, and any other adverse information.[190] As with the federal FCRA, these laws do not uniformly address notice or consent to the collection of personal information, associated uses of personal information, or the duration of storage of most types of personal information. Two states with substantial credit processing facilities, South Dakota and New Jersey, do not, however, offer additional statutory pro-

183. *See infra* notes 198-200 and accompanying text.

184. *See infra* notes 201-203 and accompanying text.

185. *See infra* notes 204-208 and accompanying text.

186. *See infra* notes 209-211 and accompanying text.

187. *See infra* notes 212-214 and accompanying text.

188. Congress has authorized the states to adopt non-conflicting rights. *See* 15 U.S.C. § 1681t.

189. *See, e.g.*, LA. REV. STAT. ANN. § 9:3571 (West 1991); ME. REV. STAT. ANN. tit. 10, §§ 1311-1329 (West 1980 & Supp. 1990); MASS. ANN. LAWS ch. 93, §§ 50-68 (Law. Co-op. 1985 & Supp. 1991); N.M. STAT. ANN. §§ 56-3-1 to 56-3-8 (Michie 1986 & Supp. 1990); N.Y. GEN. BUS. LAW § 380 (McKinney 1984 & Supp. 1991).

190. *See, e.g.*, ME. REV. STAT. ANN. tit. 10, § 1321 (West 1980 & Supp. 1990); N.Y. GEN. BUS. LAW § 380j (McKinney 1984 & Supp. 1991).

tection to supplement the federal rights.[191]

States may also regulate personal information in connection with electronic fund transfers. The federal law does not preempt consistent state regulation.[192] These state laws do not generally restrict the overbroad collection of personal information nor the duration of storage of personal information. They may, however, provide additional restrictions on the dissemination of transaction records.[193] New Jersey, for example, permits the disclosure to a third party of information relative to an electronic fund transfer only in specified circumstances: if the disclosure is necessary to complete the transaction; if the client gives written consent; if the disclosure is necessary to resolve or investigate errors; or if the disclosure is for the purpose of verifying the existence and condition of an account for a third party, including credit bureaus and merchants.[194] Permissible disclosure for verification purposes does, in practice, mean that the financial institution will have significant authority to disclose electronic fund transfer activities.

A few states have prohibited the collection of certain types of unnecessary personal information in response to credit fraud problems.[195] Specifically, these laws limit a merchant's ability to mark on a customer's credit card charge form, personal information including the individual's address and telephone number. Virginia prohibits merchants from requiring a customer to reveal a credit card number when payment for a transaction is to be made by check.[196] Several national retail stores, such as the consumer electronics chains Radio Shack and Newmark &

191. Such rights might protect the residents of the state, such as local cardholders, as well as ensure fair information practices by local card issuers and local transaction processing companies.

192. 15 U.S.C. § 1693q.

193. *See, e.g.*, MASS. ANN. LAWS ch. 167B, § 16 (Law. Co-op. 1987); N.J. STAT. ANN. § 17:16K-3 (West 1984).

194. *See* N.J. STAT. ANN. § 17:16K-3 (West 1984).

195. *See, e.g.*, CAL. CIV. CODE § 1747.8 (West Supp. 1991); DEL. CODE ANN. tit. 11, § 914 (Supp. 1990); MD. COM. LAW CODE ANN. § 13-318 (Supp. 1991); N.Y. GEN. BUS. LAW § 520-a (McKinney Supp. 1991); WASH. REV. CODE ANN. § 62A.3-512 (West Supp. 1991). If a cardholder's name, account number, expiration date, address and telephone number are available, fraudulent charges may easily be made to the card account. These laws seek to protect cardholders and card issuers from merchants' practices that may facilitate such crime.

196. VA. CODE ANN. § 11-33.1 (Michie Supp. 1991). *See also* DEL. CODE ANN. tit. 11, § 915 (Supp. 1990); FLA. STAT. ANN. § 832.075 (West Supp. 1991).

Lewis, still have computer systems that are not configured to process sales, including cash sales, without a customer's name and address.

Some states, such as Illinois and Connecticut, have enacted laws restricting the permissible disclosures of bank customer financial information including information on bank account activity.[197] These confidentiality laws affect the uses of personal information only.

