Vanderbilt Journal of Transnational Law

Volume 35
Issue 2 *March 2002*

Article 7

2002

The European Union Data Privacy Directive and International Relations

Steven R. Salbu

The European Union Data Privacy Directive and International Relations

*Steven R. Salbu**

ABSTRACT

This Article explores the European Union Data Privacy Directive and its impact upon international relations. Part II provides a background upon which the Privacy Directive is built. In Part III, the Article confronts the differences between how the United States and its European counterparts address privacy issues generally. Part IV analyzes the Privacy Directive in detail, while Part V explores possible effects that the Privacy Directive might have on international relations.

TABLE OF CONTENTS

I. INTRODUCTION 656
II. A PRIMER ON CONTEMPORARY DATA PRIVACY ISSUES .. 657
III. EUROPEAN VERSUS U.S. PHILOSOPHIES AND APPROACHES TO PRIVACY 665
IV. THE EU DATA PRIVACY DIRECTIVE 668
A. *Restrictions on Collection and Use of Data* 669
1. Opt-in Rights 670
2. Access and Objection Rights 671
a. Access Rights 672
b. Objection Rights 673
B. *Restrictions on Data Flows to Countries Lacking Adequate Privacy Protections* 675
1. U.S. Safe Harbor Provisions Development and Negotiation 678
2. The Nature of the Safe Harbor Principles 680
V. THE EU APPROACH AND INTERNATIONAL RELATIONS ... 685

---

* Associate Dean for Graduate Programs, Bobbie and Coulter R. Sublett Centennial Professor, University Distinguished Teaching Professor, University of Texas at Austin. B.A., Hofstra University; M.A., Dartmouth College; J.D., College of William and Mary; M.A., Ph.D., Wharton School of the University of Pennsylvania. The Author would like to thank participants in the University of Michigan's Conference on Corporate Governance, Stakeholder Accountability, and Sustainable Peace for their helpful comments and suggestions. Special thanks go to Tim Fort and Cindy Schipani, the Conference's faculty organizers.

A. *The Challenge* 685
1. The Potential for Enhanced International Relations, Human Rights, and World Peace 685
2. The Potential for International Strife .. 687
a. Time 687
b. Space 688
B. *The EU Data Privacy Directive as an Approach to Internet Governance* 689
1. Does the Directive Capture a Global Perspective on Privacy? 690
2. The Future of the Data Privacy Directive's Outward Reach After September 11, 2001 693
VI. CONCLUSION 695

I. INTRODUCTION

Recently, the European Union passed the Data Privacy Directive (Directive), under which Member States are required to enact implementing legislation.[1] The Directive is the world's most ambitious and far-reaching data privacy initiative of the high-technology era. Its global pervasiveness, and therefore its extraterritorial effects, raise interesting questions regarding tension between the goal of uniform Internet policies and the importance of respecting sovereignty and national autonomy. The resolution of this tension may ultimately affect international relations in the new century.

This Article examines these dynamics. Part II is a primer on contemporary data privacy issues, the foundation upon which the EU Directive is built. Part III briefly discusses differences between U.S. and European approaches to these privacy issues, highlighting a present lack of global uniformity, even among two Western, developed, regional economies. Part IV analyzes the EU Directive and includes some critical observations, highlighting potential pitfalls and shortcomings. Part V looks at the relationship between the EU approach and international relations, examining possible effects on the furtherance or hindrance of a harmonious and cohesive world community.

