THE CHANGING FACE OF PRIVACY PROTECTION IN THE EUROPEAN UNION AND THE UNITED STATES

FRED H. CATE*

---

* Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington. Senior Counsel for Information Law, Ice Miller Donadio & Ryan.

I am grateful for the thoughtful comments of Professor Ronald J. Krotoszynski, Jr. that appear in this same issue. I agree entirely with his cautionary words about new technologies and the potential dangers of embracing them mindlessly. I commend to the reader his close analysis of cases, especially those involving the First Amendment, although it is clear that I disagree with some of the conclusions he draws from those cases. For example, all of the cases he puts forward as supporting government restraints on information involve *false* expression; I therefore question their predictive value for how the Supreme Court might evaluate a restriction on *true* speech. Similarly, the expression in commercial contexts, which he treats as lower value speech and therefore less worthy of protection under the First Amendment—as did the Court itself in the 1970s and 1980s—I believe is more likely to receive full First Amendment protection today, in light of the fundamental importance of such expression in most of our lives and the Court's repudiation of *Posadas*. *See* Posadas de Puerto Rico Assoc. v. Tourism Co. of Puerto Rico, 478 U.S. 328 (1986); 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 509 (1996) (holding that the decision in *Posadas* incorrectly performed First Amendment analysis by deferring to the legislature).

Even if, however, Professor Krotoszynski is correct that the Court might conclude that the First Amendment is not an obstacle to a ban on the collection or use of true, lawfully obtained information, my reading of the Constitution and the interests at stake leads me to conclude that the Court *should* not.

I disagree with Professor Krotoszynski's reading of the Takings Clause and recent Takings jurisprudence. Although the Takings Clause—unlike the First Amendment—is not central to my analysis of information privacy issues and why the government should proceed very cautiously before regulating information to address those issues, it is by no means clear that, as Professor Krotoszynski writes, "a state legislature could simply pass legislation declaring that no property interest accrues from the collection of personal information." Ronald J. Krotoszynski, Jr., *Identity, Privacy, and the New Information Scalpers: Recalibrating the Rules of the Road in the Age of the Infobahn*, 33 IND. L. REV. 233, 246 (1999). On the contrary, the Court's solicitude in *Ruckelshaus v. Monsanto Co.*,467 U.S. 986 (1984), for an entity's "reasonable investment-backed expectation with respect to its control over the use and dissemination of the data" I believe suggests that states would face significant constitutional hurdles if they were to attempt to prohibit outright the collection or use of data. *Id.* at 1011.

The assertion of Professor Krotoszynski's that I find most intriguing is his proposal that we eliminate the historical dividing line between the government and everyone else for purposes of regulating the collection and use of personal information. *See* Krotoszynski, *supra*, at 250-51. The special protection that applies to personal information in the hands of the government is justified on significant constitutional and practical grounds. The current structure of data protection is a trade-off: the government gets the power to compel disclosure of data; in exchange, it is subject to special restraints on its use of those data. To abolish that distinction, either by giving private parties government-like powers to compel citizens to disclose personal information or by weakening the privacy protections applicable to the government by extending them to private entities, seems to me profoundly unwise.

At heart, Professor Krotoszynski's arguments and mine differ most in terms of the vision they reflect. He writes of "abuses" and "confidential" data without defining what these are. If these terms refer to collecting information illegally, or distributing false and harmful data about an individual, or violating a promise concerning the use of personal information, then current law already provides significant penalties and I agree with him that it should. If, however, as I suspect, Professor Krotoszynski means something broader by these terms, then I do not share the vision that

INTRODUCTION

"Privacy" is the new hot topic in Washington and other national and state capitals as we head into the new millennium. The debate over privacy is reaching a fevered pitch as policymakers, public interest advocates, and industry leaders clash over how much is enough and over what role the government should play in protecting it. The U.S. Congress, after decades of virtually ignoring privacy issues, considered almost 1000 bills—one out of eight bills introduced—addressing some aspect of privacy in its 104th session. The 105th Congress debated an even broader array of privacy bills, ranging from identity theft[1] to collecting data from children,[2] confidentiality of health care records[3] to employers' use of credit reports,[4] privacy in banking[5] to privacy on the Internet.[6] Congress also held a series of hearings on privacy issues.[7] State legislatures were

---

something must be done. My vision is dominated instead by the benefits we all share of a society dominated by open information flows, the wide range of valuable services that such flows make available, the broad array of steps that the very technologies and markets that Professor Krotoszynski laments make available to me to protect my privacy, and fear of burdensome and costly government regulation to protect privacy, such as Europe now enjoys.

Our differences, however, and especially on such fundamental issues, highlight the issues involved in, and the importance of, the growing debate over information privacy. I am grateful to the editors of the *Indiana Law Review* for inviting me to participate in their symposium and to appear alongside Professor Krotoszynski, and I am grateful to Professor Krotoszynski for his insightful commentary. Finally, I want to thank my research assistant, Reid Cox, for his help with this article.

1. *See* Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, 112 Stat. 3007 (1998).

2. *See* Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

3. *See* S. 2609, 105th Cong. (1998); H.R. 3900, 105th Cong. (1998); H.R. 3605, 105th Cong. (1998); S. 1712, 105th Cong. (1998); S. 1921, 105th Cong. (1998); H.R. 52, 105th Cong. (1998); S. 1368, 105th Cong. (1998); H.R. 3756, 105th Cong. (1998); S. 1890 and S. 1891, 105th Cong., 2d Sess. (1998).

4. *See* Consumer Reporting Employment Clarification Act of 1998, Pub. L. No. 105-347, 112 Stat. 3208 (1998).

5. *See* H.R. 4388, 105th Cong. (1998); H.R. 4478, 105th Cong. (1998).

6. *See* H.R. 4667, 105th Cong. (1998); H.R. 98, 105th Cong. (1998); H.R. 2368, 105th Cong (1998); H.R. 4470, 105th Cong. (1998); Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

7. *See, e.g., Protection of Children's Privacy on the World Wide Web: Hearings on S. 2326 "Children's Online Privacy Protection Act of 1998" Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science & Transportation*, 105th Cong. (1998); *National ID Card: Hearings Before the Subcomm. on National Economic Growth, Natural Resources and Regulatory Affairs of the House Government Reform and Oversight*, 105th Cong. (1998); *Financial Information Privacy Act: Hearings Before House Comm. on Banking & Financial Services*, 105th Cong. (1998); *Electronic Commerce: Privacy in Cyberspace: Hearings*

no less attentive to privacy issues. In 1998, 2367 privacy bills were introduced or carried over in U.S. state legislatures; forty-two states enacted a total of 786 bills.[8]

The Federal Trade Commission has led a series of privacy-related initiatives, including a recently completed audit of web site privacy policies.[9] In addition, in 1998 the Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site.[10] The Commission has announced the conclusion of its second Internet privacy case, a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented the personal information collected from children, including information about family finances, would be maintained anonymously.[11] The Department of Commerce convened a major conference on privacy last summer, and the President, Vice President, and Secretary of Commerce have all threatened regulatory action to protect privacy if industry self-regulation does not improve. Privacy even made it into the President's 1999 State of the Union address.[12]

This debate is prompted largely by extraordinary technological innovations

---

Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce, 105th Cong. (1998); *Hearings on H.R. 2448 "Protection from Personal Intrusion Act" and H.R. 3224 "The Privacy Protection Act of 1998" Before the House Comm. on the Judiciary*, 105th Cong. (1998); *Privacy of Individual Genetic Information: Hearings Before the Senate Comm. on Labor and Human Resources*, 105th Cong. (1998); *Privacy Protection: Hearings on H.R. 2448 "Protection From Personal Intrusion Act" and H.R. 3224 "Privacy Protection Act of 1998" Before the House Comm. on the Judiciary*, 105th Cong. (1998); *Medical Privacy Protection: Hearings on H.R.52 "The Fair Health Information Practices Act" Before the Subcomm. on Government Management, Information and Technology of the House Comm. on Government Reform and Oversight*, 105th Cong. (1998); *Privacy in Electronic Communications: Hearings Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (1998).

8. *See Privacy Legislation in the States*, PRIV. & AM. BUS., Nov./Dec. 1998, at 1, 3.

9. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) (visited January 3, 2000) <http://www.ftc.gov/reports/privacy3/index.htm>.

10. *See* GeoCities, Docket No. C-3849 (Feb. 12, 1999) (Final Decision and Order available at <http://www.ftc.gov/os/1999/9902/9823015d&o.htm>).

11. *See* Liberty Financial, Case No. 9823522 (proposed consent agreement available at <http://www.ftc.gov/os/1999/9905/lbtyord.htm>).

12. "As more of our medical records are stored electronically, the threats to all our privacy increase. Because Congress has given me the authority to act if it does not do so by August, one way or another, we can all say to the American people, we will protect the privacy of medical records and we will do it this year." President William Jefferson Clinton, State of the Union Address (1999) <http://www.whitehouse.gov/WH/New/html/19990119-2656.html>.

that are dramatically expanding both the practical ability to collect and use personal data and the economic incentive to do so. Computers and the networks that connect them have become a dominant force in virtually all aspects of society in the United States and throughout the industrialized world. Information services and products today constitute the world's largest economic sector.[13] Institutions and individuals alike are flocking to the Internet—and particularly to the World Wide Web—in record numbers, making it the fastest-growing medium in human history.[14]

First made available to the public in 1992, the Web is used today by more than 147 million people and continues expanding at approximately thirty percent per year.[15] Much of the Web's explosive growth is due to the rapid increase in businesses online. In 1995, World Wide Web hosts designated ".com" for commercial uses slightly outnumbered those designated ".edu" for educational institutions, which were the historical backbone of the Internet. By January 1998, ".com" sites outnumbered their ".edu" counterparts more than two-to-one.[16]

The growth and commercialization of the Web are only two examples of a much larger trend. Computers, computer networks, and digital information increasingly dominate business, government, education and entertainment. Businesses are investing heavily in information technologies and increasingly taking advantage of new information services. Consider these examples:

- During the 1980s, U.S. businesses alone invested $1 trillion in information technology;[17] since 1990 they have spent more money on computers and communications equipment than on all other capital equipment combined.[18] This trend is reflected throughout the economy. Beginning in 1996, for example, U.S. consumers have purchased more computers each year than televisions.[19]
- A 1999 University of Texas study calculates that the Internet generated $301 billion in revenue in the United States last year, including $102 billion in

---

13. *See National Telecommunications and Information Administration Fact Sheet*, May 30, 1995, at 2.

14. Only five years after its creation, it reached more than 50 million homes in the United States. By comparison, it took 38 years for radio to reach 50 million U.S. homes, 13 for television, and 10 for cable.

15. *See The Big Picture Geographics* (visited Dec. 1, 1999) <http://cyberatlas. internet. com/big_picture/geographics/cia.html>.

16. *See Host Distribution by Top-Level Domain Names* (visited Dec. 1, 1999) <http://www.nw.com/zone/WWW-9501/dist-byname.html>; *Distribution by Top-Level Domain Name by Name* (visited Dec. 1, 1999) <http://www.nw.com/zone/WWW/dist-bynum.html>.

17. *See* Howard Gleckman, *The Technology Payoff*, BUS. WEEK, Jun. 14, 1993, at 57.

18. *See* Larry Irving, *Equipping Our Children with the Tools to Compete Successfully in the New Economy*, remarks to the Conference on Technology and the Schools: Preparing the New Workforce for the 21st Century, Randolph Center, VT, Oct. 28, 1996 <http://www.ntia.doc.gov.ntiahome/speeches/1028961i_vermont.html>.

19. *See id. See generally* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 5-7 (1997).

on-line sales. By comparison, the U.S. telecommunications industry accounted for $270 billion in revenue during the same period.[20]

- The Internet now carries twenty-five times more mail within the United States each day than the U.S. Post Office. The Electronic Messaging Association reports that about four trillion e-mails were received in the United States in 1998, up from two trillion in 1997. By contrast, the U.S. Postal Service handles about 160 billion letters and packages per year.[21]
- A Booz-Allen Hamilton study found that a single banking transaction costs $1.08 at a bank branch, sixty cents at an ATM machine, twenty-six cents with PC banking, but only thirteen cents on the Internet.[22]
- Alamo Rent-a-Car trimmed an estimated $1 million from its administrative budget by opening a Web site that lets tour operators tap directly into reservation and billing systems. Airlines are offering incentives for customers to book travel online, and many companies and government offices now handle procurement and manage relations with vendors exclusively online.[23]
- During first quarter 1997, Dell Computer Corporation sold more than $1 million of computers every day via the Internet. By the third quarter, that figure had risen to $3 million per day. Eighteen months later it is more than $14 million per day.[24]

As we see, the dominance of the Internet and of digital information generally is reflected clearly in the degree to which activities wholly unrelated to the provision or transmission of information—such as banking, insurance, air transportation, medicine, and even heavy industries like automobile production—are being transformed by information technologies.

The extraordinary role of information products and services and their transforming affect on virtually all aspects of human activity are certainly not limited to the United States. Currently 205 countries are connected to the Internet. Moreover, the U.S. share of Internet users is declining. According to studies by Computer Industry Almanac, Inc., in 1981 eighty percent of Internet users were in the United States; by 1994 that figure had fallen to sixty-five percent; and by the end of 1997, fifty-five percent of Internet users were in the United States.[25] One year later, the United States accounted for only fifty-two

---

20. *See The Internet Economy Indicators* (visited Dec. 1, 1999) <http://www.InternetIndicators.com>.

21. *See As E-Mail Grows Up, So Do the Uses for It*, GLOBE AND MAIL (Toronto), Oct. 13, 1998, at C2; *Notebook*, TIME, Jan. 25, 1999, at 15.

22. *See* Sharon Reier, *Battlelines Are Forming for Next "War of Wires,"* INT'L HERALD TRIB., Sept. 30, 1996.

23. *See* Clinton Wilder, *Big Businesses Head to Online Procurement*, TECHWEB NEWS, Nov. 23, 1998, at 1.

24. *See Dell Tops $18 Billion in Annual Revenue; Internet Sales Rise to $14 Million per Day; Company Announces 2-for-1 Stock Split*, BUS. WIRE, Feb. 16, 1999.

25. *See* Computer Industry Almanac Inc., *Top 15 Countries with the Most Internet Users* (visited Dec. 1, 1999) <http://www.c-i-a.com/199801pr.htm>.

percent of people worldwide who use the Internet at least once each week.[26] Finland, Norway, and Iceland all have higher per capita percentages of Internet users than the United States.[27]

The result of this extraordinary proliferation of computers and networks is that more data than ever before is made available in digital format, which is significant because digital information is easier and less expensive than nondigital data to access, manipulate, and store, especially from disparate, geographically distant locations. Also more data is generated in the first place because of the ease of doing so, the very low cost, and the high value of data in an increasingly information-based society. Data often substitutes for what would previously have required a physical transaction or commodity. In electronic banking transactions, for example, no currency changes hands, only data. And recorded data, such as a list of favorite web sites or an automatically generated back-up copy of a document, also makes the use of computers easier, more efficient, and more reliable. Finally, computer technologies and services often record a wide array of data necessary to complete a transaction or make its use more convenient, such as the web sites visited or the time and date an e-mail message is sent.

The ramifications of such a readily accessible storehouse of electronic information are astonishing: other people know more about you—even things you may not know about yourself—than ever before. Data routinely collected about you includes your health, credit, marital, educational, and employment histories; the times and telephone numbers of every call you make and receive; the magazines to which you subscribe and the books you borrow from the library; your cash withdrawals; your purchases by credit card or check; your electronic mail and telephone messages; and where you go on the World Wide Web.[28]

According to a 1994 estimate, U.S. computers alone held more than five billion records, trading information on every man, woman, and child an average of five times every day. Just one industry—credit reporting—accounted for 400 million credit files, which are updated with more than two billion entries every month.[29]

As a result, a growing number of citizens and lawmakers in the United States and around the world are concerned about protecting privacy. According to a June-July 1998 *Privacy & American Business*/Louis Harris survey, eighty-seven percent of the 1008 respondents reported being "concerned" or "very concerned" about personal privacy. Eighty-two percent said they had "lost all control over how personal information is circulated and used by companies," and sixty-one percent said that their privacy was not protected adequately by law or business

---

26. *See Latest Headcount: 148 Million Online* (visited Dec. 1, 1999) <http://cyberatlas.internet.com/big_picture/geographics/cia.html>.

27. *See* Computer Industry Almanac Inc., *15 Leading Countries in Internet Users Per Capita* (visited Dec. 1, 1999) <http://www.c-i-a.com/19980319.htm>.

28. *See* James Gleick, *Big Brother Is Us*, N.Y. TIMES, Sep. 29, 1996, at F1.