2. Personal Information and Telecommunications Services

Communications privacy statutes, similar to the federal ECPA, also exist at the state level.[198] These state criminal laws sometimes grant greater protections than the federal statute against unauthorized access to communications. Like the federal law, the state statutes generally prohibit the collection and storage of the contents of a communication without at least one party's consent. Some states go further than the federal law and restrict the collection or use of transaction data (i.e., the identities of the parties to a communication and existence of the communication). Pennsylvania, for example, generally prohibits the use of pen registers or trap and trace devices to collect transaction information.[199] Pennsylvania also requires the consent of both parties to a communication in order for disclosures of the contents or disseminations of transaction data to be permissible.[200]

Like the federal laws, the state statutes generally do not address issues of the duration of the storage of personal information such as transaction records, the unnecessary collection of personal information or associated uses of personal information.

197. *See, e.g.*, CONN. GEN. STAT. ANN. § 36-9k (West 1987); Ill. Ann. Stat. ch. 17, ¶ 360(c) (Smith-Hurd 1981 & Supp. 1991).

198. *See, e.g.*, ALA. CODE §§ 13A-11-30 to 13A-11-37 (1982); DEL. CODE ANN. tit. 11, §§ 1335-1336 (1987 & Supp. 1990); MINN. STAT. ANN. § 626A.02(2)-(3) (West Supp. 1991); 18 PA. CONS. STAT. ANN. §§ 5701-5775 (1983 & Supp. 1991).

199. *See* 18 PA. CONS. STAT. ANN. § 5771 (Supp. 1991).

200. Pennsylvania is a two-party consent state. *See* 18 PA. CONS. STAT. ANN. § 5704(4) (1983 & Supp. 1991). A Pennsylvania Commonwealth Court has recently ruled against the introduction of caller identification without the consent of both parties to the communication. *See* Barasch v. Pennsylvania Pub. Util. Comm'n, 576 A.2d 79 (Pa. Commw. Ct. 1990), *aff'd*, Pennsylvania Pub. Util. Comm'n v. Bell, No. 201, 202, 1992 Pa. S. Ct. LEXIS 242.

3. Personal Information and Home Entertainment and Information Services

In several states, home entertainment and home information service record-keeping activities may be subject to specific protections.[201] Federal law authorizes the states to adopt more restrictive laws for the protection of certain personal information related to home entertainment.[202] Like the federal laws, the existing state laws tend to limit the kinds of personal information that may be collected about subscribers to cable television and video rental services, though some extend the protections to electronic information services offered to households, such as Prodigy, CompuServe, or Dialog. The statutes also limit the manner of collection of personal information from subscribers. In addition, they contain stricter prohibitions on the dissemination of information about subscribers including the identities of subscribers and details about those subscribers' use of particular electronic information services, cable viewing selections, or video rental film choices. It is significant to note that New Jersey, a state with a major processing center for cable billing records, has a law protecting against the dissemination of information about cable subscribers and their viewing habits.[203] Where other local laws provide fewer privacy rights, New Jersey risks the loss of cable processing businesses. Nevertheless, the state believes that privacy protection is important.

4. Personal Information and Employment Records

A number of states require privacy for personnel record-keeping activities.[204] Some states impose limits on the type of

201. *See* CAL. CIV. CODE § 1799.3 (West Supp. 1991) (video rental privacy); CAL. PENAL CODE § 637.5 (West 1988) (cable communications privacy); CONN. GEN. STAT. ANN. §§ 53-420 to -422 (West 1985) (cable and information services privacy); CONN. GEN. STAT. ANN. § 53-450 (West Supp. 1991) (video rental privacy); DEL. CODE ANN. tit. 11, § 925 (Supp. 1990) (video rental privacy); MICH. COMP. LAWS ANN. §§ 445.1711-.1715 (West Supp. 1991) (video rental privacy); N.J. STAT. ANN. § 48:5A-54 to -63 (West Supp. 1991) (cable services privacy); R.I. GEN. LAWS ANN. § 11-18-32 (Supp. 1990) (video rental privacy); WIS. STAT. ANN. § 134.43 (West 1989) (cable services privacy).

202. 18 U.S.C. § 2710(f).

203. *See* N.J. STAT. ANN. § 48:5A-54 to -63 (West Supp. 1991).