---

1. Data Privacy Directive, Council Directive 95/46/EC, 1995 O.J. (L 281) [hereinafter EU Directive].

II. A PRIMER ON CONTEMPORARY DATA PRIVACY ISSUES

Privacy is a concern that obviously predates modern technology.[2] It is also easily taken for granted. As one scholar observes, privacy is a lot like freedom: people do not appreciate its value and importance until it is threatened or lost.[3] In an era of burgeoning information technology, privacy also can become an afterthought, a secondary consideration in the race to find and exploit the next cutting-edge development.[4]

Since the 1980s, but prior to public diffusion of developing Internet technology, legal scholars recognized how seriously computers can threaten privacy.[5] The advantages of technology come at a price: one person's "enhanced information" can invade another person's privacy.[6] This double-edged sword naturally creates conflict, based on both self-interest and ideology.[7]

Reasons for concern have escalated, and they continue to grow. Privacy is becoming increasingly susceptible to ever more sophisticated technologies. Electronic identification cards, wiretaps, biometrics, and video surveillance cameras all have the potential to erode privacy.[8] Digital interactive television technology soon may tell advertisers exactly which programs people view in their homes,

---

2. Andrew J. Frackman & Rebecca C. Martin, *Surfing the Wave of On-Line Privacy Litigation*, N.Y. L.J., Mar. 14, 2000, at 5 (observing that privacy concerns and fears of government and corporate collection of data pre-date the Internet).

3. David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. L. REV. 831, 831 (1991).

4. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1286 (1998) (noting that privacy issues were historically afterthoughts, and that as technology drives people to continue making rapid advances, they react only "after the fact" to technology's social consequences).

5. *See, e.g.*, Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1997) (recognizing that computer technology creates threats to privacy that were unimaginable shortly before the technology's development, and discussing these threats in detail).

6. *See, e.g.*, Elizabeth deGrazia Blumenfeld, Survey, *Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before the Government Steps In?*, 54 BUS. LAW. 349, 351-52 (1998) (observing that the Internet's great promise is accompanied by great risk in the form of potential privacy invasions).

7. The conflict of self-interest is as follows: companies marketing their own products or the products of others have reason to be wary of losing the capabilities created by Internet technology to legal or regulatory constraints. On the other hand, many data subjects will be interested in constraining marketing efforts in order to protect their personal privacy. For a discussion of the conflicting ideologies, see *infra* notes 49-57 and accompanying text.

8. Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L. REV. 661, 662-63 (1999).

refining target advertising[9] in ways that are potentially both beneficial and frightening.[10]

No modern technology poses a greater threat to privacy than the Internet.[11] Interactive computer technology allows researchers to collect data more cheaply and efficiently.[12] Conversion of data into binary form enables the common person to store, use, and misuse data in powerful new ways.[13] Computer technology also allows commercial and other entities[14] to accomplish data collection tasks more quickly and inexpensively.[15] What once took days of manual labor now can be accomplished with a keystroke; what once required substantial capital now can be achieved by anyone with a computer and a modem.[16]

By the late 1990s, the potential had become a reality, as a Federal Trade Commission (FTC) survey analyzed 1402 websites and concluded that ninety-two percent collected personal data, and that the majority did so without posting privacy disclosure statements.[17]

---

9. Tom Foremski, *Digital Interactive Television*, FIN. TIMES, July 5, 2000, at 11 (describing new technologies being pursued by companies such as Microsoft, DirectTV, and AOL, through which the fusion of television and computers will enable two-way communications between programmers and viewers).

10. For discussion of the latest developments in this area, see Shelley Emling, *Digital Opens Up Future of Cable TV: Technology Adds Money-Making Options for Companies, Services for Customers*, AUSTIN AM.-STATESMAN, July 28, 2001, at A1. The potential benefit to consumers is improvement in the utility of the advertising viewed. *Id.* While some may see this as a positive change, it may be frightening to others who dislike becoming increasingly vulnerable to what they see as marketing and advertising wiles. *Id.* Moreover, the very notion that programmers and advertisers are collecting information about consumers as they watch television is disturbing. *Id.*

11. Marilynn Larkin, *Web privacy worries won't go away*, LANCET, April 22, 2000, at 1471, *available at* 2000 WL 9005462 (observing that, in the United States, Internet privacy breaches are reported in the news daily).