29. *See* 142 CONG. REC. S11,868 (Sep. 30, 1996) (statement of Sen. Bryan); Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J. L. & PUB. POL'Y 591, 593 (1994).

practices. Seventy-eight percent of respondents said that they had refused to give out personal information because of concern for their privacy.[30] A *Business Week*/Harris poll, released in March 1998, suggests that concern about privacy may be escalating. Seventy-eight percent of the 999 respondents said that they would use the Web more if privacy were better protected, and fifty percent of current Internet users responded that the government should pass laws now to regulate how personal data is collected and used on the Internet.[31] Surveys in other nations yield similar results.

As Marc Rotenberg, Director of the Washington-based Electronic Privacy Information Center, has observed: "Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century."[32]

Among the wide variety of national and multinational legal regimes for protecting privacy, two dominant models have emerged, reflecting two very different approaches to the control of information. The European Union ("EU") has enacted a sweeping data protection directive that imposes significant restrictions on most data collection, processing, dissemination, and storage activities, not only within Europe, but throughout the world if the data originates in a member state. The United States has taken a very different approach that extensively regulates government processing of data, while facilitating private, market-based initiatives to address private-sector data processing.

The interaction between these two systems is of far more than merely academic interest. The EU and the United States are each other's largest trading partners, with total trade and investment exceeding $1 trillion annually.[33] Moreover, information, especially digital information, is inherently global. Data ignores national and provincial borders, and, unlike a truckload of steel or a freight train of coal, data is difficult to pinpoint and almost impossible to block, through either legal or technological means. As a result, the laws applicable to information of one nation or group of nations inherently impact other nations; when nations pursue different legal regimes applicable to information, conflict between those laws is inevitable. In the case of the EU and the United States, that conflict implicates core values.

Under the EU data protection directive, information privacy is a basic human right; the failure of the U.S. legal system to treat it as such offends European values and has led the EU to threaten to suspend information flows to the United States. This threat is understandable in light of the directive's treatment of privacy as a human right, and the threat is necessary if the privacy of European nationals is to be protected effectively in a global information economy. In the United States, however, the government is constitutionally prohibited under the First Amendment from interfering with the flow of information, except in the

---

30. *See* P&AB *Survey Overview: Consensual Marketing Is Coming*, PRIV. & AM. BUS., Jan./Feb. 1999, at 1, 4-5.

31. *See* Heather Green et al., *A Little Privacy, Please*, BUS. WEEK, Mar. 16, 1998, at 98.

32. *Id; see generally* CATE, *supra* note 19, at 90.

33. *See* David L. Aaron, *Euro-age Bright for US Firms*, J. COMMERCE, Jan. 14, 1999, at 6A.

most compelling circumstances. The EU data protection directive is plainly contrary to that constitutional maxim, and the suggestion that the directive should be extended to the United States exacerbates that conflict, as well as threatens U.S. leadership in information technologies and services.

This Article examines the expanding conflict and emerging compromises between the EU and the United States over data protection. Part II briefly examines the requirements of the EU directive, particularly with regard to transborder data flows; the interpretative statements of European regulators about the directive's requirements; and implementation of the directive by member states. Part III examines the framework for privacy protection in the United States and the limits imposed on that framework by the Constitution. The Article concludes by addressing the conflict between the fundamental principles undergirding the European and U.S. systems of data protection, current political efforts to minimize that conflict, and the inadequacies of both systems in the context of the Internet.

I. EUROPEAN UNION

A. Data Protection Directive

Europe was the site of the first national privacy legislation, beginning with Sweden in 1973, and today virtually all European countries have broad privacy or data protection statutes.[34] Those statutes have been paralleled and, in some cases, anticipated by multinational action. In 1980 the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD)[35] issued *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*[36] The guidelines outline basic principles for both data protection and the free flow of information among countries that have laws conforming with the protection principles. The guidelines, however, have no binding force and permit broad variation in national implementation.

One year after the OECD issued its guidelines, the Council of Europe promulgated a convention *For the Protection of Individuals with Regard to*

---

34. In 1970 the German state of Hesse enacted the first data protection statute; Sweden followed in 1973 with the first national statute. Today, Austria, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom have broad privacy or data protection statutes. *See* CATE, *supra* note 19, at 32-34.

35. The OECD was founded in 1960 by 20 nations, including the United States, "to promote economic and social welfare throughout the OECD area by assisting member governments in the formulation and coordination of policies; to stimulate and harmonize members' aid efforts in favor of developing nations; and to contribute to the expansion of world trade." Robert C. Boehmer & Todd S. Palmer, *The 1992 EC Data Protection Proposal: An Examination of Its Implications for U.S. Business and U.S. Privacy Law*, 31 AM. BUS. L.J. 265, 271 n.33 (1993).

36. O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980).

Automatic Processing of Personal Data.[37] The Convention, which took effect in 1985, is similar to the Guidelines, although it focuses more on the importance of data protection to protect personal privacy.

The resulting protection for personal privacy was far from uniform, for at least four reasons. First, not all of the Council of Europe member states had adopted implementing legislation. In fact, by 1992, only ten countries—Austria, Denmark, France, Germany, Ireland, Luxembourg, Norway, Spain, Sweden, and the United Kingdom—had ratified the Convention, while eight—Belgium, Cyprus, Greece, Iceland, Italy, Netherlands, Portugal, and Turkey—had signed without ratification.[38] Second, some of the national data protection legislation existed prior to adoption of the Convention. Third, the Convention was not self-executing and therefore both permitted each country to implement its national laws conforming to the Convention's terms in very different ways and denied rights to citizens in those countries which had failed to ratify the convention. Finally, the Convention did not include definitions for important terms, such as what constitutes an "adequate" level of data protection; as a result, member countries were free to adopt inconsistent definitions in their national legislation.

As a result of the variation and uneven application among national laws permitted by both the guidelines and the convention, in July 1990, the Commission of the then-European Community published a draft *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[39] The draft directive was part of the ambitious program by the countries of the EU[40] to create not merely the "common market" and "economic and monetary union" contemplated by the Treaty of Rome,[41] but also the political union embodied in the Treaty on European Union signed in 1992 in Maastricht.[42]

The shift from economic to broad-based political union brought with it new attention to the protection of information privacy. On March 11, 1992, the European Parliament amended the commission's proposal to eliminate the distinction in the 1990 draft between public- and private- sector data protection and then overwhelmingly approved the draft directive. On October 15, 1992, the Commission issued its amended proposal; on February 20, 1995, the Council of

---

37. Eur. T.S. No. 108 (Jan. 28, 1981).

38. *See generally* Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORD. L. REV. S137, S143-48 (1992).

39. Com(92)422 final-SYN 287 (Oct. 15, 1992).

40. The 15 current members of the EU are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

41. Treaty Establishing the European Economic Community, Mar. 25, 1957, 28 U.N.T.S. 3, art. 2 (1958), as amended by the Single European Act, O.J. (L 169) 1 (1987), [1987] 2 C.M.L.R. 741, and the Treaty on European Union, Feb. 7, 1992, O.J. (C 224) 1 (1992), [1992] 1 C.M.L.R. 719, reprinted in 31 I.L.M. 247 (1992).

42. Treaty on European Union, Feb. 7, 1992, O.J. (C 224) 1 (1992), [1992] 1 C.M.L.R. 719, reprinted in 31 I.L.M. 247 (1992).

Ministers adopted a *Common Position with a View to Adopting Directive 94/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.*[43] The directive was formally approved on October 24, 1995, and took effect three years later.[44] On October 25, 1998, data protection law became significantly stronger throughout Europe.

The directive requires each of the fifteen EU member states to enact laws governing the "processing of personal data," which the directive defines as "any operation or set of operations," whether or not automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[45] "Personal data" is defined equally broadly as "any information relating to an identified or identifiable natural person."[46] This would include not only textual information, but also photographs, audiovisual images, and sound recordings of an identified or identifiable person, whether dead or alive.

As a practical matter, the directive does not apply in only two contexts: activities outside of the scope of Community law, such as national security and criminal law, and the processing of personal data that is performed by a "natural person in the course of a purely private and personal activity."[47]

National laws enacted in compliance with the directive must guarantee that "processing of personal data" is accurate, up-to-date, relevant, and not excessive. Personal data may be used only for the legitimate purposes for which they were collected and kept in a form that does not permit identification of individuals longer than is necessary for that purpose. Personal data may be processed only with the consent of the data subject, when legally required, or to protect "the public interest" or the "legitimate interests" of a private party, except when those interests are trumped by the "interests of the data subject."[48] The processing of personal data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life"[49] is severely restricted and in most cases forbidden without the written permission of the data subject.[50]

The directive requires member states to enact laws guaranteeing individuals access to, and the opportunity to correct, processed information about them. At a minimum, those laws must permit data subjects "to obtain, on request, at

---

43. 1995 O.J. (C 93) 1.

44. *See* Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 O.J. 95 (L281) [hereinafter *Directive 95/46/EC*].

45. *Id.* art. 2(b).

46. *Id.* art. 2(a).

47. *Id.* art. 3(2).

48. *Id.* art. 7.

49. *Id.* art. 8.

50. *See id.*

reasonable intervals and without excessive delay or expense, confirmation of the existence of personal data relating to them, communication to them of such data in an intelligible form, an indication of their source, and general information on their use."[51]

National laws under the directive must also permit data subjects to correct, erase or block the transfer of "inaccurate or incomplete data,"[52] and the opportunity to object at any time "on legitimate grounds" to the processing of personal data.[53] The directive requires that data subjects be offered the opportunity to have personal data erased without cost before they are disclosed to third parties, or used on their behalf, for direct mail marketing.

Data processors must inform persons from whom they intend to collect data, or from whom they have already collected data without providing this disclosure, of the purposes for the processing; the "obligatory or voluntary" nature of any reply; the consequences of failing to reply; the recipients or "categories of recipients" of the data; and the data subject's right of access to, and opportunity to correct, data concerning her.[54]

The directive requires that data processors—called "controllers" in the directive—notify the applicable national "supervisory authority" before beginning any data processing.[55] "Controller" is such a menacing term; under the directive, "controllers" include not only giant data processing companies, but also individuals who record the names and addresses of business contacts in their data organizers; students operating web sites which invite visitors to register; and neighborhood children who record orders for Girl Scout cookies.

Under the directive, member states' national laws must require that the notification include, at a minimum: the name and address of the controller; the purpose for the processing; the categories of data subjects; a description of the data or categories of data to be processed; the third parties or categories of third parties to whom the data might be disclosed; any proposed transfers of data to other countries; and a description of measures taken to assure the security of the processing. Controllers must also notify the supervisory authority of changes in any of the above information.

Each member state must establish an independent public authority to supervise the protection of personal data. Each "supervisory authority" must have, at minimum, the power to investigate data processing activities, including a right of access to the underlying data, as well as the power to intervene to order the erasure of data and the cessation of processing, and to block proposed transfer of data to third parties. The supervisory authority must also be empowered to hear complaints from data subjects and must issue a public report, at least annually, concerning the state of data protection in the country. The directive requires each supervisory authority to investigate data processing that

---

51. *Id.* art. 13(1).
52. *Id.* art. 14(3).
53. *Id.* art. 15(1).
54. *Id.* art. 11(1).
55. *Id.* art. 18(1).

"poses specific risks to the rights and freedoms of individuals."[56] Each supervisory authority is required to keep and make available to the public a "register of notified processing operations."[57]

The directive requires that member states' laws provide for civil liability against data controllers for unlawful processing activities, and provide "dissuasive" penalties for noncompliance with the national laws adopted pursuant to the directive.[58] In addition to requiring the supervisory authority to enforce those laws and to hear complaints by data subjects, the directive mandates creation of a "right of every person to a judicial remedy for any breach of the rights guaranteed by this Directive."[59]

Finally, and most central in ongoing U.S.-EU discussions about data protection and trade, Article 25 of the directive requires member states to enact laws prohibiting the transfer of personal data to non-member states that fail to ensure an "adequate level of protection,"[60] although member states are forbidden from restricting the flow of personal data among themselves because of data protection or privacy concerns.[61] The directive provides that the adequacy of the protection offered by the transferee country "shall be assessed in the light of all circumstances surrounding a data transfer," including the nature of the data, the purpose and duration of the proposed processing, the "rules of law, both general and sectoral," in the transferee country and the "professional rules and security measures which are complied with" in that country.[62]

The prohibition in Article 25 is subject to exemptions, provided in Article 26, when (1) the data subject has consented "unambiguously" to the transfer; (2) the transfer is necessary to the performance of a contract between the data subject and the controller or of a contract in the interest of the data subject concluded between the controller and a third party; (3) the transfer is legally required or necessary to serve an "important public interest"; (4) the transfer is necessary to protect "the vital interests of the data subject;" or (5) the transfer is from a "register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest. . . ."[63]

Because of the difficulty of separating data collected within Europe from data collected elsewhere, the directive effectively requires multinational businesses to conform all of their data processing activities to European law. Even businesses that do not operate in Europe may violate the directive if they collect, process, or disseminate personal data about European nationals or via multinational networks.

---

56. *Id.* art. 18(4).
57. *Id.* art. 21.
58. *Id.* arts. 23, 25.
59. *Id.* art. 22.
60. *Id.* art. 25(1).
61. *See id.* art. 25(2).
62. *Id.*
63. *Id.* art. 26(1).

Effective October 1998, these became the minimum levels of protection; individual states have the freedom to adopt more stringent protection.[64]

B. European Privacy Concepts and Principles

The EU data protection directive and national European data protection laws reflect at least eight broad, overlapping principles.

1. Purpose Limitation Principle.—The first principle of European data protection requires that information be collected only for specific and specified purposes, used only in ways that are compatible with those purposes, and stored no longer than is necessary for those purposes. An important corollary to the purpose limitation principle is that information unnecessary to those purposes should not be collected.[65]

2. Data Quality Principle.—The data quality principle requires that information be accurate and up-to-date.

3. Data Security Principle.—The data security principle requires that measures appropriate to the risks involved be taken to protect the security of data processing and transmission. The focus of this principle is not only to protect the physical data from "accidental or unlawful destruction or accidental loss," but also to ensure compliance with European laws prohibiting "unauthorized alteration or disclosure or any other unauthorized form of processing."[66]

4. Special Protection for Sensitive Data Principle.—The principle that special protection be provided for sensitive data requires that there be restrictions on, and special government scrutiny of, data collection and processing activities of information identifying "racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] concerning health or sexual life."[67] Under the directive, such data collection or processing is generally forbidden outright.

5. Transparency Principle.—Guaranteeing transparent processing of personal data requires that processing activities "be structured in a manner that will be open and understandable."[68] At minimum, this requires that individuals about whom personal information is to be collected be informed of that fact, the purposes for which the data will be used, and the identity of the person

---

64. Article 32 permits member states to delay compliance with the directive in two areas. First, member states may allow existing processing to continue under current rules for up to three years after the date on which the implementing national law or regulations come into effect. Second, member states may exempt the processing of data "already held in manual filing systems" from the application of most substantive provisions of the directive until as late as October 24, 2007. However, during the long transition to full coverage, individuals are to be allowed access to manual files concerning them, with the right to demand correction or deletion of inaccurate data. *See id.* art. 32.

65. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 13-14 (1996).

66. *Directive 95/46/EC*, *supra* note 44, art. 17(1).

67. *Id.* art. 8.

68. SCHWARTZ & REIDENBERG, *supra* note 65, at 15.

responsible for the data collection. In most cases, European law seems to indicate that consent must be obtained before personal information is collected or processed.

6. Data Transfers Principle.—The data transfer principle restricts authorized users of personal information from transferring that information to third parties without the permission of the data subject. In the case of transborder transfers, the directive prohibits data transfers outright to countries lacking an "adequate level of protection."[69]

7. Independent Oversight Principle.—The last two principles are closely related. The independent oversight principle requires that there be effective and independent oversight of data processing activities. At minimum, this seems to require that some authority have the power to audit data processing systems, investigate complaints brought by individuals, and enforce sanctions against noncomplying data processors. Under the directive, that oversight includes registration of all data processors and collection and processing activities. As a result, no person in Europe, other than an individual engaged in a "purely private and personal activity,"[70] may collect information that identifies specific individuals without the knowledge and permission of a national government.

8. Individual Redress Principle.—The individual redress principle requires that individuals have a right to access their personal information, correct inaccurate information, and pursue legally enforceable rights against data collectors and processors who fail to adhere to the law. This principle seems to require not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or a government agency to investigate and/or prosecute noncompliance by data processors. The directive would require that individuals have the opportunity to have recourse to independent government authorities empowered to investigate and prosecute complaints.

With these eight principles, the data protection directive marks the high-water mark of legal protection for information privacy. It is distinguished by its breadth in the data, activities, and geographic area to which it applies. It is very much a European product, reflecting the tenor of predecessor national data protection laws and the economic demand for a larger, more unified EU.