204. *See, e.g.*, CAL. LAB. CODE § 1198.5 (West 1989); CONN. GEN. STAT. ANN. §§ 31-128a to -128h (West 1987); ILL. STAT. ANN. ch. 48, ¶¶ 2001-2012 (Smith-Hurd 1986 & Supp. 1991); MASS. ANN. LAWS ch. 149, § 52C (Law. Co-op. 1989).

personal information that may be maintained concerning employees, such as lifestyle information.[205] But these state laws generally do not address the manner or scope of data collection[206] or the storage of most types of personal information. The laws do tend to provide employees with rights of access to employers' personnel records and require that employers investigate any complaints about accuracy. Under some of the laws, employees are granted a right to have an explanatory statement included in any file when there is an unresolved dispute regarding accuracy of personal information.[207] In addition, some state laws may require that an employee give consent before the employer discloses any personal information to third parties, except for disclosures made to verify an employee's dates of employment, title or position, and wage or salary.[208]

5. Personal Information and Insurance Records

Many states have adopted statutory guidelines for the collection, use and dissemination of personal information by insurance companies.[209] These laws generally require that notice be given to individuals prior to the collection of personal information. Insurance companies are sometimes required to grant individuals access to files containing personal information and to have a procedure for correcting errors.[210] Some laws limit the use of certain information in making adverse insurance decisions. The District of Columbia, for example, prohibits the collection or use of information concerning the AIDS virus or other blood test results for underwriting decisions.[211] The insurance

205. *See* ILL. ANN. STAT. ch. 48, ¶ 2009 (Smith-Hurd 1986); MASS. ANN. LAWS ch. 149, § 52C (Law. Co-op. 1989).

206. *But see infra* note 213 and accompanying text. Some states have rules prohibiting employers from asking job applicants certain personal information. *See, e.g.*, N.Y. EXEC. LAW § 296(1)(d) (McKinney 1984); Holland v. Edwards, 119 N.E.2d 581 (N.Y. 1954). These rules are designed to prevent unlawful employment discrimination.

207. *See* CONN. GEN. STAT. ANN. § 31-128e (West 1987); MASS. ANN. LAWS ch. 149, § 52C (Law. Co-op. 1989).

208. *See* CONN. GEN. STAT. ANN. § 31-128f (West 1987).

209. *See, e.g.*, D.C. CODE ANN. §§ 35.221 to .229 (1988 & Supp. 1990); GA. CODE ANN. §§ 33-39-1 to 33-39-23 (Harrison 1990); ILL. ANN. STAT. ch. 73, ¶¶ 1065.701 to .724 (Smith-Hurd Supp. 1991).

210. *See, e.g.*, CONN. GEN. STAT. ANN. §§ 38-508, 38-509 (West 1987); GA. CODE ANN. §§ 33-39-9, 33-39-10 (Harrison 1990).

211. *See* D.C. CODE ANN. § 35-224 (1988 & Supp. 1990).

statutes do not, however, generally address concerns related to unnecessary collections of personal information or the storage of obsolete personal information.

6. Personal Information and Special Protections

Some additional and curious privacy rights are also found in state statutes. In California, for example, anyone in the business of organizing car pools is prohibited from disclosing to others any personal information (such as name, address, place of employment, and hours of employment) collected for the purpose of making car pool arrangements.[212]

A variety of state laws deal with other privacy protection issues, such as polygraph testing for employees and AIDS testing.[213] These laws generally do not deal with issues of data minimization or data quality (including rights of access and correction). Instead, they restrict certain types of data collection techniques such as the polygraph or restrict disclosures of medical test results. Most states, in fact, have statutory prohibitions on the disclosure of medical records without the patient's consent.[214]

C. *The Open Range of Unsatisfied Concerns*

The state rights of privacy do not consistently fill the gaps left by the federal industry-specific protections. The four common law rights can cover some aspects of commercial data processing activities, but remain far from satisfying the privacy concerns left untouched by federal law. The seclusion right can only apply in limited circumstances to the collection of personal information.[215] False light publicity and publicity to private matters only address particular types of disseminations of personal information[216] and the misappropriation right might only cover uses of profile information.[217] In addition, without firm precedents, the slow and costly legal process for aggrieved indi-

212. *See* CAL. PENAL CODE § 637.6 (West Supp. 1991).

213. *See, e.g.*, CAL. LAB. CODE § 432.2 (West 1990) (polygraph testing); ME. REV. STAT. ANN. tit. 5, §§ 19203-19208 (West 1989 & Supp. 1990) (AIDS testing).

214. *See* SMITH, *supra* note 153, at 21-24.