12. Edmund Sanders, *For Sale: Your Personal Data—Cheap, Easy, OnLine*, L.A. TIMES, June 24, 2000, at A1 (observing that personal information is increasingly available to everyone, not just to specialty marketers and brokers able to pay steep prices).

13. Michael W. Heydrich, Note, *A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOK. J. INT'L L. 407, 408-09 (1999) (noting that "[w]ith the capacity to convert data into binary form, the ability to store and use personal data has increased significantly, thus making the individual's personal information more susceptible to misuse.").

14. The threat to privacy is posed not only by commercial firms, but also by other entities and organizations. Government agencies are an obvious example. Recently, the FBI has come under scrutiny and criticism for the data surveillance system that it, perhaps imprudently, called "Carnivore." FBI surveillance via Carnivore has raised search and seizure concerns, in addition to more generic privacy concerns. *See generally* Jon Baumgarten et al., *FBI's E-Mail "Wiretap" Under Scrutiny*, 5 CYBERSPACE LAW. 28 (2000).

15. Sanders, *supra* note 12.

16. *Id.*

17. Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶ 11 (1999), *at* http://www.richmond.edu/jolt/v6i1/belgum.html (citing Federal Trade Commission, Privacy Online:

More anecdotally, Professor Sovern describes modern media as "filled with horror stories about the use of personal information."[18]

Lack of disclosure is a serious problem. Internet-enhanced invasion of privacy can be especially insidious because the technology facilitates the collection of personal data without the knowledge of the subject.[19] Among the more disturbing concerns is the collection of identifying information, such as address, social security number, medical information, financial information, and credit card information.[20]

Some critics of the non-consensual flow of personal information posit property arguments in support of the electronic privacy movement.[21] They contend that the subjects of personal information have the right to control its use, including the right to sell it.[22] Some property-based discussions appear to be based on conceptions of fairness.[23] Others have focused on the purported externalities pertaining to uncompensated use of private data.[24] Still others have discussed property-related policy approaches to privacy issues, such as the possibility of licensing private information.[25] In a world where

---

A Report to Congress, June 1998, *available at* http://www.ftc.gov/reports/privacy3/toc.htm).

18. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1035 (1999) (detailing examples of the amounts and varieties of information that can be accessed inexpensively by anyone, including a reporter identifying himself with the name of a man on trial for kidnapping and murder).

19. Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 505 (1999) (observing that data collection in cyberspace is invisible—*i.e.*, occurs without the knowledge of the person about whom data is being collected).

20. Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1, ¶ 4.

21. Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 687 (2000).

22. Bartow observes, "[I]f information about us is to be bought and sold, the initial purchase should be from us, since we are the ultimate content providers. If intangible property rights are rewards for the effort expended in creating the thing to be protected, we are entitled to ownership of our personal information." *Id.* at 687.

23. Belgum, *supra* note 17, ¶¶ 39-40 (arguing that "[p]rivacy market opportunists begin with the assumption that, even though privacy may be a 'fundamental human right,' that does not mean that individuals should not have the ability to decide for themselves how much that right is worth to them personally, and whether to sell, trade or give away their private information in their own self-interest.").

24. Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97, 103 (2001) (noting that "websites benefited through the largely unrestricted collection of personal data while consumers suffered injury due to the degradation of their personal privacy from this data collection. In other words, degradation of consumer privacy resulted as a third-party externality of free-market data-collection norms of the website industry.").

25. *See generally* Kalinda Basho, Comment, *The Licensing of Our Personal Information: Is it a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507 (2000).

companies pay or otherwise compensate consumers for personal information with increasing frequency,[26] expectations regarding information rights are likely to shift.