C. Interpretation of the Directive by the Article 29 Working Party

Article 29 of the EU directive created a "Working Party on the Protection of Individuals with regard to the Processing of Personal Data," charged with interpreting key portions of the directive.[71] The Working Party is composed of representatives from member states' data protection authorities and from the EU itself. Under Article 30, the Working Party is given broad responsibilities, including the power to "give the Commission an opinion on the level of

---

69. *Directive 95/46/EC*, *supra* note 44, art. 25(1).

70. *Id.* art. 3(2).

71. *See id.* art. 29.

protection in . . . third countries;" "on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community;" and "draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries."[72]

The Working Party met for the first time on January 17, 1996, and since that time, under the chairmanship of Peter J. Hustinx, President of the Dutch data protection authority, the Working Party has focused extensive attention on data transfers to non-European countries under Articles 25 and 26. The Working Party's conclusions to date are reflected in a series of working documents, which were reissued in July 1998 into a single document.[73]

1. Objectives.—The Working Party has identified three objectives that any data protection system must satisfy to comply with the directive's "adequacy" requirement:

> 1) deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterized by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.
> 2) provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.
> 3) provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.[74]

These three objectives focus on the availability of independent verification, investigation, and enforcement, and of compensation and other sanctions for failure to comply with substantive data protection obligations.

2. Substantive Rules.—The substantive rules identified by the Working Party as a precondition to a finding of "adequacy" include:

> 1) the purpose limitation principle—data should be processed for a

---

72. *Id.* arts. 30(1)(b), (3), (6).

73. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, WORKING DOCUMENT ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLES 25 AND 26 OF THE EU DATA PROTECTION DIRECTIVE (July 24, 1998) [hereinafter TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES].

74. *See id.*

specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. . . .

2) the data quality and proportionality principle—data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

3) the transparency principle—individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. . . .

4) the security principle—technical and organizational security measures, should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5) the rights of access, rectification and opposition—the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. . . .

6) restrictions on onward transfers—further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e., the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.[75]

According to the Working Party, certain types of data processing must be subject to additional controls. Those situations include:

1) sensitive data—where "sensitive" categories of data are involved [data concerning "racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] concerning health or sexual life"[76]] additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

2) direct marketing—where data are transferred for the purposes of direct marketing, the data subject should be able to "opt-out" from having his/her data used for such purposes at any stage.

---

75. *Id.*

76. *Directive 95/46/EC*, *supra* note 44, art. 8.

> 3) automated individual decision—where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.[77]

3. Self-regulation.—Recognizing that few if any other countries provide the level of statutory data protection that the EU data protection directive requires, the Working Party has addressed the extent to which extra-legal mechanisms—particularly industry self-regulation and private contracts—may satisfy the requirements of Article 25.

The Working Party has defined self-regulation as "any set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned."[78] The Working Party stressed that the standard for judging "adequacy" must continue to be the six substantive and three procedural requirements identified for evaluating data protection laws. Again, much of the Working Party's discussion of self-regulatory measures focused on the importance of assuring independent verification, investigation, and enforcement, and of providing compensation and other sanctions for failure to comply with substantive data protection obligations. For example, the Working Party has concluded that "remedial" sanctions are insufficient; "genuinely dissuasive and punitive" sanctions must also be available to provide an incentive for future compliance with self-regulatory standards. Similarly, the Working Party would require an "independent" arbiter or adjudicator, either "from outside the profession or sector concerned" or, if a body including industry representatives, including at least an equal number of "consumer representatives."[79]

4. Contracts.—As with self-regulation, the Working Party has stressed that for a contract to provide adequate data protection, it must comply with the nine principles identified above. This, the Working Party concludes, is "a major though not impossible challenge."[80] Because of the difficulties inherent in enforcing contractual terms for data protection on a party outside of the EU, the Working Party discusses in detail mechanisms for maintaining European oversight. "The preferred solution," according to the Working Party,

> would be for the contract to provide that the recipient of the transfer has no autonomous decision-making power in respect of the transferred data, or the way in which they are subsequently processed. The recipient is bound in this case to act solely under the instructions of the transferor, and while the data may have been physically transferred outside of the EU, decision-making control over the data remains with the entity who

---

77. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES, *supra* note 73.
78. *Id.*
79. *Id.*
80. *Id.*

> made the transfer based in the Community. The transferor thus remains the data controller, while the recipient is simply a sub-contracted processor. In these circumstances, because control over the data is exercised by an entity established in an EU Member State, the law of the Member State in question will continue to apply to the processing carried out in the third country, and furthermore the data controller will continue to be liable under that Member State law for any damage caused as a result of an unlawful processing operation.[81]

This describes few of the situations in which data are currently transferred from one country to another. However, the Working Party goes on to consider alternatives for maintaining European oversight over such transfers:

> • the transferor, perhaps at the moment of obtaining the data initially from the data subject, could enter into a separate contractual agreement with the data subject stipulating that the transferor will remain liable for any damage or distress caused by the failure of the recipient of a data transfer to comply with the agreed set of basic data protection principles.[82]
> • a member state could enact a national law specifying continuing liability for data controllers transferring data outside the Community for damages incurred as a result of the actions of the recipient of the transfer.[83]
> • a member state could require a contractual term which grants the supervisory authority of the member state in which transferor of the data is established a right to inspect, either directly or through an agent, the processing carried out by the processor in the third country.[84]
> • a standards body or specialist auditing firm could be required to provide external verification of the recipient's processing activities.[85]

Despite the availability of these and other alternatives, the Working Party is openly skeptical about the practicality of using contracts to provide for adequate data protection. The Working Party has stressed that "there remain significant doubts as to whether it is proper, practical, or indeed feasible from a resource point of view, for a supervisory authority of an EU Member State to take responsibility for investigation and inspection of data processing taking place in a third country."[86] In addition, all contracts with private parties are subject to the laws of the countries in which those parties are domiciled. A number of those laws may impose disclosure obligations (relating, for example, to tax regulations, securities and commodities rules, civil and criminal discovery orders) on private

---

81. *Id.* (footnotes omitted).
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*

parties that clearly trump any contractual obligations. The problem of such an overriding law "simply demonstrates the limitations of the contractual approach. In some cases a contract is too frail an instrument to offer adequate data protection safeguards, and transfers to certain countries should not be authorized."[87]

5. Exemptions.—Finally, the Working Party has stressed that the exemptions from the adequacy requirement, set forth in Article 26, are to be construed "restrictively." For example, the Working Party has concluded that for an individual to consent to the transfer of data concerning him or her to a country lacking adequate data protection, that consent must be unambiguous, freely given, specific to each proposed transfer, and informed, not just to the nature of the transfer but also as to the "particular risks" posed by each transfer.[88]

The Working Party's broad reading of Article 25's restriction on transborder transfers of personal data and its narrow reading of the exemptions to that restriction in Article 26 create a high standard for what constitutes "adequate" data protection.

D. Implementation of the Directive

The data protection directive—like all EU directives—requires that member states enact statutes transposing its terms into national law. Those national laws may offer greater, but not less, protection than the directive, but they may not impose any limits on the movement of data among member states. Those laws are interpreted in the first instance by national courts. However, because the laws are carrying out the requirements of a directive, the ultimate judicial interpreter of the national laws is the European Court of Justice. Members states which fail to comply by the effective date of the directive can be sanctioned by the EU. Moreover, in certain circumstances, the terms of the directive may come into force directly, so that citizens are not denied the protection guaranteed to them by the directive.

To date, only five EU member states—Greece, Italy, Portugal, Sweden, and the United Kingdom—have enacted national laws to comply with the directive, although laws are pending in most other member states.[89] Most of the other

---

87. *Id.*

88. *See id.*

89. THE SECOND ANNUAL REPORT OF THE EU WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, adopted on November 30, 1998, summarized progress towards implementing the directive in national legislation in other member states as follows:

> In Belgium, the Bill to transpose the directive, revised following the opinion of the Council of State, was submitted to Parliament in April 1998.
>
> In Denmark, the Bill was submitted on 30 April 1998, and Parliament finished its first reading in June.
>
> In Spain, the preliminary Bill amending current legislation on data protection (organic law 5/1992) was submitted to the Council of State for opinions and should be

member states are expected to have enacted laws transposing the directive by 2000, and it must be remembered that each of the member states which has not yet transposed the directive into national law nonetheless has an existing data protection law still in force.

In the five countries that have implemented the law to date, the newly adopted national data protection laws have included a number of provisions affecting both the substantive level of data protection in each country and the ease of complying with each country's laws, particularly with regard to transborder data flow. A quick survey of three of these laws provides a number of important examples.

Sweden's new Personal Data Protection Act, which was enacted on April 29,

---

discussed by Parliament during summer 1998; however, most of the provisions have already been transposed by the "Ley Organica" 5/1992 of 29 October 1992 on the automatic processing of personal data

In Germany, ... [t]he Ministry of Interior . . . submitted a bill on 1 December 1997, on which the Federal Data Protection Commissioner made comments on 30 January 1998. A new bill of 8 April 1998 has not been dealt with further because of the national election on 27 September 1998. Due to the constitutional principle of incontinuity of legislation, a new draft bill has to be submitted to the Parliament in the new legislative period. . . .

In France, a report was sent to the Prime Minister in March 1998 and will be followed by a new report on telematic networks. The French authority responsible for data protection, the Commission Nationale de l'Informatique et des Libertés (CNIL) will be consulted concerning the preliminary bill, which was not however available at the time of the drafting of this report.

In Ireland, the Justice Minister is responsible for legislation on data protection. The legislation necessary to apply the directive, which will include amendments to the law of 1988 on data protection, is being drafted. . . .

In Luxembourg, transposition of the directive into national law falls to the Ministry of Justice. A bill was drawn up in 1997, but was later withdrawn. A new bill will be examined by Parliament in September 1998.

The Netherlands government had announced its intention to replace the current law on data protection, in force since 1 July 1989, with an entirely new law on the same subject, in accordance with the provisions of the directive. On 16 February 1998, a bill was submitted to Parliament to that end. The relevant parliamentary subcommittee gave its opinion in June 1998, and the debate in plenary session is expected to take place before the end of this year.

The Austrian federal chancellery (Österreichisches Bundeskanzleramt) prepared a draft for transposition of the directive into national law, which was examined by the Council responsible for data protection; a revised version should be submitted to Parliament in autumn 1998. . . .

In Finland, an ad hoc committee responsible for the transposition of the directive (Henkilötietotoimikunta) completed its work in 1997. The bill was submitted to Parliament in July 1998. . . .

Id.

1998, and took effect on October 24, 1998, effectively abandons mandatory registration of data processing activities. After twenty-five years' experience with such a system—the longest in Europe—Sweden concluded that such registration was burdensome and unnecessary for effective protection of privacy rights. Instead, the new Swedish law allows data processors to avoid registration if they appoint a "personal data representative." The personal data representative, usually a lawyer, "shall have the function of independently ensuring that the controller of personal data processes personal data in a lawful and correct manner and in accordance with good practice and also points out any inadequacies to him or her."[90] The personal data representative must also help aggrieved data subjects seek resolution of their complaints with the data processor. Once the data processor has informed the supervisory authority of the name and address of its personal data representative, further recourse to the supervisory authority is necessary only if the personal data representative does not believe that the data processor is in compliance with the national law or cannot achieve successful resolution of a data subject's complaint. This provision promises to streamline the process of complying with the national law and effectively eliminate registration with the national authority as a condition of processing personal data.

Similarly, Sweden has determined to allow "research ethics committees"—Institutional Review Boards in the United States—at hospitals and universities to handle *all* data protection functions related to data involved in the studies and protocols those IRBs approve.[91] The national supervisory authority will effectively have *no* role with regard to such data, other than its judicial role (i.e., hearing complaints), thereby avoiding having data protection issues addressed by two separate regulatory authorities—the supervisory authority and an IRB.

At the same time, while Sweden has reduced the burden of complying with its national data protection law, it has also shown that it is serious about data protection. For example, the Swedish data protection commissioner, Anitha Bondestam, has required American Airlines to obtain the "explicit consent" of Swedish passengers before recording information concerning their meal preferences or requests for wheelchairs or other assistance in American's Sabre reservation system. Commissioner Bondestam reasoned that the data were especially sensitive because they could reveal health or religious information. American has lost two judicial appeals; the matter is now before the Swedish Supreme Court.[92]

Sweden's new law also prohibits outright the processing of personal data "concerning legal offences involving crime, judgments in criminal cases, coercive penal procedural measures or administrative deprivation of liberty" by

---

90. Swedish Personal Data Act (1998:204), art. 37.

91. *See id.* art. 19.

92. *See* American Airlines v. Sabre. Kammarrätan i Stockholm (Administrative Court of Appeals, Stockholm), Apr. 1997.

anyone other than a public authority.[93] However, the law exempts from this prohibition and most of its other substantive restrictions processing of personal data "exclusively for journalistic purposes or artistic or literary expression"—an exception that is far broader than that contained in the directive itself.[94]

Italy, by contrast, was a comparative latecomer to European-style data protection. However, in January 1997 Italy enacted a sweeping law implementing the directive—the Protection of Individuals and Legal Persons Regarding the Processing of Personal Data Act. This law, which took effect on May 8, 1997, defines "personal data" as "any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including by a personal identification number[.]"[95] This definition is broader than the directive's, which only applies to natural persons, and clearly encompasses even encrypted or anonymized data that "can be identified, even indirectly, by reference to any other information[.]"[96]

The Italian law specifies that consent for the processing of sensitive data must be in writing and that such processing must be specially authorized by the national government's supervisory authority which is a much broader restriction than that contained in the directive.[97] The law's disfavor for the processing of such personal data is further reflected in the provision specifying that if the supervisory authority fails to respond within thirty days to a request for authorization to process sensitive data, the request "shall be considered to have been dismissed."[98]

The Italian data protection law contains a stronger restriction on data export than that required by the directive. The law requires that the exporter notify the supervisory authority of any proposed transfer of data outside of EU member states, whether "temporarily or not, in any form, and by any means whatsoever," not less than fifteen days before the proposed transfer. Where sensitive data are involved, the notification is required for transfer even to other EU member states and must take place at least twenty days before the proposed transfer.[99]

As in the directive, transfers are prohibited to countries which do not provide adequate data protection. However, for transfers involving sensitive data, the law requires that the protection must be "equal to that ensured by Italian laws."[100] As a result, to transfer data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, . . . [or] concerning health or sex life," the transferor would have to demonstrate that the destination

---

93. Swedish Personal Data Act, *supra* note 90, art. 21.

94. *Id.* art. 7.

95. Protection of Individuals and Legal Persons Regarding the Processing of Personal Data Act (1998), art. 1(2)(c) (It.).

96. *Id.* art.

97. *See id.* art. 21.

98. *Id.* art. 22(2).

99. *See id.* arts. 28(1)-(2).

100. *Id.* art. 28(3).

country offers *equivalent*, not merely adequate, data protection. This was the language originally considered, but later rejected as too stringent, for the EU directive.

The United Kingdom's new Data Protection Act,[101] which received the Royal Assent on July 16, 1998, but is not expected to be brought into effect by the government until at least April 1999, is perhaps the most different of the five national laws transposing the directive. While Sweden, Italy, Greece, and Portugal enacted laws largely mirroring the broad style and structure of the directive—often referred to as "framework" legislation, because of the need for subsequent legislation or regulations to provide necessary detail—the United Kingdom adopted a lengthy, extraordinarily detailed law that leaves few questions unaddressed. Running to more than 100 pages and including seventy-five articles and sixteen schedules (four times longer than any of the other national laws), the U.K. law includes detailed provisions on all of the subjects covered by the EU data protection directive, as well as jurisdictional issues, the administration of the new law, and the interaction of various government offices. The law even includes specific sections on direct marketing and credit reports, and detailed exemptions from specific sections of the law for "national security," "crime and taxation," "health, education and social work," "regulatory activity," "journalism, literature and art," "research, history and statistics," "information available to the public or under enactment, "disclosures required by law or made in connection with legal proceedings etc.," "domestic purposes," and "miscellaneous exemptions;" the law empowers the Secretary of State to promulgate additional exemptions.[102]

The likely effect of this level of detail is not necessarily to change the level of protection afforded privacy, but rather to provide a statute that is difficult to understand without legal assistance, but that leaves fewer important matters to the discretion of the national supervisory authority.

As the examples of Sweden, Italy, and the United Kingdom suggest, the process of transposing the directive into national law introduces significant differences in the legal standards applicable to the processing of personal data in each member state. This is a far cry from the uniform data protection standards anticipated by the directive's proponents. These variations in protection are of comparatively minor concern to European data processors because the directive forbids outright one member state from interfering with the flow of personal data to another member state, no matter how much their national laws may differ. But the variety of national data protection standards heightens the concerns of non-European data processors, who anticipate having to comply separately with the national law of each member state from which they wish to export, or about whose citizens they process, personal data.