215. *See supra* notes 153-58 and accompanying text.

216. *See supra* notes 159-69 and accompanying text.

217. *See supra* notes 170-77 and accompanying text.

viduals seeking recovery and the difficulty of proving damages in tort serve as a discouragement to the vindication of privacy invasions.

The state statutory rights similarly do not generally afford protection to the concerns left untreated by federal legislation. In the context of financial services, complementary state regulation may restrict the storage of certain types of sensitive information for credit reporting activities[218] and the disclosure of electronic fund records[219] and banking records,[220] and some further statutory rights may prevent the collection of unnecessary information in connection with certain forms of payment.[221] Yet on the whole, issues of notice and consent to the collection of personal information, associated uses of personal information and the duration of storage of personal information are not addressed for most financial services.

For telecommunications services, state protections are also confined to the narrow range of privacy concerns seen in federal law. Although some states may address the collection and use of the contents as well as transaction information,[222] the statutes usually do not focus on the collection of excessive amounts of personal information, associated uses of personal information or the duration of storage of personal information.

State legislation similarly tends to avoid most of the privacy concerns in the workplace. While some states have statutes governing personnel record-keeping and a particular information gathering technique (polygraphs), the state laws generally ignore issues of information collection, associated use of personnel information and the duration of storage of employees' personal information.[223]

In several isolated industries, however, the states have adopted legislation that addresses each of the privacy concerns. Like the federal laws, state legislation on home entertainment gives considered treatment to each of the privacy concerns for

218. *See supra* note 190 and accompanying text.
219. *See supra* notes 193-94 and accompanying text.
220. *See supra* note 197 and accompanying text.
221. *See supra* notes 195-96 and accompanying text.
222. *See supra* notes 199-200 and accompanying text.
223. *See supra* notes 204-08 and accompanying text.

cable and video services.[224] In some cases, the states go further and apply these same rules to information services provided to households.[225] In the insurance industry, state regulation covers the collection, use and dissemination of personal information, though not all aspects are targeted, such as the collection of unnecessary information and the duration of storage.[226]

The failure of state common law and statutory rights to respond fully to each of the privacy concerns associated with commercial information processing is emphasized by the varying acceptance in different state courts of common law privacy rights[227] and by the varying adoption in state legislatures of statutory protection. The diversity of state legislation nevertheless appears to cover more subject matter areas than existing federal legislation. However, each state has its own separate set of statutory rights and few, if any, of the fifty states cover a significant portion of the entire list of common law and statutory examples. Systematically available privacy rights appear to remain at the frontier of unresolved problems for the existing information economy.

IV. A MISSION FOR THE CAVALRY—FRAMING THE DEBATE FOR INTELLIGENT INFORMATION PRIVACY PROTECTION[228]

Since information processing occurs today throughout every industry, the privacy concerns are not unique to activities in any one context. Because privacy rights in the United States for commercial information processing depend on legislation targeted at narrow problems and rather limited common law rights, the lack of a coherent and systematic approach to existing privacy concerns presents an undesirable policy void. The multitude of non-comprehensive and overlapping federal and state

224. *See supra* notes 201-03 and accompanying text.

225. *See supra* note 201.

226. *See supra* notes 209-211 and accompanying text.

227. *See supra* notes 149, 151, 152.

228. A number of points in this discussion draw heavily on a paper prepared by the author for a workshop organized by Computer Professionals for Social Responsibility and the Electronic Frontier Foundation held in Washington, D.C., June 25-26, 1991. *See* Joel R. Reidenberg, Developing Cyberspace Privacy Policy: A Working Paper on the Legal Challenge for the Private Sector, prepared for the Symposium on "Civilizing Cyberspace: Minding the Matrix" (June 1991).

laws makes the task of identifying the rights of individuals and the obligations of entities processing personal information difficult to discern, if they are available at all. The majority of industry is not fully dealing with these issues[229] and the globalization of information processing networks[230] leaves companies in the United States vulnerable to foreign regulatory impediments imposed on the basis of privacy concerns.[231] Without consistently available rights treating each privacy concern, individuals cannot enforce fair information practices for the treatment of personal information. This suggests that the legal approach for commercial data processing activities needs to be restructured in the United States.

In considering a new approach to information privacy protection, a variety of issues will have critical significance for the success of any attempt to deal with the privacy concerns. Other ways of addressing these concerns in different countries may offer illustrative guidance for United States policy. The European frameworks take a more formal approach to the treatment of privacy concerns. Europeans have not historically been hesitant to regulate commercial activities and several European countries have adopted omnibus legislation governing private sector data processing.[232] Among these broad laws, there are a number of important differences relating to the scope of coverage and the regulatory enforcement mechanisms.[233] In particular, several of

229. *See* EQUIFAX REPORT, *supra* note 13, at 98 (noting that only 32% of corporate spokespeople, 20% of banks and thrifts, 18% of credit grantors, and 14% of insurance companies surveyed said their companies had formed a board or panel devoted to privacy issues).

230. *See, e.g.*, Herman & Halvey, *supra* note 53, at 12 ("[I]t has become commonplace for a bank to transmit customer account information and other financial data on individual and corporate customers . . . across international borders.").

231. *See supra* note 16.

232. *See supra* notes 15 and 23.

233. Most of the laws establish a data protection agency with enforcement powers over the private sector. Most of the national laws require registration with the regulatory agency prior to the commencement of any data processing activities. In general, no use may be made of personal information for purposes which are not registered with the data protection agency. If the regulatory agency denies registration, no data processing activities may occur. These registration schemes have posed a number of sensitive problems for data processing. Often the registration process can in itself be intrusive to the point of stifling new legitimate activities. Similarly, it can be difficult to determine whether a particular use of personal information is within the scope of a registered purpose. *See* NUGTER, *supra* note 15; Flaherty, *supra* note 5.

the laws apply protections to legal persons as well as natural persons,[234] several apply protection to manual files as well as computer records,[235] and several impose more stringent restrictions on third party disclosures of personal information. The regulatory principles in many of the national laws are more detailed than those found in the European Convention.[236] For example, the French law specifically requires that individuals be given notice prior to any data collection.[237] The Commission of the European Community believes that the effect of these differences is likely to impede the development of the single European market and has proposed a directive to harmonize these laws and establish a community standard of privacy protection.[238]

The European experience suggests that the precise enumeration of legal rights or principles addressing the privacy concerns of data collection (including notice, consent, necessity, and accuracy),[239] uses (including associated uses)[240] and the duration of storage[241] requires careful consideration.[242]

The proper jurisdictional level for any new American approach is also a threshold issue. Because personal information flows are not confined to state or national borders, it may be most appropriate to adopt any new rights at the federal level. Differences in privacy protection among the states could readily have adverse or distorting effects on interstate commerce and international data flows.[243] Business has historically supported

234. Countries that have enacted such laws include Austria and Luxembourg. *See Data Protection Roundup*, PRIVACY L. & BUS., July 1991, at 2, 7; COMMISSION OF THE EUROPEAN COMMUNITIES, THE TEDIS-EDI LEGAL WORKSHOP, Eur. Comm. Doc. AT/dd(89)1814, at 82 (July 24, 1989).

235. Countries that have enacted such laws include Holland, France, Germany and Denmark. *See Data Protection Roundup*, PRIVACY L. & BUS., July 1991, at 2-7; TEDIS-EDI LEGAL WORKSHOP, *supra* note 234, at 84-85.

236. *See supra* note 23.

237. *See* Loi No. 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertes, art. 27, J.O. du 7 janvier 1978, *modified*, J.O. du 25 janvier 1978.

238. *See* Draft EC Directive, *supra* note 15.

239. *See supra* notes 26-41 and accompanying text.

240. *See supra* notes 42-50 and accompanying text.

241. *See supra* note 51 and accompanying text.

242. Discussion of the specific formulation of principles responding to privacy concerns is beyond the scope of this Article. A variety of examples can be found for drafting such language. *See* OECD Guidelines, *supra* note 20; European Convention, *supra* note 20; Draft EC Directive, *supra* note 15.

243. *See supra* notes 16 and 53.

uniformity of any mandatory rules to avoid the confusion of fifty separate sets of state privacy regulations.[244]

Sensitivity to the commercial needs of an information economy is also an important consideration for any new framework. Industry is properly worried that constraints on processing of personal information may impose cost burdens on legitimate activities, whether or not those activities are truly objectionable to individuals, and may hamper the development of information processing networks;[245] consumers overwhelmingly desire the benefits that accrue from information processing activities, such as the ready availability of credit at low costs.[246] A balance must exist if the business environment is to be conducive to the development of new information services and information networks.[247]

In thinking about a workable balance between privacy concerns and commercial needs, policy-makers should consider that the depth of any particular concern is likely to vary with each specific data processing activity.[248] For example, associated uses

---

244. *See* PRIVACY COMM'N, *supra* note 2, at 32.