---

101. Data Protection Act, 1998 (1998 Chapter 29) (UK).

102. *Id.* arts. 28-38.

II. UNITED STATES

When compared with the omnibus, centralized data protection of the EU directive and member states' national laws, U.S. privacy protection stands in stark contrast and to some observers seems to pale altogether. The novelty and urgency of the recent surge of attention to privacy in the United States may appear to lend credence to this view. This section addresses the extent of privacy protection in the United States by first surveying the major legal protections for privacy, and then considering the principles that both undergird that protection and impose limits on it.

A. Constitutional Framework

In the United States, there is no explicit constitutional guarantee of a right to privacy. The Supreme Court, however, has interpreted many of the amendments constituting the Bill of Rights to provide some protection to a variety of elements of individual privacy against intrusive government activities.[103]

None of these provisions refer to privacy explicitly, and the circumstances in which privacy rights are implicated are as widely varied as the constitutional sources of those rights. Moreover, it must be remembered that constitutional rights protect only against state action and are generally "negative" in nature.[104] As a result, any constitutional concept of "privacy" applies only against the government and at most requires that the government refrain from taking actions which impermissibly invade privacy.

1. Expression, Association, and Religion.—The Court has identified a number of privacy interests implicit in the First Amendment.[105] In *NAACP v. Alabama*,[106] the U.S. Supreme Court struck down an Alabama ordinance requiring the NAACP to disclose its membership lists, finding that such a requirement constituted an unconstitutional infringement on NAACP members' First Amendment right of association.[107] In *Breard v. City of Alexandria*,[108] the Court upheld an ordinance prohibiting solicitation of private residences without

---

103. *See* CATE, *supra* note 19, at 49-66.

104. Only the Thirteenth Amendment, which prohibits slavery, applies to private parties. *See* Clyatt v. United States, 197 U.S. 207, 216-220 (1905). Although state action is usually found when the state acts toward a private person, the Supreme Court has also found state action when the state affords a legal right to one private party which impinges on the constitutional rights of another, *see* New York Times Co. v. Sullivan, 376 U.S. 264, 265 (1964), and in rare cases when a private party undertakes a traditionally public function, *see* Marsh v. Alabama, 326 U.S. 501 (1946), or when the activities of the state and a private entity are sufficiently intertwined to render the private parties' activities public, *see* Evans v. Newtown, 382 U.S. 296 (1966).

105. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceable to assemble . . . ." U.S. CONST. amend. I.

106. 357 U.S. 449 (1958).

107. *See id.* at 464-65.

108. 341 U.S. 622 (1951).

prior permission. The Court found in the First Amendment's free speech guarantee an implicit balance between "some householders' desire for privacy and the publisher's right to distribute publications in the precise way that those soliciting for him think brings the best results."[109] The Court has invoked this same implied balancing test is numerous other cases. In *Kovacs v. Cooper*,[110] the Court upheld a Trenton, New Jersey, ordinance prohibiting the use of sound trucks and loudspeakers:

> The unwilling listener is not like the passer-by who may be offered a pamphlet in the street but cannot be made to take it. In his home or on the street he is practically helpless to escape this interference with his privacy by loudspeakers except through the protection of the municipality.[111]

In *Rowan v. U.S. Post Office*,[112] the Court upheld a federal statute which permitted homeowners to specify that the Post Office not deliver to their homes "erotically arousing" and "sexually provocative" mail.[113] In *Federal Communications Commission v. Pacifica Foundation*,[114] the Court allowed the Federal Communications Commission to sanction a radio station for broadcasting "indecent" programming, finding that "the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder."[115] In *Frisby v. Schultz*,[116] the Court upheld a Brookfield, Wisconsin statute that banned all residential picketing, writing that the home was "the one retreat to which men and women can repair to escape from the tribulations of their daily pursuits"[117] and "the last citadel of the tired, the weary, and the sick."[118] In *Carey v. Brown*,[119] the Court wrote that "the State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society."[120]

Although the Court rarely specifies the source of these privacy rights, it treats them as values implicitly balanced with the First Amendment right to free

---

109. *Id.* at 644.
110. 336 U.S. 77 (1949).
111. *Id.* at 86-87.
112. 397 U.S. 728 (1970).
113. *Id.* at 729-30.
114. 438 U.S. 726 (1978).
115. *Id.* at 748.
116. 487 U.S. 474 (1988).
117. *Id.* at 484 (quoting Carey v. Brown, 447 U.S. 455 (1980)).
118. *Id.* (quoting Gregory v. City of Chicago, 394 U.S. 111, 125 (1969) (Black, J., concurring)).
119. 447 U.S. 455 (1980). The Court in *Carey* struck down the Illinois ordinance at issue that prohibited residential picketing, on the grounds that the ordinance excluded labor picketing. *See id.* at 470.
120. *Id.* at 471.

expression. In *Stanley v. Georgia*,[121] however, the Court explicitly linked privacy and free expression by identifying the mutual interests that they serve. The Court overturned a conviction under Georgia law for possessing obscene material in the home. While the "States retain broad power to regulate obscenity," Justice Marshall wrote for the unanimous Court, "that power simply does not extend to mere possession by the individual in the privacy of his own home."[122] The Court based its decision squarely on the First Amendment, which the Court found included the "right to be free, except in very limited circumstances, from unwanted governmental intrusion into one's privacy."[123] The Court concluded: "If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."[124]

2. Searches and Seizures.—Most of the Supreme Court's jurisprudence concerning a constitutional right to privacy has centered on the Fourth Amendment's prohibition on unreasonable searches and seizures.[125] This prohibition reflects two deeply rooted concerns: that citizens' property be protected from seizure by the government and that citizens' homes and persons be protected from warrantless or arbitrary searches. These concerns are reflected in the Declaration of Independence and many of the colonial debates and writings, as well as in the Constitution. In 1886, the Supreme Court first applied the term "priva[cy]" to the interests protected by the Fourth Amendment.[126] Four years later, Supreme Court Justice Louis Brandeis joined forces with Samuel Warren to articulate "The Right to Privacy" in the *Harvard Law Review*.[127] Justice Brandeis boldly stated his views on privacy in his 1928 dissent in *Olmstead v. United States*.[128] Five of the nine justices had found that wiretapping of telephone wires by federal officials did not constitute a search or seizure because there had been no physical trespass and nothing tangible had been taken. Justice Brandeis wrote:

---

121. 394 U.S. 557 (1969).

122. *Id.* at 568.

123. *Id.* at 564.

124. *Id.* at 565.

125. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

126. Boyd v. United States, 116 U.S. 616, 625-26 (1886).

127. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

128. 277 U.S. 438 (1928).

> The protection guaranteed by the [Fourth and Fifth[129]] Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[130]

Almost forty years later, the Court adopted Justice Brandeis' reasoning in *Katz v. United States*.[131] The case addressed the constitutionality of federal authorities' use of an electronic listening device attached to the outside of a telephone booth used by Charles Katz, who the authorities suspected of violating gambling laws. The Court found that this method of gathering evidence infringed on Katz' Fourth Amendment rights, even though his property had not been invaded.[132] The Court found that the Constitution protects whatever one "seeks to preserve as private, even in an area accessible to the public. . . ."[133] In his concurrence, Justice Harlan introduced what was later to become the Court's test for what was "private" within the meaning of the Fourth Amendment.[134] Justice Harlan wrote that the protected zone of Fourth Amendment privacy was defined by the individual's "actual," subjective expectation of privacy, and the extent to which that expectation was "one that society was prepared to recognize as 'reasonable.'"[135] The Court adopted that test in 1968 and continues to apply it today, with somewhat uneven results.[136] The Court has found "reasonable" expectations of privacy in homes, businesses, sealed luggage and packages, and even drums of chemicals, but no "reasonable" expectations of privacy in bank records, voice or writing samples, phone numbers, conversations recorded by concealed microphones, and automobile passenger compartments, trunks, and

---

129. "No person shall . . . be deprived of life, liberty, or property, without due process of law . . ." U.S. CONST. amend. V.

130. *Olmstead*, 277 U.S. at 478-79 (Brandeis, J., concurring).

131. 389 U.S. 347 (1967).

132. *See id.* at 353.

133. *Id.* at 351.

134. *See id.* at 360-61 (Harlan, J., concurring).

135. *Id.* at 361 (Harlan, J., concurring).

136. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).

glove boxes.[137]

3. Fundamental Decision-making.—The U.S. Supreme Court's most controversial constitutional right to privacy has developed within a series of cases involving decisionmaking about contraception, abortion, and other profoundly personal issues. In 1965, the Court decided in *Griswold v. Connecticut*[138] that an eighty-year-old Connecticut law forbidding the use of contraceptives violated the constitutional right to "marital privacy."[139] Justice Douglas, writing for the Court, offered a variety of constitutional loci for this right:

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one. . . . The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[140]

But the Court could not specifically identify a constitutional basis for the right to marital privacy. Instead, Justice Douglas wrote that the "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."[141] It was in these "penumbras, formed by emanations" that the Court grounded this new right.[142]

Eight years later, the Court extended this privacy right in *Roe v. Wade*[143] to encompass "a woman's decision whether or not to terminate her pregnancy."[144] Rather than base that right, directly or indirectly, on one or more of the specific guarantees of the Bill of Rights, the Court looked instead to "the Fourteenth Amendment's concept of personal liberty and restrictions upon state action. . . ."[145] Notwithstanding this broad foundation, however, the Court in *Roe*

---

137. *See* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1368-70 (1992).

138. 381 U.S. 479 (1965).

139. *Id.* at 485-86.

140. *Id.* at 484.

141. *Id.*

142. *Id.*

143. 410 U.S. 113 (1973).

144. *Id.* at 153.

145. *Id.* The Fourteenth Amendment provides, in relevant part: "No State shall make or enforce any law which shall . . . deprive any person of life, liberty, or property, without due process of law. . . ." U.S. CONST. amend. XIV, § 1.

found that the constitutional "guarantee of personal privacy" only includes "personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty'. . . ."[146] The Court specified that those fundamental rights include activities concerning marriage, procreation, contraception, family relationships, and child rearing and education.[147] Government regulation of those activities "may be justified only by a 'compelling state interest,'" and they must be "narrowly drawn to express only the legitimate state interests at stake."[148]

Although the Supreme Court indicated that government intrusion into inherently private areas of personal life would be subject to strict scrutiny, the Court has limited the scope of what it considers "private." In 1988, in *Bowers v. Hardwick*,[149] the Court declined to extend the right of privacy to the interests of homosexuals to engage in sodomy within their homes. The following year, in *Webster v. Reproductive Health Services*,[150] the Court upheld a Missouri statute imposing significant limitations on performing abortions, including an outright ban on the use of public funds, employees, or facilities to perform abortions not necessary to save the mother's life or to counsel a woman to have such an abortion. Chief Justice Rehnquist, writing for a five-justice plurality of the Court, argued that the privacy interest at issue was merely "a liberty interest protected by the Due Process Clause" and not a "fundamental" constitutional right.[151] As Laurence Tribe has written, the reasoning in *Webster* suggests that a woman's "right" to an abortion is "apparently no different from her 'right' to drive a car, say, or open a store, or work as a dentist."[152]

4. Nondisclosure.—Although the Court has identified constitutional privacy interests in a variety of settings, the area most likely to be applicable to the interest of individuals in information privacy has arisen in a series of cases involving nondisclosure of sensitive information. In 1977, the Supreme Court decided *Whalen v. Roe*.[153] *Whalen* involved a challenge to a New York statute requiring that copies of prescriptions for certain drugs be provided to the state. The Court held that the requirement would infringe upon patients' privacy rights.[154] In his opinion for the unanimous Court, Justice Stevens wrote that the constitutionally protected "zone of privacy" included two separate interests: "the interest in independence in making certain kinds of important decisions" and "the individual interest in avoiding disclosure of personal matters . . . ."[155] The first

---

146. *Roe*, 410 U.S. at 152 (quoting Palko v. Connecticut, 302 U.S. 319, 325 (1937)).
147. *See id.* at 152-53.
148. *Id.* at 155.
149. 478 U.S. 186 (1986).
150. 492 U.S. 490 (1989) (plurality opinion).
151. *Id.* at 520.
152. LAURENCE H. TRIBE, ABORTION: THE CLASH OF ABSOLUTES 23 (1990).
153. 429 U.S. 589 (1977).
154. *See id.* at 603-04.
155. *Id.* at 599-600.

interest is clearly grounded in *Roe v. Wade*,[156] *Griswold v. Connecticut*,[157] and similar cases, to which Justice Stevens cited. The second interest appears to be a new creation of the *Whalen* Court, although based on the "Fourteenth Amendment's concept of personal liberty" identified in *Roe*.[158] Nevertheless, having found this new privacy interest in nondisclosure of personal information, the Court did not apply strict scrutiny, apparently because the interest was not a right involving a "fundamental" interest. Instead, the court applied a lower level of scrutiny, and held that the statute did not infringe the individuals' interest in nondisclosure.[159]

Likewise, federal appellate courts in the Second, Third, Fifth, and Ninth Circuits have reached similar results, finding a constitutional right of privacy in individuals not being compelled by the government to disclose personal information, particularly medical records.[160] However, by extending the right of nondisclosure beyond fundamental rights, these courts have applied a lower standard of scrutiny than that applicable in cases involving marriage, procreation, contraception, family relationships, and child rearing and education. Instead of strict scrutiny, these courts used intermediate scrutiny:

> The government may seek and use information covered by the right to privacy if it can show that its use of the information would advance a legitimate state interest and that its actions are narrowly tailored to meet the legitimate interest. The more sensitive the information, the stronger the state's interest must be.[161]

Courts in the Fourth and Sixth Circuits, however, have severely limited the scope of the *Whalen* nondisclosure privacy right. In 1993, the Court of Appeals for the Fourth Circuit decided *Walls v. City of Petersburg*.[162] *Walls* involved a city employee's claim that her dismissal for refusing to answer an official questionnaire violated her constitutional right to nondisclosure. The employee particularly objected to Question 40, which asked "Have you ever had sexual relations with a person of the same sex?"[163] The appellate court, while acknowledging that the "relevance of this question to Walls' employment is uncertain," nonetheless found that "Question 40 does not ask for information that

---

156. 410 U.S. 113, 153 (1973).

157. 381 U.S. 479, 485-86 (1965).

158. *Whalen*, 429 U.S. at 598 n.23.

159. *See id.* at 603-04. The Court also explicitly rejected the application of the Fourth Amendment right of privacy, writing that Fourth Amendment cases "involve affirmative, unannounced, narrowly focused intrusions." *Id.* at 604 n.32.

160. *See* Doe v. Southeastern Pa. Transp. Auth., 72 F.3d 1133 (3d Cir. 1995); Doe v. Attorney General, 941 F.2d 780 (9th Cir. 1991); Barry v. City of New York, 712 F.2d 1554 (2d Cir. 1983); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); Schacter v. Whalen, 581 F.2d 35, 37 (2d Cir. 1978); Plante v. Gonzalez, 575 F.2d 1119 (5th Cir. 1978).

161. *Doe*, 941 F.2d at 796 (citations omitted).

162. 895 F.2d 188 (4th Cir. 1990).

163. *Id.* at 190.

Walls has a right to keep private."[164] The court reasoned that because the Supreme Court had found no fundamental right to *engage* in homosexual acts, there could be no constitutional right not to disclose such practices.[165] The Court of Appeals for the Sixth Circuit has similarly restricted the right not to disclose personal information to information concerning fundamental rights.[166]

5. The Limits of Constitutional Protections for Privacy.—

a. First Amendment.—While the Constitution affords substantial protection for personal privacy from invasion by the government, it affords effectively no protection for privacy from interference by private parties and it even restricts the government's efforts to create statutory, regulatory, or common law tools for protecting privacy from non-governmental intrusion. In short, the Constitution is the source not only of privacy rights, but also of other significant rights against which all government efforts—treaty commitments, statutes, regulations, administrative and executive orders, and daily functions—must be measured. One of the most important of these rights, the one most often implicated by government efforts to protect privacy, and one of the most distinct products of U.S. history and culture, is the First Amendment restraint on government abridgement of freedom of expression or of the press.[167] Any effort by the government to protect privacy, whether through direct regulation or the creation or enforcement of legal causes of action among private parties, must be consonant with the First Amendment if that protection is to survive constitutional review.