245. Notice obligations for the collection of disclosed information or the storage of transaction information could, in many instances, pose substantial difficulties and added costs for the processing entities. New technologies may give rise to associated uses for information that were unforeseeable at the time the personal information was originally compiled. These associated uses may be highly desirable from the individual's point of view and could be too costly to accomplish if strict notice or consent requirements were to be applied rigorously to such uses. *See* EQUIFAX REPORT, *supra* note 13, at VIII; *Hearings II*, *supra* note 30, at 46-47 (statement of Richard A. Barton, Senior Vice President, Gov't Affairs, Direct Marketing Assoc.).

Even with respect to the storage of personal information, businesses may find archival data is useful or needed at some unspecified time in the future. To the extent that such later uses do not raise privacy concerns, restrictions on the storage of personal information would impose unnecessary burdens on data processing activities. Similarly, the over-extensive collection of personal information may prove useful at a later time without implicating individuals' concerns regarding subsequent use or dissemination. As a result, businesses seek the flexibility to collect and maintain disclosed and transactional information of a broad nature.

246. *See* EQUIFAX REPORT, *supra* note 13, at VIII.

247. *See Hearings II*, *supra* note 30, at 103-04 (statement of Jerry Saltzgaber, C.E.O. of Citicorp Point-of-Sale Information Services); PRIVACY COMM'N, *supra* note 2, at 27-28.

248. In addition, some of the privacy concerns may be resolved through the use of technology. Recent disputes over caller identification and the Lotus/Equifax marketing database partly reflect inappropriate technological infrastructure decisions. Initial proposals for caller identification chose not to offer blocking functions. Similarly, the choice of CD-ROM for a marketing database containing personal information on

and dissemination of personal information is likely to be more troubling than the storage itself. The specific content of various types of personal information is also likely to affect the relative weight given to a particular concern. An individual may be more troubled by storage of a lifestyle profile than storage of bank account routing numbers. Similarly, the importance of a particular concern may depend on whether the personal information was disclosed by an individual, resulted from a transaction entered into by the individual, or became available through other means. For example, if an individual received a sizable electronic fund transfer, the recipient may be willing to share that information with a friend, but would be outraged if the bank disclosed the transaction record to a salesman or if the amount were deduced by a neighbor from other available records. On the other hand, an undisclosed collection of personal information may be more troubling if the information is obtained directly from an individual as compared to an acquisition of personal information from a public source. In addition, there may be further nuances or differences in the application of privacy concerns that are appropriate in the context of particular industries. The scope of consent to associated uses of personal information, for example, may be implicit in one context, but not in another.

While the public interest suggests that an articulated set of legal rights respond systematically to the plethora of privacy concerns, a purely general approach is likely to lead to difficulties balancing individual and commercial interests. Some means to accommodate both varying contexts for the processing of personal information and varying levels of concern may be necessary. European models offer an instructive view of some of these implementation difficulties. The basic principles espoused by the European Convention have proven ambiguous in a variety of specific data processing contexts, such as credit card processing, marketing and telecommunications. To clarify these ambigui-

---

shopping habits precluded erasure of unwilling participants and the correction of inaccurate personal information. Information networks may be structured to provide only the minimal amount of personal information necessary to accomplish a particular task and to delete personal information as soon as it is no longer needed. Encryption may also provide a means of assuring some anonymity as well as preventing unauthorized access to personal information.

ties, the Council of Europe has developed or issued recommendations on the interpretation of the European Convention in a number of private sector contexts,[249] including direct marketing,[250] employment relations,[251] and payments.[252] These recommendations, while not binding on treaty signatories or industry, reflect the difficulty of trying to apply general principles to rapidly changing information processing activities. The Commission of the European Communities has similarly explored industry applications for telecommunications services.[253]

The trend in more recent European national legislation also recognizes the complexity of the information economy and the need for greater flexibility. British law, for example, provides a set of general principles and recognizes particular industry applications for health and social work, financial services and education.[254] It also provides a number of exemptions for particular data processing activities such as payroll and accounts.[255] The Dutch law, while setting out broad privacy rights, allows industry groups to develop sectoral privacy codes.[256] When approved by the Dutch regulatory agency, these codes effectively provide a safe-harbor from prosecution for data processing activities that comply with the relevant code.

---

249. The European Convention established a Consultative Committee to make advisory opinions and recommendations on the application of these principles for particular situations. *See* European Convention, *supra* note 20, at arts. 18-19.

250. Council of Europe Recommendation R(85)(20) on the Protection of Personal Data used for Purposes of Direct Marketing (Oct. 25, 1985).

251. Council of Europe Recommendation R(89)(2) on the Protection of Personal Data used for Employment Purposes (Jan. 18, 1989).

252. Council of Europe Recommendation R(90)(19) on the Protection of Personal Data Used for Payment and other Related Operations (Sept. 13, 1990).

253. *See* Commission Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks, 1990 O.J. (C277), COM(90)314 final SYN 288 at 75.

254. *See* Data Protection Act of 1984, art. 29-30, 35 (Eng.), *reprinted in* NUGTER, *supra* note 15, at 380, 383.

255. Data Protection Act of 1984, art. 29-30, *reprinted in* NUGTER, *supra* note 15, at 381.

256. *See* Act of 28th December 1988 providing rules for the protection of privacy in connection with personal data files, Council of Eur. Doc. No. CJ-PD(89)4 §§ 15-16 (1989) [hereinafter Data Protection Act of 1988], *reprinted in* NUGTER, *supra* note 15, at 397-410. *See also* Peter Hustinx, *The Dutch Data Protection Bill*, PRIVACY L. & BUS. 11, 14 (Nov. 1988) (noting observation of Dutch Ministry of Justice Legal Advisor on Public law that "we wanted to differentiate according to sectors because these rules have to be applied to the specific problems of each sector.")

The implementation problems seen in Europe indicate that any new American framework should consider a flexible interpretive or application mechanism. Without a flexible means of applying and implementing any comprehensive rights, general principles will be unlikely to keep pace with new technologies and will be likely to hamper the development of new information services. The Dutch interpretive procedure offers one possible solution for guidance on rapidly evolving technologies and information processing activities.[257] In the Dutch example, principles applicable to all personal information processing may be adapted to particular contexts by industry experts.[258] For this type of framework to function in the United States, underlying legal rights will still need to be available.

In the United States, the development of a flexible mechanism raises further issues of regulatory process and enforcement. If underlying legal rights are elaborated for systematic application to information processing activities, one possible approach to assure flexibility for contextual differences may be the creation of a privacy board.[259] Such a board need not have power to issue detailed privacy regulations, but might be given authority to determine if industry codes of practice properly balance privacy and commercial needs and comply with the underlying rights. Without creating substantial bureaucracy, a board could promote consistent privacy guidance for industry and allow a clear safe-harbor for those information processing organizations complying with an approved industry-drafted code. Companies not in compliance with approved codes might then be subject to private or public enforcement actions. Without a safe-harbor, these entities would have a greater burden to prove that the elaborated legal rights were not violated. If the implementation mechanism that is ultimately chosen does not allow sufficient

257. *See also* Miller, *supra* note 1, at 1155 (arguing that "an attempt to achieve a workable balance between privacy and efficiency for any *particular* application of computer technology has little promise of success unless proper account is taken of the great variety of factors and relationships that tend to encourage computerization system interconnection and data sharing.").

258. *See* Data Protection Act of 1988, *supra* note 256, at § 15, *reprinted in* NUGTER, *supra* note 15, at 400.

259. *See supra* note 67 (discussion of the H.R. 3669 and H.R. 685 legislative initiatives).

flexibility, future technological advances may frustrate information privacy.

V. CONCLUSION

A host of privacy concerns arise from the commercial processing of personal information. These concerns relate to the full range of data processing activities. In the United States today, a narrow and haphazard collection of privacy rights protect individuals. These rights exist through industry-specific federal legislation, state common law doctrines and industry-specific state legislation. The rights do not respond coherently or consistently to data processing privacy concerns. In some contexts, the aggregation of rights responds clearly to isolated privacy concerns, yet in other contexts, there will be no available rights.

In light of the proliferation of information technologies and networks, the United States needs to re-evaluate the legal protection available to individuals. Some enforceable legal rights appear necessary and a flexible mechanism to interpret and implement these rights seems to be critical for the success of information privacy in the context of rapidly progressing technologies.