This tension between the First Amendment as protecting privacy and as prohibiting the government from restricting expression in order to protect privacy runs throughout First Amendment jurisprudence. Ken Gormley has written that over time, "the First Amendment came to be viewed as possessing two distinct hemispheres."[168] One was the traditional freedom to speak and associate without governmental interference. The other was "the less familiar freedom of the citizen to think and engage in private thoughts, free from the clutter and bombardment of outside speech."[169] Neither yields any significant protection for privacy, beyond that already implicit in the First Amendment's guarantees to speak, associate, and worship without governmental interference.

The association and expression cases clearly suggest the recognition of a constitutional right of privacy, in the sense of solitude or seclusion from intrusion, based on the First Amendment. That right is necessarily limited, however, to restricting the conduct of government and the government's creation of legal rights that private parties might use to interfere with the privacy of others. Moreover, case law recognizing the right is relatively overshadowed by

---

164. *Id.* at 193.

165. *See id.*

166. *See* J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981) (disseminating juveniles' social histories prepared by state probation officers does not violate privacy rights).

167. *See* U.S. CONST. amend. I.

168. Gormley, *supra* note 137, at 1381.

169. *Id.*

cases indicating that the right carries little weight when balanced against other, explicit constitutional rights, especially in situations involving activities outside of the private home. For instance, the Court has accorded privacy rights little protection when confronted with freedom of association claims of groups such as the American Communist Party.[170] The Court often has overturned ordinances restricting door-to-door solicitation with little if any comment on the privacy interests of the occupants.[171]

Similarly, the Court has often demonstrated little concern for the privacy interests of unwilling viewers or listeners, rejecting claims against broadcasts of radio programs in Washington, D.C. streetcars,[172] R-rated movies at a drive-in theater in Jacksonville, Florida,[173] and a jacket bearing an "unseemly expletive" worn in the corridors of the Los Angeles County Courthouse.[174] Moreover, plaintiffs rarely win suits brought against the press for disclosing private information. When information is true and obtained lawfully, the Supreme Court repeatedly has held that the state may not restrict its publication without a showing that the government's interest in doing so is "compelling" and that the restriction is no greater than is necessary to achieve that interest.[175] This is "strict scrutiny," the highest level of constitutional review available in the United States. Protection of privacy rarely constitutes a sufficiently compelling interest to survive strict scrutiny. Even if information published by the press is subsequently proved to be false, the Supreme Court has demonstrated extraordinary deference to the First Amendment expression rights of the press and little concern for the privacy interests involved.[176]

In fact, when privacy rights conflict with free expression rights before the Court, the latter prevail, virtually without exception. Under the Court's strict scruting requirement, it has struck down laws restricting the publication of confidential government reports,[177] and of the names of judges under investigation,[178] juvenile suspects,[179] and rape victims.[180] The dominance of the free expression interests over the privacy interests is so great that Peter Edelman

---

170. *See* Noto v. United States, 367 U.S. 290 (1961); Scales v. United States, 367 U.S. 203 (1961); Communist Party v. Subversive Activities Control Bd., 367 U.S. 1 (1961).

171. *See, e.g.*, Staub v. City of Baxley, 355 U.S. 313 (1958); Schneider v. State, 308 U.S. 147 (1939); Lovell v. City of Griffin, 303 U.S. 444 (1938).

172. *See* Public Util. Comm'n v. Pollack, 343 U.S. 451 (1952).

173. *See* Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975).

174. *See* Cohen v. California, 403 U.S. 15 (1971).

175. *See, e.g.*, Florida Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979); Landmark Communications Inc. v. Virginia, 435 U.S. 829 (1978); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).

176. *See, e.g.*, Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988); Time, Inc. v. Hill, 385 U.S. 374 (1967).

177. *See* New York Times Co. v. United States, 403 U.S. 713 (1971).

178. *See Landmark Communications, Inc.*, 435 U.S. at 829.

179. *See Smith*, 443 U.S. at 97.

180. *See Florida Star*, 491 U.S. at 524; *Cox Broad. Corp.*, 420 U.S. at 469.

has written:

> [T]he Court [has] virtually extinguished privacy plaintiffs' chances of recovery for injuries caused by truthful speech that violates their interest in nondisclosure. . . . If the right to publish private information collides with an individual's right not to have that information published, the Court consistently subordinates the privacy interest to the free speech concerns.[181]

This is true irrespective of whether the speaker is an individual or an institution. Even wholly commercial expression is protected by the First Amendment. The Court has found that such expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a "substantial" public interest, and that the intrusion "directly advances" that interest and is "narrowly tailored to achieve the desired objective."[182] The Court does not characterize expression as "commercial," and therefore subject government regulations concerning it to this "intermediate scrutiny," just because it occurs in a commercial context. The speech of corporations is routinely accorded the highest First Amendment protection—"strict scrutiny" review—unless the Court finds that the purpose of the expression is to propose a commercial transaction[183] or that the expression occurs in the context of a regulated industry or market (such as the securities exchanges) and concerns activities which are, in fact, being regulated (the sale of securities).[184]

Any governmental effort to protect privacy from intrusion by non-governmental entities, either directly or through the passage or enforcement of laws permitting suits by private parties, faces significant First Amendment obstacles. This is particularly true when the privacy protection would apply to information concerning government activities and the qualifications and behavior of government officials, or would restrict access on the basis of the content of the material to be protected.

b. Fifth Amendment.—The Fifth Amendment to the U.S. Constitution prohibits the government from taking private property for public use without both due process of law and just compensation.[185] Historically, the Supreme Court has applied the "Takings Clause" to require compensation when the government physically appropriated real property, even if only a tiny portion of the property

---

181. Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195, 1198 (1990).

182. Board of Trustees v. Fox, 492 U.S. 469, 480 (1989); Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 (1980).

183. *See Central Hudson*, 447 U.S. at 562.

184. *See* Lowe v. Securities & Exch. Comm'n, 472 U.S. 181 (1985).

185. "No person shall . . . be deprived of life, liberty, or property, without due process of law, nor shall private property be taken for public use, without just compensation." U.S. CONST. amend. V.

at issue was occupied[186] or if that occupation was only temporary.[187] Beginning in 1922, however, the Court has found a compensable taking even when the government does not engage in physical occupation[188] and when the property involved is not land or even tangible, corporeal property, but rather a legal entitlement,[189] government benefit,[190] or interest in continued employment.[191] In 1984, the Court decided *Ruckelshaus v. Monsanto Co.*,[192] which extended the Fifth Amendment's Takings Clause to protect stored data.

The Supreme Court's recognition of these "regulatory takings"—including takings of stored data—suggests that privacy regulations that substantially interfere with a private party's use of data that she has collected or processed, may require compensation under the Fifth Amendment. In *Ruckelshaus*, the Supreme Court found that the Environmental Protection Agency's use of plaintiff's proprietary research data constituted a compensable taking.[193] As in all regulatory takings cases, the Court in *Ruckelshaus* faced two fundamental questions: whether there was "property" and, if so, whether it was "taken" by the government's action.[194] The first question presented little difficulty because state law recognizes a property right in "trade secrets" and other confidential business information, and the possessors of such data have long been accorded property-like rights to control access to, and the use of, business information.[195] To answer the second question, the Court focused on Monsanto's "reasonable investment-backed expectation with respect to its control over the use and dissemination of the data,"[196] finding that Monsanto had invested substantial resources in creating the data and reasonably believed that they would not be disclosed by the EPA.

To be certain, not all regulations of private property constitute takings. Although the Court has put forward a number of tests for determining when a

---

186. *See* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419 (1982) (involving only 1.5 cubic feet of private property occupied).

187. *See* First English Evangelical Lutheran Church v. County of Los Angeles, 482 U.S. 304 (1987) (ordering just compensation where plaintiff was denied use of its property for six years).

188. *See* Pennsylvania Coal Co. v. Mahon, 260 U.S. 393 (1922) (holding that state abrogated right to remove coal from property).

189. *See, e.g.*, Logan v. Zimmerman Brush Co., 455 U.S. 422 (1982) (holding that there was property interest in statutorily created cause of action for discrimination against the disabled); United States Trust Co. v. New Jersey, 431 U.S. 1 (1977) (finding a property interest in common law contract rights).

190. *See, e.g.*, Mathews v. Eldridge, 424 U.S. 319 (1976) (holding that there exists a property interest in Social Security benefits).

191. *See, e.g.*, Perry v. Sindermann, 408 U.S. 593 (1972) (finding a property interest exists in continued employment).

192. 467 U.S. 986 (1984).

193. *See id.* at 1013.

194. *See id.* at 1000.

195. *See id.* at 1003.

196. *Id.* at 1011.

regulatory taking occurs, the common element in them all is that a taking occurs when the government's regulation "denies an owner economically viable use" of his property.[197] In the classic formulation of property rights as a bundle of sticks, a taking may exist where the government eliminates any one of those sticks, but a taking is certain to exist when the government effectively seizes the entire bundle by eliminating all of the sticks.

Even when a government regulation deprives a property owner of all use of his property, the Supreme Court has historically declined to find a taking, and therefore not required compensation, when the regulation merely abated a "noxious use" or "nuisance-like" conduct. Such a regulation does not constitute a taking of private property, because one never has a property right to harm others.[198] In 1992, however, the Supreme Court backed away from this "prevention of harmful use" exception, recognizing that the government could virtually always claim that it was regulating to prevent a harmful use.[199] Instead, the Court now requires that when a government regulation deprives property "of all economically beneficial use," the government must show that the power to promulgate the regulation inhered in the "background principles of the State's law of property and nuisance."[200] In other words, the Court seems to be asking if the property owner's expectations were reasonable in light of the government's recognized power and past practice.

Data protection regulation may legitimately prompt takings claims. If the government prohibits the processing of personal data, it could deny the owner all or most of the "economically viable use" use of that data. Moreover, if Congress were to enact privacy protection along the lines of the EU directive, that legislation might very well restrict all use of that data and thereby constitute a complete taking.[201] At first glance, this may seem an odd result, because the data collected or processed, in order to be subject to privacy regulation in the first place, must be about another person. How can one person have a constitutional property right to hold and use data about another? However, this result is not that surprising in light of current law in the United States, which rarely accords individuals ownership interests in key information about themselves. As Professor Branscomb has demonstrated in her study, *Who Owns Information?*, in the United States, telephone numbers, addresses, Social Security numbers, medical history, and similar personal identifying data are almost always owned

---

197. Lucas v. South Carolina Coastal Council, 505 U.S. 1003, 1016 (1992); *see also* Agins v. City of Tiburon, 447 U.S. 255, 260 (1980); Andrus v. Allard, 444 U.S. 51, 64 (1979).

198. *See* Jan G. Laitos, *The Takings Clause in America's Industrial States After Lucas*, 24 U. TOL. L. REV. 281, 288 (1993).

199. *See Lucas*, 505 U.S. at 1026.

200. *Id.* at 1027, 1029.

201. A legislature can effect a taking just as a regulatory agency can. *See, e.g., Agins*, 447 U.S. 255. Both are generally referred to as "regulatory takings," although the former is actually a "legislative taking." *See generally* Parking Ass'n of Ga., Inc. v. City of Atlanta, 515 U.S. 1116 (1995) (Thomas, J., dissenting from denial of cert.).

by someone else—the Post Office, the government, or a physician or hospital.[202] Moreover, individuals exercise few rights in data about themselves which are readily perceptible, such as gender, age, or skin color. A photographer who takes a picture on a public street has the legal right to use that picture for a wide variety of noncommercial and even commercial uses without the permission of the individuals depicted. In fact, those individuals have no legal right to market or even copy or publicly display the photograph which includes their images without the photographer's permission.[203]

A data processor exercises property rights in his data because of his investment in collecting and aggregating them with other useful data. It is this often substantial investment that is necessary to make data accessible and useful, as well as the data's content, that the law protects. In the current regulatory environment in the United States, discussed below, it is reasonable for an information processor to believe and to invest resources in the belief that she will be able, within some limits, to use the data she collects and processes. In fact, as Arthur Miller has argued, the "expand[ing] protection for commercial information reflects a growing awareness that the legal system's recognition of the property status of such information promotes socially useful behavior"[204] and therefore encourages reliance by data processors. A legislative, regulatory, or even judicial[205] determination that denies processors the right to use their data could very likely constitute a taking and require compensation. Data processors who acquire or process data after enactment of new privacy standards would be on notice and therefore less likely to succeed in claiming takings. But for the billions of data files currently possessed and used by U.S. individuals and institutions, a dramatic alteration in user rights makes a compelling case for the existence of a taking.

The determination of whether a government action constitutes a taking, of course, turns on the details of the specific action and property involved. It is sufficient here to note that the personal information held by others is likely the subject of property and related rights. Those rights are in almost every case possessed by the data processor, not the persons to whom the data pertain. And because these data are accorded property-like protection, they are subject to

---

202. *See* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS (1994).

203. *See* 17 U.S.C. §§ 101-106 (1994 & Supp. 1997).

204. Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 469 (1991).

205. *See* Note, *Trade Secrets in Discovery: From First Amendment Disclosure to Fifth Amendment Protection*, 104 HARV. L. REV. 1330 (1991).

> Courts are widely considered "state actors" for purposes of constitutional analysis, and the Supreme Court has recognized that the takings clause applies to the courts. In a 1967 concurrence, Justice Stewart asserted that the fourteenth amendment forbids a state to take property without compensation "no less through its courts than through its legislature."

Id. at 1336 (quoting Hughes v. Washington, 389 U.S. 290, 298 (1967) (Stewart, J., concurring)).

being taken by government regulation, thereby triggering an obligation to compensate the data owner.

Government efforts to protect privacy would have to clear considerable constitutional hurdles, including the First and Fifth Amendments.

6. State Constitutions.—At least eight states have adopted explicit constitutional guarantees of personal privacy. As with federal constitutional protections, these rights virtually always impose restrictions only on governmental activities. Often these protections are vague and aspirational. Moreover, when state constitutional rights and federal law conflict, federal law prevails. Therefore, state constitutional privacy rights have thus far been of little significance in the day-to-day protection of personal privacy. Nonetheless, these provisions are significant to the extent that they restrict the activities of state governments, serve as a potential source of future restraints on government activities, and indicate a growing interest in privacy protection.

Some state constitutional privacy protections merely repeat federal constitutional provisions. For example, Minnesota includes in its constitution the text of the Fourth Amendment to the Federal Constitution.[206] The constitutions of Hawaii and Louisiana both include Fourth Amendment-like provisions, but they have been modified to explicitly prohibit "invasions of privacy. . . ."[207] Some state constitutional protections for privacy incorporate exceptions as broad as the protection they purport to afford privacy. Arizona's constitution provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."[208] Such a right presumably would exist even without this constitutional provision. In 1980, Florida amended its constitution to provide that: "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law."[209]

Other states' provisions are less qualified or more specific. Alaska amended its constitution in 1972 to provide that "[t]he right of the people to privacy is recognized and shall not be infringed."[210] In 1974, California added privacy to the "inalienable rights" protected under its constitution: "All people . . . have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy."[211] This provision is particularly noteworthy, because in 1994 the California Supreme Court found that it was applicable to private, as well as governmental, actions.[212] The Illinois constitution provides that "[t]he people shall have the right to be secure . . . against . . . invasions of privacy."[213] In 1978, Hawaii

---

206. *See* MINN. CONST. art. I, § 10.
207. HAW. CONST. art. I, § 7; LA. CONST. art. I, § 5.
208. ARIZ. CONST. art. II, § 8.
209. FLA. CONST. art. I, § 23.
210. ALASKA CONST. art. I, § 22.
211. CAL. CONST. art. I, § 1.
212. *See* Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994) (en banc).
213. ILL. CONST. art. 1, § 6.

amended its constitution to add: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."[214] This is the most specific and protective of any of the state constitutional provisions guarding privacy interests, in practice as well as on paper. At least partially based on this provision, a Hawaiian court ruled in December 1996 in favor of same-sex marriages.[215]

Even the most protective state constitutional provisions, however, have yielded little protection for information privacy. For example, even in the 1994 case in which the California Supreme Court extended the state constitutional right to privacy to private actions, the Court found that a mandatory drug-testing program for college athletes did not violate that right.[216] This same result was reached by the U.S. Supreme Court the following year without the benefit of an explicit constitutional guarantee to privacy.[217] Moreover, in the context of global information networks and national and multinational information users, state protection is of limited significance.

B. Federal Statutes

The laws and regulations governing the use of personal information are many and varied, but as a rule they each address a specific government agency, industry, or economic sector and often only specific issues. Even when legal protection is at its height, it is still often limited to certain activities, such as disclosure of personal data, and qualified by exemptions.[218]

Privacy-based controls on the *government*'s collection and use of data are far more extensive than those applicable to non-governmental organizations. For example, the federal Privacy Act obligates government agencies to (1) store only relevant and necessary personal information; (2) collect information to the extent possible for the data subject; (3) maintain records with accuracy and completeness; and (4) establish administrative and technical safeguards to protect the security of records.[219] The Privacy Act also limits disclosure of individuals' records.[220] However, the Act explicitly restricts its provisions from prohibiting the release of any material for which disclosure is required under the Freedom of Information Act (FOIA).[221] The FOIA permits "any person" to obtain access to all federal "agency records," subject to nine enumerated exemptions.[222] In

---

214. HAW. CONST. art. 1, § 6.

215. *See* Lyle Denniston, *Judge OKs Same-Sex Marriages*, BALTIMORE SUN, Dec. 4, 1996, *available in* 1996 WL 6649965.

216. *See Hill*, 865 P.2d at 669.

217. *See* Vernonia Sch. Dist. v. Acton, 515 U.S. 646 (1995).

218. *See generally* CATE, *supra* note 19, at 76-89.

219. *See* 5 U.S.C. §§ 552a(e)(1)-(5) (1994).

220. *See id.* § 552a(b).

221. *See id.* § 552a(t)(2).

222. *See* 5 U.S.C. § 552 (1994). Two of the nine exemptions are designed to protect privacy: Exemption 6 precludes disclosure of "personnel and medical files and similar files the disclosure

other words, any information to which the FOIA applies and which is not within one of the FOIA's nine enumerated exemptions, must be disclosed irrespective of the Privacy Act. In addition, the Privacy Act provides twelve exemptions that permit disclosure of information to other government agencies.[223] For example, the Act does not apply to Congress. It does not restrict disclosures to law enforcement agencies, and, under the broadest exemption, the Act does not apply to data requested by another government agency for "routine use."[224]

There are many other statutes and regulations which protect the privacy of citizen information from government disclosure of data. For example, federal law prohibits the Department of Health and Human Services from disclosing social security records, but permits all disclosures "otherwise provided by Federal law" or regulation.[225] Similarly, federal law prohibits the Internal Revenue Service from disclosing information on income tax returns[226] and the Census Bureau from disclosing certain categories of census data.[227] Finally, many states have adopted laws and regulations that mirror their federal counterparts.

Congress has also enacted a variety of laws addressing the protection of personal information in *private* industry sectors, such as in the context of financial transactions. The Fair Credit Reporting Act of 1970[228] (the "Act") "sets forth rights for individuals and responsibilities for consumer credit reporting agencies in connection with the preparation and dissemination of personal information in a consumer report bearing on the individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living."[229] The Act requires that credit reporting agencies follow "reasonable procedures to assure maximum possible accuracy"[230] of the information in their credit reports and implement a dispute resolution process to investigate and correct errors.[231] Agencies also must inform consumers about whom adverse decisions on credit, employment, or insurance are made based on a consumer report, of the use and source of the report. The

---

of which would constitute a clearly unwarranted invasion of personal privacy," and Exemption 7(C) bans release of "records or information compiled for law enforcement purposes [which] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy." *Id.* § 552(b)(6)-(7)(C). Many states have government disclosure statutes with privacy-based exemptions similar to those provided in the FOIA.

223. *See id.* § 552(a)(b)(1)-(12).

224. *Id.* § 552(a)(b)(3).

225. 42 U.S.C. § 1305 (1994).

226. *See* 26 U.S.C. §§ 6103, 7431 (1994 & Supp. 1997).

227. *See* 13 U.S.C. §§ 8-9 (1994 & Supp. 1997).

228. 15 U.S.C. §§ 1681-1681t (1994).

229. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 210 (1992).

230. 15 U.S.C. § 1681e(b).

231. *See id.* § 1681i.

agencies must provide consumers with a copy of their reports upon request.[232]

Prior to being amended at the end of 1996, the Act's protections were weakened by a series of broad loopholes. On September 30, 1996, Congress passed the Consumer Credit Reporting Reform Act,[233] which closed many of these loopholes and significantly strengthened the protection for information privacy provided by the Fair Credit Reporting Act. For example, the Reform Act narrowed the broad "legitimate business need" purpose for which credit reports could be disseminated without the consumer's authorization to permit the distribution of credit reports only for a "legitimate business need . . . in connection with a business transaction that is initiated by the consumer" or "to review an account to determine whether the consumer continues to meet the terms of the account."[234] Consumer credit reports may now be furnished for employment purposes only if the employer certifies that the employee has consented.[235] Medical information may no longer be included in a credit report furnished in connection with employment, credit, insurance, or direct marketing, without the consent of the consumer.[236] If a credit reporting agency furnishes consumer credit information to be used for marketing credit or insurance opportunities to consumers, the agency must establish and publish a toll-free telephone number that consumers can call to have their names removed from lists provided for such direct marketing purposes.[237] Persons who acquire such information from credit reporting agencies for marketing credit and insurance services must inform consumers that credit information was used, identify the credit agency from which the data were obtained, and provide information about consumers' legal rights.[238]

The Act prohibits 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, and any other adverse information older than seven years.[239] Prior to the 1996 amendments, the Act permitted even obsolete information to 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.[240] Although these dollar thresholds were set in 1970, they had not been increased in twenty-five years to keep pace with inflation.[241]

---

232. *See id.* § 1681m.

233. *Id.* §§ 1681-1681t (Supp. 1997).

234. *Id.*

235. *See id.*; *see also* Consumer Reporting Employment Clarification Act of 1998, Pub. L. No. 105-347, 112 Stat. 3208.

236. *See* 15 U.S.C. §§ 1681-1681t.

237. *See id.* § 1681b(c)(5).

238. *See id.* § 1681m(d).

239. *See id.* § 1681c(a); *see also* Consumer Reporting Employment Clarification Act of 1998, Pub. L. No. 105-347, 112 Stat. 3208.

240. *See* 15 U.S.C. § 1681c(b) (1994).

241. *See* Reidenberg, *supra* note 229, at 213 n.92.

The 1996 Reform Act continued to permit the dissemination of obsolete information, but it raised the dollar thresholds to permit dissemination in connection with an employment application for a position with a salary over $75,000, a credit transaction over $150,000, or the underwriting of life insurance over $150,000.[242]

The revised act specifies a number of situations in which credit agencies and, in some cases, the persons to whom they supply information, must provide information to consumers, including a general requirement that agencies inform consumers of their legal rights under the Fair Credit Reporting Act.[243] In a dramatic extension of the law, the Reform Act provides that credit reporting agencies must delete any disputed data that they cannot verify within thirty days, as well as comply with a variety of new procedural requirements concerning correcting data and notifying recipients of credit reports of disputed or inaccurate data.[244] No longer must the consumer prove information false to have it excluded. In a second significant development, the Act now requires anyone who furnishes data to a credit reporting agency to correct inaccurate data, to notify any agency to which it has reported data if it determines that those data are inaccurate, and to disclose to any agency to which it is reporting data if those data's accuracy is disputed.[245] Finally, the Reform Act directed the Federal Reserve Board to make recommendations to Congress within six months concerning the data processing activities of organizations not covered by the Fair Credit Reporting Act and the extent to which those activities "create undue potential for fraud and risk of loss to insured depository institutions. . . ."[246]

After passage of the Reform Act's amendments, the Fair Credit Reporting Act significantly restricts the content, disclosure, and use of credit information, while not addressing the collection and use of personal information generally.[247]

Other statutes provide protection for certain specific privacy-related interests. For example, the Fair Credit Billing Act of 1974,[248] requires that creditors furnish consumers with copies of their credit transaction records and provide consumers with an opportunity to dispute errors, during which time creditors are restricted from disclosing information about delinquent payments.[249] The Fair Debt Collection Practices Act of 1977[250] limits debt collectors' disclosures to some

---

242. *See* Department of Defense Appropriations Act, § 2406(a)(2) (codified at 15 U.S.C. § 1681c(b) (Supp. 1997)).

243. *See* 15 U.S.C. § 1681g(a), (c) (Supp. 1997).

244. *See id.* § 1681i(a).

245. *See id.* § 16815-2.

246. *Id.* § 2422. *See* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD (1997) [hereinafter REPORT TO THE CONGRESS].

247. *See* 15 U.S.C. §§ 1681a(f), (d) (1994 & Supp. 1997).

248. *Id.* § 1666 (1994).

249. *See* Reidenberg, *supra* note 229, at 213.

250. 15 U.S.C. § 1692c(b) (1994).

third parties (but not credit reporting agencies) of a debtor's financial situation.[251]

The Electronic Communications Privacy Act of 1986[252] prohibits the interception or disclosure of the contents of any electronic communication, such as telephone conversations or e-mail, or even of any conversation in which the participants exhibit "an expectation that such communication is not subject to interception under circumstances justifying such an expectation."[253] There are a number of exceptions to this apparently broad privacy right, the most significant of which is that the prohibition does not apply if any one party to the communication consents to disclosure.[254] The prohibition also does not apply to switchboard operators, employees of telecommunications service providers, employees of the Federal Communications Commission, or anyone assisting the holder of a warrant, provided they are acting within the scope of their duties.[255] The prohibition also does not apply if the communication intercepted was "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public," including any marine or aeronautical system, amateur and citizens band radio, or "general mobile radio services."[256]

Prior to 1996, there was no statutory protection for information about telecommunications transactions, such as telephone numbers or time, place, and duration of call.[257] The Electronic Communications Privacy Act did not apply to "transactional" information, so service providers faced no legal limits on collecting, storing, or disclosing such data. In fact, the statute explicitly authorizes the use of "a pen register or a trap and trace device" to record information about other individuals' conversations or transmissions.[258] On February 1, 1996, however, Congress passed the Telecommunications Act of 1996, which included provisions protecting the privacy of "Customer Proprietary Network Information"[259] ("CPNI"). The Act defines CPNI as "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the

---

251. *See id.*

252. 18 U.S.C. §§ 2510-2520 (1994 & Supp. 1997).

253. *Id.* §§ 2510-11(2) (1994).

254. *See id.* § 2511(2)(c).

255. *See id.* § 2511(2).

256. *Id.* § 2511(2)(g).

257. The Federal Communications Commission regulated the disclosure of such information as a way of promoting competition among telephone companies. *See* 47 C.F.R. § 64.702(d)(3) (1997). Under the Commission's regulations, a regulated telecommunications service provider could not provide information about telecommunications transactions to its own subsidiaries which offered "enhanced" services, unless it also disclosed that information to competitors. *See id. See generally* Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 37-41 (1998).

258. 18 U.S.C. § 2511(2)(h)(i) (1994).

259. Pub. L. No. 104-104, 11 Stat. 56 § 702 (codified at 47 U.S.C. § 222 (Supp. 1996)).

customer solely by virtue of the carrier-customer relationship."[260] Under the Act, service providers may "use, disclose, or permit access to individually identifiable" CPNI only as necessary to provide the telecommunications service from which the information is derived or services necessary to that telecommunications service.[261] Service providers are free to use CPNI as necessary to protect their own business interests.[262] Although the Act only restricts the disclosure of information and the exemption for related services such as telephone directories is considerable, the new provision reflects Congress' growing attention to privacy concerns.

The Cable Communications Policy Act of 1984[263] provides extensive privacy-related regulation of cable television service providers. The Act restricts the collection, storage, and disclosure of "personally identifiable information" without the subscriber's consent,[264] and requires that service providers provide their subscribers with access to information collected about them.[265] The Act also requires that the cable service provider inform the customer at least once a year of the information it collects, the "nature, frequency, and purpose of any disclosure" of that information, the duration of its storage, the times and places at which a customer may have access to that information, and the terms of the statute.[266] The Act provides for statutory damages against cable operators who violate their customers' rights under the Act.[267] It also includes some exemptions, particularly for disclosures of information "necessary to render, or conduct a legitimate business activity related to" the provision of cable service,[268] but it nonetheless constitutes the broadest set of privacy rights in any federal statute.

Federal law also protects against the disclosure of video tape rental and sale records. The Video Privacy Protection Act of 1988,[269] adopted in response to congressional outrage over the disclosure of the list of videos rented by Judge Robert Bork during his ill-fated Supreme Court nomination confirmation hearings, prohibits the disclosure of titles of particular films rented by identifiable customers. The statute also requires the destruction of personally identifiable information not later than one year after the information if no longer necessary for the purpose for which it was collected.[270] There are significant exemptions, for example, "if the disclosure is incident [sic] to the ordinary course

---

260. *Id.* (codified at 47 U.S.C. § 222(f)(1)).
261. *Id.* (codified at 47 U.S.C. § 222(c)(1)).
262. *See id.* (codified at 47 U.S.C. § 222(d)).
263. 47 U.S.C. § 551(a)(1) (1994).
264. *Id.* § 551(c).
265. *See id.* § 551(d).
266. *Id.* § 551(a).
267. *See id.* § 551(f).
268. *Id.* § 551(c)(2).
269. 18 U.S.C. § 2710 (1994).
270. *See id.* § 2710(e).

of business of the video tape service provider. . . ."[271] Moreover, data about user viewing habits may be disclosed for marketing purposes if the user has been given an opportunity to "opt out" of such disclosure.[272] As a result, lists are widely available containing information on user viewing habits and other demographic information, such as median age and income.

Congress' most recent privacy law, the Children's Online Privacy Protection Act,[273] restricts the online collection of information about children under 13. The Act requires that operators of commercial web sites which target children or are aware that they are collecting information from children provide notice of their data collection policies and seek parental consent before collecting information from children.[274] The Act defers to the Federal Trade Commission most of the keys issues about the form and substance of parental notification and consent. The Commission adopted implementing regulations on October 20, 1999, which will take effect on April 21, 2000.[275] The Act also features a "safe harbor" option which allows industry groups to submit self-regulatory mechanisms to the Commission which, if approved would create a presumption that persons in compliance with these self-regulatory mechanisms are also in compliance with the Act.[276]

C. State Statutes

At least thirteen states have general privacy statutes applicable to government activities. Some states also have statutory privacy rights that apply to the private sector. We can see three approaches reflected in these state statutory provisions.[277]

Two states, Massachusetts and Wisconsin, have adopted general rights of privacy, although these statutes largely restate the common law privacy torts which are discussed below. For example, Massachusetts provides that "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy,"[278] but state courts largely limit this right to the "public disclosure of private facts" tort discussed below. Similarly, Wisconsin's facially broad privacy statute—"The right of privacy is recognized in this state"[279]—is restricted to the torts of intrusion, public disclosure of private facts, and misappropriation.[280] Even in those limited contexts, the statute specifically

---

271. *Id.* § 2710(b)(2)(E).

272. *See id.* § 2710(b)(2)(D).

273. Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (to be codified at 15 U.S.C. § 6501).

274. *See id.*

275. *See id.*

276. *See id.*

277. *See* Reidenberg, *supra* note 229, at 227-28.

278. MASS. GEN. LAWS ANN. ch. 214, § 1B (1996) (West 1989).

279. WIS. STAT. ANN. § 895.50 (West 1998).

280. *See id.*

exempts from any prior restraint designed to protect privacy "constitutionally protected communication privately and through the public media. . . ."[281]

A number of states have eschewed the appearance of broad privacy protection and have instead codified one or more of the common law privacy torts (discussed below).[282] Finally, many states have enacted industry-specific privacy legislation in areas similar to federal private sector statutes.[283] These sectoral statutes have been the focus of recent intense state legislative activity, with forty-two states enacting a total of 786 bills in 1998.[284] Already in 1999, states have considered an extraordinary array of privacy statues addressing issues ranging from direct marketing to medical records. New York has adopted fourteen new privacy laws and is still considering others.[285] Like their federal counterparts, "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."[286] The new array of state statutes is also focusing new attention on issues surrounding the interaction of these laws with each other and with federal law, especially in the context of the Internet and electronic information transfers.

D. Tort Law

Following publication of Samuel Warren's and Louis Brandeis' article, "The

---

281. *Id.* § 895.50(1)(a).

282. *See, e.g.*, CAL. CIV. CODE § 3344 (West 1997); FLA. STAT. ANN. § 540.08 (West Supp. 1999); N.Y. CIV. RIGHTS LAW §§ 50-51 (McKinney 1992 & Supp. 1999).

283. *See, e.g.*, CAL. LAB. CODE § 1198.5 (West Supp. 1999) (employee personnel records); CONN. GEN. STAT. ANN. § 31-128f (West 1997) (employee personnel records); DEL. CODE ANN. tit. 11, §§ 1335-36 (1995) (intrastate telephone service); MASS. GEN. LAWS ANN. ch. 93, §§ 50-68 (West 1997) (credit reporting); N.J. STAT. ANN. § 48:5A-54 to -63 (West 1998) (cable subscriber information and viewing habits); N.Y. GEN. BUS. LAW § 380 (McKinney 1996) (credit reporting); 18 PA. CONS. STAT. ANN. §§ 5701-775 (West 1983 & Supp. 1999) (intrastate telephone service).

284. *See Privacy Legislation in the States*, PRIV. & AM. BUS., Nov./Dec. 1998, at 1, 3.

285. *See* A.B. 7047, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (identify theft); A.B. 5543, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (temporary state privacy commission); A.B. 137, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (limits credit card and debit card issuers' release of customer names); A.B. 467, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (regulates personal identification of a credit card holders); A.B. 5384, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (credit card fraud prevention); A.B. 5917, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (telemarketing and unsolicited advertisements); A.B. 8110, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (limits use of registration lists and title information made available to contracting parties); AB. 8116, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (prohibits the disclosure of photos by state agencies); A.B. 1830, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (confidentiality of electronic toll records); A.B. 7044, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (privacy of e-mail addresses); A.B. 7045, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (unsolicited e-mail advertisements); A.B. 8130, 222nd Legis., 1st Reg. Sess. (N.Y. 1999) (Internet privacy).

286. Reidenberg, *supra* note 229, at 229.

Right to Privacy" in the *Harvard Law Review* in 1890,[287] seventy years passed before William Prosser proposed a structure for the common law privacy rights that Warren and Brandeis advocated.[288] Dean Prosser analyzed the numerous state court opinions recognizing various forms of a "right to privacy," and then categorized that right into four distinct torts: physical intrusion, misappropriation, false light, and publication of private facts.[289] This structure, included in the *Restatement (Second) of Torts* (for which Dean Prosser served as reporter), replaced the single privacy right found in the first *Restatement of Torts*. The second *Restatement* provides:

> Section 652A. General Principle
>
> (1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
>
> (2) The right of privacy is invaded by
>
> (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or
>
> (b) appropriation of the other's name or likeness, as stated in § 652C; or
>
> (c) unreasonable publicity given to the other's private life, as stated in § 652D; or
>
> (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.[290]

The tort of unreasonable intrusion lends little support to information privacy, other than as a potential restriction on the means of gathering information. Like the other three privacy torts, this one requires that the intrusion involve "solitude or seclusion of another or his private affairs or concerns" and that it be "highly offensive to a reasonable person."[291] This tort is recognized in some form in all but six states.

The tort of appropriation only applies to the "name or likeness" of an individual,[292] and therefore is of limited value as a protection for information privacy. Only about two-thirds of the states recognize this tort and most of them require that the appropriation be for "commercial gain," such as advertising.

The tort of "unreasonable publicity given to the other's private life" applies

---

287. Warren & Brandeis, *supra* note 127.
288. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
289. *See id.* at 389.
290. RESTATEMENT (SECOND) OF TORTS § 652A (1976).
291. *Id.* § 652B.
292. *Id.* § 652C.

only when there is a disclosure to a large audience of private information that would be "highly offensive to a reasonable person and is not of legitimate concern to the public."[293] In addition to these limits, the U.S. Supreme Court has ruled that lawfully obtained, truthful information on a matter of public significance can never be the subject of legal liability, at least not without satisfying the requirements of strict scrutiny.[294] In *Philadelphia Newspapers, Inc. v. Hepps*,[295] the Court reaffirmed that punishing true speech was "antithetical to the First Amendment's protection. . . ."[296] Susan M. Gilles has noted that "[i]f the constitutional requirement of proof of falsity articulated in libel cases is extended to privacy cases, then the private-facts tort is unconstitutional."[297] This tort is recognized in all but six states, but the number of successful public disclosure actions has been insignificant.[298]

The final privacy tort is "publicity that unreasonably places the other in a false light before the public."[299] To be actionable under the false light tort, the publication must be both false and highly offensive to a reasonable person.[300] In 1967, in *Time, Inc. v. Hill*,[301] the Supreme Court extended the First Amendment privileges previously recognized in the context of defamation to actions for false light privacy.[302] The Court thus required plaintiffs to show that the defendant knew the publication was false or recklessly disregarded its truth or falsity.[303] Fewer than two-thirds of states recognize this tort.

These state tort actions are the principal source today of adjudicated legal rights concerning privacy. However, they offer little protection for information privacy. Even in their limited areas, only one award to a privacy tort plaintiff has ever survived the Supreme Court's First Amendment scrutiny.[304]

E. U.S. Privacy Principles

Privacy protection in the United States reflects four features of American society and system of government. Understanding those four features is critical to recognizing both the level of privacy protection that exists in the United States

---

293. *Id.* § 652D. *See also id.* § 652D cmt. a.

294. *See* Florida Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).

295. 475 U.S. 767 (1986) (holding a private-figure defamation plaintiff could not recover damages without also showing that the statements at issue were false).

296. *Id.* at 777.

297. Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 8 (1995).

298. *See* RESTATEMENT (SECOND) OF TORTS § 652E (1976).

299. *Id.*

300. *See id.*

301. 385 U.S. 374 (1967).

302. *See id.* at 387-88.

303. *See id.*

304. *See* Cantrell v. Forest City Publ'g Co., 419 U.S. 245 (1974).

and the limits on that protection and on the means by which it may be achieved.

1. Rights Against the Government.—First, the U.S. Constitution reflects the conviction that the greatest threat to individual liberty is the government. As a result, rights articulated in the Constitution generally are protected only against government actions. Only the Thirteenth Amendment, which prohibits slavery, applies directly to private parties.[305] All other constitutional rights—whether to speak freely, confront accusers, or be tried by a jury of one's peers—regulate the public, but not the private, sector.

One dominant theme of constitutional rights is the protection of citizens from government intrusion into their privacy. A vigorous First Amendment, as we have seen, permits individuals the privacy of their own thoughts, beliefs, and associations.[306] The Third Amendment keeps government soldiers from being quartered in private homes.[307] The Fourth Amendment prohibits unreasonable searches and seizures.[308] The Fifth Amendment restricts government from interfering with private property, provides for due process and compensation when it does so, and protects citizens from self-incrimination.[309] Collectively, these and other provisions of the Constitution impose extraordinary limits on government authority to intrude on private property, compel testimony, or interfere with practices closely related to individual beliefs, such as protest, marriage, family planning, or worship.

Controlling a government's actions is an essential step to protecting privacy not only because of a government's size and power, but also because of its isolation from the market—a mechanism, as is discussed in greater detail below, that plays a vital role in protecting individuals from private-sector intrusion.

The effect of these constitutional protections, however, is not just to protect privacy from government intrusion. Legal respect for private property, for example, also allows individuals to separate themselves from each other, perhaps the best guarantee of privacy. The laws that attend private property are what empower one person to exclude another from her land, home, papers, and possessions, and to call upon the state to protect those objects from physical intrusion and interference.

2. Importance of Open Information Flows.—The second feature of the U.S. information society is the extraordinary importance placed in the United States on the unrestricted flow of information. As the Federal Reserve Board noted in its report to Congress on data protection in financial institutions, "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."[310]

The significance of open data flows is reflected in the constitutional provisions not only for freedom of expression, but for copyrights, to promote the

---

305. *See* Clyatt v. United States, 197 U.S. 207, 216-220 (1905).

306. *See* U.S. CONST. amend. I.

307. *See id.* amend. III.

308. *See id.* amend. IV.

309. *See id.* amend. V.

310. REPORT TO THE CONGRESS, *supra* note 246, at 2.

creation and dissemination of expression, and for a post office, to deliver the mail and the news.[311] Federal regulations demonstrate a sweeping preference for openness, reflected in the Freedom of Information Act, Government in the Sunshine Act, and dozens of other laws applicable to the government. There are even more laws requiring disclosure by private industry, such as the regulatory disclosures required by securities and commodities laws, banking and insurance laws, and many others.

The focus on openness both advances and restricts privacy interests. It furthers privacy by guaranteeing that citizens have affordable access to data, particularly about themselves, thereby facilitating the identification and correction of inaccurate information. This is a key function, for example, of the disclosure requirements in the FOIA. It also facilitates privacy protection by supporting a vigorous, independent press, which has repeatedly proved invaluable in investigating and exposing privacy intrusions by both government and private parties.[312]

The focus on openness, however, also reflects an understanding that in a democracy and a market economy, privacy is not an unmitigated good. As a result, efforts to enhance personal privacy are balanced against the costs that those efforts impose on the free flow of information, the election and supervision of governments, the development of efficient markets, and the provision of valuable services.

Protecting the privacy of information imposes real costs on individuals and institutions. Judge Richard Posner has written:

> Much of the demand for privacy . . . concerns discreditable information,

---

311. *See* U.S. CONST. art. I, § 8.

312. In 1991, Lotus Development Corporation and Equifax abandoned plans to sell "Households," a CD-ROM database containing names, addresses, and marketing information on 120 million consumers, after receiving 30,000 calls and letters from individuals asking to be removed from the database. *See* Lawrence M. Fisher, *New Data Base Ended by Lotus and Equifax*, N.Y. TIMES, Jan. 24, 1991, at D4. Cancellation of "Households" led Lotus to abandon "Lotus Marketplace," a similar CD-ROM database with information on seven million U.S. businesses. Eight months later, Equifax, one of the United States' largest credit bureaus, decided to stop selling consumer names and addresses to direct marketing firms altogether, a business that had earned the company $11 million the previous year. *See* Shelby Gilje, *Credit Bureau Won't Sell Names*, SEATTLE TIMES, Aug. 9, 1991, at D6.

More recently, Lexis-Nexis, operator of one of the largest legal and general information databases in the world, has revamped plans for "P-Track," a service that provides anyone willing to pay the $85-$100 search fee with personal information, including maiden names and aliases, about "virtually every individual in America." Kathy M. Kristof, *Deluged Lexis Purging Names from Databases*, L.A. TIMES, Nov. 8, 1996, at D5. The database reportedly includes current and previous addresses, birth dates, home telephone numbers, maiden names, and aliases. Initially, Lexis was also providing Social Security numbers. However, in response to a storm of protest, Lexis stopped displaying Social Security numbers, and it is honoring the requests of anyone who wishes to be deleted from the database. *See id.*

> often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is . . . to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit . . . .[313]

Privacy facilitates the dissemination of false information, protects the withholding of relevant true information, and interferes with the collection, organization, and storage of information on which businesses and others can draw to make rapid, informed decisions. The costs of privacy include both transactional costs incurred by information users seeking to determine the accuracy and completeness of the information they receive, and the risk of future losses resulting from inaccurate and incomplete information. Therefore, privacy may reduce productivity, lead to higher prices for products and services, and make some services untenable altogether.

Moreover, even when the information disclosed is not inherently significant, or in the context of a relationship where health or safety are at stake, there is nonetheless value in curiosity. As Judge Posner has noted, "casual prying" is not only a common feature of everyday life, it "is also motivated, to a greater extent than we may realize, by rational considerations of self-interest. Prying enables one to form a more accurate picture of a friend or colleague, and the knowledge gained is useful in one's social or professional dealings with him."[314] Even the term "idle curiosity," according to Judge Posner, is "misleading. People are not given to random, undifferentiated curiosity."[315] For example, "[g]ossip columns recount the personal lives of wealthy and successful people whose tastes and habits offer models—that is, yield information—to the ordinary person in making consumption, career, and other choices. . . . [They] open people's eyes to opportunities and dangers; they are genuinely informational."[316] Protection for privacy, therefore, not only interferes with the acquisition of information that has a particular, identified significance, it also impedes a voyeuristic curiosity that is widely shared and that serves valuable purposes for both individuals and society.

The protection of privacy may also interfere with other constitutional values, such as the protection for expression in the First Amendment and the protection for private property in the Fifth Amendment.

The late Professor Anne Branscomb wrote: "Information is the lifeblood that sustains political, social, and business decisions."[317] Although U.S. law offers extensive protection to individuals from government collection and use of

---

313. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399 (1978).

314. *Id.* at 395-96.

315. *Id.* at 396.

316. *Id.*

317. Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 987 (1983).

personal data, the commitment to open information flows is so great that our laws extend virtually no direct protection to data, other than trade secrets, in the marketplace.

3. Preference for Private Action.—The third significant feature is that the United States has historically depended heavily on private industry, private property, and individual self-reliance. Constitutional rights are generally "negative"; they do not obligate the government to *do* anything, but rather to *refrain* from unnecessarily interfering with individuals' freedom to act. This also explains the very high protection in U.S. law for private agreements. Citizens do not have to make promises to one another, but when we do, the government makes available valuable resources to enforce those promises.

The preference for private action and individual responsibility is especially clear when information is involved. The U.S. Supreme Court has repeatedly interpreted the First Amendment to deny plaintiffs aggrieved by even false and harmful speech any remedy, stressing instead, in the words of Justice Brandeis, "the remedy to be applied is more speech, not enforced silence."[318]

The focus on individual and collective private action inevitably restrains the power of the government to pass sweeping privacy laws. But it also facilitates considerable privacy protection through the use of technologies, markets, industry self-regulation and competitive behavior, and individual judgment. For example, technological innovations such as adjustable privacy protection settings in both Netscape and Microsoft Explorer, encryption software, anonymous remailers, and, in fact, the Internet itself all facilitate privacy and individual control over the information we disclose about ourselves.

Many companies are actively competing for customers by promoting their privacy policies and practices. If enough consumers demand better privacy protection and back up that demand, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much the society really values privacy.

Considerable privacy protection also exists in private agreements. When a company promotes its privacy policy, under U.S. law it is obligated to adhere to that policy. The failure to do so may subject an institution to suits by consumers and action by the Federal Trade Commission, which is empowered by Congress to investigate "unfair or deceptive" trade practices.[319]

Industry organizations are increasingly providing standards for privacy protection and help to consumers whose privacy interests are compromised. The Direct Marketing Association, for example, operates the Mail Preference Service and the Telephone Preference Service. With a single request to each, it is possible to be removed from most DMA-member company mailing and telephone

---

318. Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring). *See* 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 497 (1996); Texas v. Johnson, 491 U.S. 397, 419 (1989).

319. *See* 15 U.S.C. § 57b-1(1997).

solicitation lists.[320]

Many industry associations have adopted guidelines and principles which may serve as models for individual company policies. Corporate compliance with privacy standards constitutes an increasingly important accolade in competitive markets, particularly among Internet users. Moreover, industry associations can help persuade member organizations to adopt and adhere to industry norms for privacy protection. The DMA, for example, has begun issuing quarterly reports on members who are being disciplined for violating DMA codes of conduct.

A consortium of privacy advocates and software companies has announced the development of a service to make privacy self-help easier on the Internet. "TRUSTe" is a program that rates Internet sites according to how well they protect individual privacy. Internet sites that provide sufficient protection for individual privacy—including not collecting personal information, not disseminating information to third parties, and not using information for secondary purposes—earn the right to display the "TRUSTe" logo.[321] The Better Business Bureau has recently launched a similar initiative—BBB Online.[322]

The majority of the individual reference services group industry has agreed to abide by the ISRG Principles, which not only establish data protection standards, but also require annual compliance audits by third parties and a commitment not to provide information to entities whose practices are inconsistent with the ISRG Principles.[323]

These more flexible, more contextual, more specific tools offer better privacy protection than an omnibus law, and at potentially lower cost to consumers, businesses, and the society as a whole. These responses are exactly what we would expect from the market if consumers value privacy protection in the private sector.

4. Limited Role for Government.—Finally, the United States has historically recognized important roles for government to keep markets open, to fill in those gaps necessary to protect vulnerable populations, such as children, and to respond to needs left unmet by traditional markets, such as protecting the environment.

The same is true for privacy. The government still plays an important role in protecting privacy, but the legal regulation of privacy in the U.S. private sector is largely limited to facilitating individual action. For example, Congress recently enacted federal restrictions on collecting information from children

---

320. *See* Direct Marketing Association, *Frequently Asked Questions to Help You Understand Direct Marketing* <http://www.the-dma.org/topframe/index5.html>. The DMA reports that these service are used by only two percent of the U.S. adult population.

321. *See How the TRUSTe Program Works* (visited Dec. 1, 1999) <http://www.truste.org>.

322. *See BBB Online Privacy Program* (visited Dec. 1, 1999) <http://www.BBBOnLine.org/>.

323. *See* FEDERAL TRADE COMMISSION, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (1997).

online,[324] and has put in place extensive data protection regulation applicable to local telephone service[325] and cable television providers,[326] which rarely operate in markets offering consumers real competitive choice. In those and similar situations, the law provides important but carefully circumscribed, basic privacy rights, the purpose of which is to facilitate—not interfere with—the development of private mechanisms and individual choice as the preferred means of valuing and protecting privacy.

CONCLUSION

An ocean of ink has been spilled comparing European and U.S. privacy protection and predicting the impact of the EU data protection directive on U.S.-European relations. At its core, the impact of the directive will be measured by the provisions of the fifteen member states' national laws transposing the directive's requirements. As ten of those countries have yet to be heard from, and in the face of many and frequent political and technological developments, predictions about the future are not only uncertain, but also likely to be unwise. With that caution clearly in mind, however, I want to advance five observations about the changing face of privacy protection in Europe and the United States. While these may strike many readers as obvious, I believe they are important to understanding and perhaps even anticipating future developments.

A. The Value of Privacy and the Role of the Government in Protecting It

First, while Europe and the United States share many values, the systems of privacy protection reflected in the EU directive and U.S. law diverge most sharply on how much they value privacy, especially in competition with other goals, and on the appropriate role for the government in protecting privacy. The directive is based on the stated belief that information privacy is a basic human right, on par with the rights of self-determination, freedom of thought, and freedom of expression. Article 1 of the EU directive obligates member states to protect the "fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[327]

The primacy of the right to privacy is further reflected in the text of the directive, which permits member states to carve out exceptions "for the processing of personal data carried out solely for journalistic purposes or the purposes of artistic or literary expressions which prove necessary to reconcile the right to privacy with the rules governing freedom of expression,"[328] but only with regard to two of the directive's substantive provisions. Member states may create exceptions to the prohibition on processing sensitive data, and the requirement

---

324. *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

325. *See* 18 U.S.C. §§ 2510-2520, 2701-2709 (1997); 47 U.S.C. §§ 222, 1001-10 (1997).

326. *See* 47 U.S.C. § 551(a) (1997).

327. *Directive 95/46/EC*, *supra* note 44, art. 1(1).

328. *Id.* art. 9.

that data subjects be notified of information processing activities.[329] By the omission of any reference to the other substantive rights from the article permitting exceptions for expressive undertakings, it is clear that the directive's drafters believe that the protection of privacy is paramount to freedom of expression and the activities of the press and other authors and artists.

As a result of the extraordinary value, it places on information privacy, the EU data protection directive requires persons who wish to collect, process, use, store, and disseminate personal information to register with their national data protection supervisory authority. This scheme is anathema to the U.S. constitutional system, which so highly values freedom of expression and of the press, freedom from government intrusion, and protection of private property, and which frankly places less value on privacy. Privacy protection in the United States is fundamentally in tension with other values. Even if the law did not recognize these competing values and regard privacy as imposing both benefits and costs, the nation's constitutional commitment to a government of limited powers, particularly when expression is involved, poses a substantial obstacle to the creation of government privacy authority. This suggests a core difference between European and U.S. privacy protection: the extent to which the government is responsible for protecting information privacy. According to Jane Kirtley, former Executive Director of the Reporters Committee for Freedom of the Press:

> Privacy advocates urge the adoption of the European model for data protection in the name of protecting individual civil liberties. But in so doing, they ignore, or repudiate, an important aspect of the American democratic tradition: distrust of powerful central government. . . . [W]hen it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart. . . . The European paradigm assumes a much higher comfort level with a far more authoritarian government.[330]

B. The Restriction on Transborder Data Flow

Article 25 of the EU directive only exacerbates the divergence between EU and U.S. law by seeking to extend European privacy laws beyond the territories of the nations enacting those laws. This effort is understandable in light of the directive's treatment of privacy as a human right, and necessary if the privacy of European nationals is to be protected effectively in a global information economy. However, Article 25 is justifiably criticized as an effort to establish European protection for information privacy as a global standard. Because of the difficulty of separating data collected within Europe from data collected elsewhere, the directive effectively requires multinational businesses to conform

---

329. *See id.*

330. Jane E. Kirtley, *The EU Data Protection and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648-49 (1995).

all of their data processing activities to EU law or to self-regulatory or contractual provisions that mirror EU law. Even businesses that do not operate in Europe may run afoul of the directive if they collect, process, or disseminate personal data about European nations or via multinational networks.

As a result, U.S. businesses with interests in personal data collected, stored, or processed in Europe, and particularly U.S. businesses with operations in Europe, fear that they will be unable to move those data legally—even if they "own" them—to the United States.

The concerns of non-European information users are not misplaced. Although the directive only took effect in 1998, the British Data Protection Registrar has forbidden, under British law, a proposed sale of a British mailing list to a United States direct mail organization.[331] France, acting under French domestic law, has prohibited the French subsidiary of an Italian parent company from transferring data to Italy because Italy did not have an omnibus data protection law.[332] The French Commission nationale de l'informatique et des libertés has required that identifying information be removed from patient records before they could be transferred to Belgium,[333] Switzerland,[334] and the United States.[335]

The United States' fear about the impact of the directive is still further exacerbated by the EU Working Party's skepticism towards extra-legal protections for privacy. In the United States, industry self-regulation and private agreements are the primary means of protecting privacy. So the Working Party's conclusion that these should be the exception, not the norm, in measuring the adequacy of privacy protection decreases the likelihood that European data protection officials will find privacy protection in the United States to be "adequate."

At its heart, however, Article 25 is merely the most recent evidence of an expanding phenomenon: the effort to use national or regional law to deal with fundamentally global issues. As we have already seen, information is inherently global. It is because of its inherently global character that information has been the subject of some of the earliest multinational agreements, treaties, and organizations. Binational postal treaties were concluded as early as 1601 between France and Spain and 1670 between France and England.[336] The Postal Congress of Berne in 1874 established a multinational postal

---

331. *See* Office of the [UK] Data Protection Registrar, *Seventh Annual Report* 33-34 (1990).

332. *See* Délibération No. 89-78 du 11 juillet 1989, *reprinted in* Commission nationale de l'informatique et des libertés, 10e Rapport 32-34 (1989).

333. *See* Délibération No. 89-98 du 26 sept. 1989, *reprinted in* Commission nationale de l'informatique et des libertés, 10e Rapport d'activité 35-37 (1990).

334. *See* Reidenberg, *supra* note 38, at S163 (citing an interview with Ariane Mole, Attachée Relations internationales, Direction juridique de la Commission nationale de l'informatique et des libertés, Paris, France (Jun. 6, 1991)).

335. *See id.*

336. *See* Ludwig Weber, *Postal Communications, International Regulation*, 5 ENCYCLOPEDIA OF PUBLIC INT'L LAW 238 (1983).

regime—administered today by the Universal Postal Union—seventy-four years before the General Agreement on Tariffs and Trade was opened for signature.[337]

Today, when data processing is wholly dominated by networked computers, information is difficult to pinpoint and almost impossible to block, through either legal or technological means. Digital information not only ignores national borders, but also those of states, territories, and even individual institutions. Not surprisingly, the inherently global nature of digital information poses extraordinary challenges to the power of national governments, and efforts to use national law to deal regulate information in one jurisdiction often pose substantial legal and practical issues in another.

This is the conundrum that Article 25 has come to symbolize. If the directive did not extend to data processing activities outside of the EU, it would be certain to fail, because of the ease with which those activities can be moved off-shore. However, by extending its application beyond the jurisdiction of EU member states, the directive presents a host of international law issues, conflicts with the information law regimes of other nations, and is hardly more likely to be effective. If a regulatory approach is to be pursued, then global standards are necessary. But the conflict between the core values of the European and U.S. systems of privacy protection makes global consensus on effective privacy standards little more than a mirage. In short, national approaches to regulating information are becoming increasingly ineffective, at the very time that the economic power of information is increasing the pressure for national governments to pursue those approaches.

C. The Search for Compromise

Despite the profound differences in core principles undergirding U.S. and European privacy law, there is likely to be some accommodation between U.S. and European interests. Both European and U.S. officials have a significant economic interest in avoiding such a trade dispute, and both sides have thus far worked diligently to do so. European data protection officials have shown an increasing willingness to at least consider the privacy protection models offered by the rest of the world. The Working Party's later working documents, while still firm about the definition of "adequacy," are more moderate in tone than were earlier documents.

United States' officials, for their part, are growing more attentive to European officials and European concerns. At the same time, as already noted, both U.S. federal and state government officials are considering increased legislation and regulation to protect information privacy. While U.S. law is likely to satisfy the "adequacy" requirement of the EU data protection directive, all of this activity has given U.S. officials something to talk about, and European

---

337. *See id.*; General Agreement on Tariffs and Trade, *opened for signature* Jan. 1, 1948, 61 Stat. 5, 6, T.I.A.S. No. 1700, 55 U.N.T.S. 188. *See generally* Fred H. Cate, *Introduction—Sovereignty and the Globalization of Intellectual Property*, 6 IND. J. GLOBAL LEG. STUD. 1 (1998).

officials some sign of "positive" movement to seize on, during extensive U.S.-EU face-to-face exchanges designed to avoid confrontation over data protection.

Moreover, European data protection officials are interested in some level of compromise not only because of their own desire to avoid a trade war and the positive signs emanating from the U.S. government, but also because they are subject to considerable pressure from within Europe. While gaining new stature by virtue of passage of the directive, European privacy regulators are nonetheless subject to pressure from European businesses, which do not want their trading relationships with U.S. companies sacrificed in the interest of data protection; European consumers, who do not want to be denied the services and products offered by non-European organizations; and other government officials in European national governments and in the EU itself, who are anxious to avoid a trade dispute. And European officials responsible for trade, while not ignoring privacy issues, have demonstrated a broader, more optimistic view of EU-United States trade relations.

These trends are clearly in evidence in the current efforts of the U.S. Department of Commerce and Directorate General XV of the European Commission to negotiate a "safe harbor" to allow U.S. companies to comply with the directive, despite the absence of "adequate" data protection law in the United States. Under the safe harbor, "[o]rganizations within the safe harbor would have a presumption of adequacy and data transfers from the European Community to them would continue. Organizations could come within the safe harbor by self-certifying that they adhere to these privacy principles. The status quo ante would exist for firms that choose not to take advantage of the safe harbor."[338]

Judging from current drafts, the safe harbor principles are substantially meaningless; they simply restate the basic principles that undergird the directive.[339] Moreover, the negotiations appear to have run aground in recent weeks in the face of widespread opposition from both Europe and the United States. The negotiations do, however, reflect the efforts of U.S. and EU officials to find some common ground on data protection. A recent letter from Ambassador David L. Aaron, Under Secretary of Commerce for International Trade Affairs, to U.S. industry leaders signals the tone of the discussions:

> We have discovered that, despite our differences in approach, there is a great deal of overlap between U.S. and EU views on privacy. Given that and to minimize the uncertainty that has arisen about the Directive's effect on transborder data transfers from the European Community to the United States, the Department of Commerce and the European

---

338. Letter from Ambassador David L. Aaron, Under Secretary for International Trade Affairs, International Trade Administration, U.S. Department of Commerce, to "Industry Representatives," (Nov. 4, 1998), *available in* <http://www.ita.doc.gov/ecom/aaron114.html> [hereinafter Letter from Ambassador Aaron].

339. *See id.* <http://www.ita.doc.gov/ecom/menu.htm#Safe>; *see also* Comments of Fred H. Cate, Robert E. Litan, Joel R. Reidenberg, Paul M. Schwartz & Peter P. Swire on International Safe Harbor Principles <http://www.ita.doc.gov/ecom/comabc.htm#cate>.

Commission have discussed creating a safe harbor for U.S. companies that choose voluntarily to adhere to certain privacy principles.[340]

Moreover, it is also noteworthy that the negotiations involve DG XV, which deals with the internal market and financial services issues within the EU, rather than the Article 29 Working Party, which has responsibility for data protection.

In addition to governmental efforts, many U.S. businesses, individually and as part of industry associations, have engaged in a widespread campaign to inform European regulators about data protection in the United States, improve their own privacy practices, and develop innovative extra-legal guarantees of better privacy protection to EU data protection officials. Obviously, not all of these efforts are in response to European developments; U.S. businesses are reacting to domestic consumer and political pressure as well. But the actions of these businesses, however motivated, are expanding the room for compromise and increasing the likelihood that at least in some industry sectors in the United States, data protection will be found to be "adequate."[341]

Taken together, the efforts of the European and U.S. government officials, internal European pressures and lack of resources experienced by many European data protection officials, and the broad-based actions of at least some U.S. businesses seem likely to diminish the likelihood of a trade war resulting from enforcement from Article 25 of the EU data protection directive. Certainly there will be at least limited enforcement of Article 25, and some U.S. businesses—perhaps many—will be caught unaware. But the possibility of an outright trade war is remote.[342]

D. The Role of the Internet

Fourth, regulatory approaches to protection privacy seem ill-suited to the Internet. The EU directive purports to create broad protection for personal privacy, but it is ill-suited to a far-flung, inherently global medium such as the Internet, as EU data protection officials have acknowledged. Recall that the directive was drafted *before* the World Wide Web was even invented. In an expansive information economy, centralized control—based on registration and direct government oversight—cannot provide meaningful privacy protection. The directive was designed for a world in which data processing took place in comparatively few, easily identifiable locations, usually with mainframe computers. With the power and widely distributed technologies of the Internet and other digital networks, the directive's centralized approach to privacy protection is outdated. Moreover, national or regional controls are particularly easy to circumvent in the Internet environment, simply by moving data processing activities outside of the territory affected. Finally, the lack of

---

340. Letter from Ambassador Aaron, *supra* note 338.

341. *See, e.g.*, John F. Mogg, Comments to the European-American Business Council, Washington, DC (Mar. 18, 1998).

342. *See generally* Fred H. Cate, *The European Data Protection Directive and European-U.S. Trade*, CURRENTS vol. Vii, no. 1, at 61 (1998).

resources for government enforcement, especially when confronted with such widespread data processing, further diminishes the likely role of the directive as an effective means of protecting privacy online.

The U.S. legal system's protection for privacy online is similarly limited, although in very different ways. There is less of a gap between the level of protection promised by the law and the level actually delivered, because the law promises substantially less protection to U.S. citizens. At present, the law only directly protects privacy online in two settings: government collection and use of data, and the collection of data from children. Otherwise, individuals may use contracts, agreements with their Internet service providers, technological tools in Internet browsers and other software, and common sense to protect their privacy online. The law may be used to enforce private promises, but, in all areas other than government data processing and data collection from children, the law largely leaves citizens to their own devices, recognizing that the technologies of the Internet may be unusually effective in protecting privacy.

The technologies and current structure of the Internet largely frustrate regulation. That may not always be the case and that certainly does not mean that effective regulation is always impossible, but merely that it is time-consuming, expensive, and seldom effective for long. In the now-famous words of John Gilmore, one of the founders of the Electronic Frontier Foundation, "the Net treats censorship as damage and routes around it."[343] Encryption technologies, anonymous remailers, multinational access, and other features of the Internet make it comparatively easy for even unsophisticated users to avoid regulation, and information that is not available from one online source is almost certain to be obtainable from another. The effect of much regulation of Internet content is simply to discourage law-abiding information providers, thereby leaving a gap that is often filled by less scrupulous providers.

These same technologies that distort the application of laws and facilitate their evasion also provide important tools for protecting vital interests. Digital technologies offer individuals enormous privacy protection and the ability to access information with disclosing anything about themselves. This is not to suggest that technologies are a panacea or that law is irrelevant, but simply that the Internet is empowering many people to protect their rights in a way that the law so far has been able to.

E. The Future of U.S. Information Law

Finally, while the EU system of data protection may be well suited to Europe, privacy protection in the United States responds to core values in this society and system of government. Certainly, that protection may be improved, but U.S. government and business leaders should avoid imposing costly new privacy protection merely as a sop to European data protection officials. As noted, the four-part approach to information privacy in the United States highlights important limits on that protection, reflected in U.S. law, markets, and

---

343. Judith Lewis, *Why Johnny Can't Surf*, L.A. WKLY., Feb. 21, 1997, at 43.

consumers. Those limits protect other important values, such as free expression; they avoid imposing unnecessary costs on commercial and social interaction of all forms, especially electronic; and they protect against creating the illusion of government-enforced privacy while in fact interfering with the development and use of more practical means for protecting information about individual citizens.

At heart, the debate about information privacy is fundamentally one about controlling information. Privacy is often confused with other issues—security, reliability, verifiability, anonymity, and so on—and to be sure it relates to other concepts; but at its core privacy is about who controls the collection, dissemination, storage, and use of information about individuals; under what authority or compulsion do they exercise that control; and what responsibilities, if any, attend that control.

In the United States, the law has historically prevented the government from exercising control over information collection and dissemination by private individuals and institutions. The law may require disclosure of certain information, especially to facilitate self-governance and open markets, but it rarely prohibits disclosure. Instead, U.S. law most often places control over information in the hands of citizens.

The U.S. approach to information privacy inevitably results in some harm to individuals' privacy, reputations, and sensibilities. But it reflects a constitutional calculation that such harm is less threatening to the body politic than the harm associated with centralized privacy protection, government interference with the information flows necessary to sustain democracies and markets, and the growing ineffectiveness of omnibus legal controls in the face of the widespread proliferation of powerful information technologies. We should be loathe to alter that delicate constitutional balance lightly, by granting to the government new authority to interfere with the flow of information in the search for new—but often illusory and costly—protection for personal privacy.