The property rights approach is appealing because it both recognizes and accommodates different preferences and priorities among consumers. Under this approach, those consumers who value their privacy highly need not sell the rights to personal data and information; those who place a lower value on privacy are free to sell their data and information.[27]

There are also good arguments in favor of maintaining the freest possible flow of information, including personal information. Society benefits from increased access to information.[28] Some commentators suggest that the free collection and use of information benefits not only businesses, but also consumers and society at large,[29] and that current pro-privacy trends may therefore more accurately be classified as "privacy panic."[30] Consumers ostensibly benefit by receiving more pertinent information, as companies better target their advertising to personal interests;[31] society ostensibly benefits as better, more efficient marketing supports e-commerce and a thriving economy.[32] In addition, all users benefit from free Internet services that are sponsored by advertisers. If Internet advertising fails to be effective, advertiser sponsorship will decline and the public could lose

---

26. Eric J. Sinrod et al., *The New Wave of Speech and Privacy Developments in Cyberspace*, 21 HASTINGS COMM. & ENT. L.J. 583, 592 (1999) (discussing programs in which online marketers provide free personal computers to consumers in exchange for monitoring rights and demographic data).

27. Eve M. Caudill & Patrick E. Murphy, *Consumer Online Privacy: Legal and Ethical Issues*, 19 J. PUB. POL'Y & MARKETING 7, 8 (2000). "A continuum suggests that consumers have varying degrees of concern with privacy and place different values on their personal information; therefore, some consumers may be willing to trade away information for a more valued incentive." *Id.*

28. Blumenfeld, *supra* note 6, at 350 (recognizing the Internet's potential to serve society as "the next commercial marketplace").

29. James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145, 150 (2001). "[T]he open flow of information not only comports with the U.S. system of self-governance, it also assists in promoting commerce, and providing citizens with significant economic and social benefits." *Id.*

30. Pamela Paul, *What Are Americans Afraid Of? Mixed Signals; When It Comes to Issues of Privacy, Consumers are Fraught with Contradictions*, AM. DEMOGRAPHICS, July 2001, at 46.

31. Robert O'Harrow, Jr., *Private or Not?; Behind the Scenes, Web Site Operators Are Gathering Information on their Visitors, A Practice that Treads the Line Between Customer Service and Invasion of Privacy*, WASH. POST, May 17, 2000, at G22 (comparing e-commerce profiling with business's historic use of memory to serve customers by knowing their personal preferences).

32. Wendy Muller, *The High Cost of Net Privacy*, STRATEGY, May 8, 2000, at 20 (providing social and economic reasons why a free Internet needs to protect business's ability to deliver effective advertisements).

many useful sites.[33] Any means of improving advertising effectiveness is also a means of supporting a robust web of services, available without charge.[34]

Skeptics counter that, unless people are careful, the benefits will come at a serious cost to personal privacy.[35] The threat comes from the government as well as the private sector.[36] Although technology can be used to circumvent the privacy of consumer information,[37] policies can be established to protect these rights.[38] Companies can be required to notify people of their intent to collect, use, or distribute personal information,[39] as well as to provide consumers with meaningful control over whether—and if so, how—these processes occur.

Specifically, both opt-in and opt-out policies provide a measure of consumer privacy protection, although the former are stronger than the latter.[40] Opt-in policies prohibit businesses from collecting, using, or sharing[41] personal information unless the subject of that

---

33. *Id.*

34. O'Harrow, *supra* note 31 (quoting DoubleClick's director of public policy, Josh Isay, who noted that "'[i]n order to keep the Internet free, Web sites need to be profitable. And in order to be profitable, they need targeted ads that work.'").

35. Robert L. Hoegle & Christopher P. Boam, *Putting a premium on privacy protection policies*, NAT'L L.J., Aug. 21, 2000, at C8 (citing consumers' and regulators' concerns about potential misuse of customer information).

36. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 LAW & POL'Y INT'L BUS. 275, 278 (1998) (noting that the federal government began collecting substantial personal information by the beginning of the 1970s).

37. This emphasis on consumers' "own information" raises questions regarding whether consumer information can be owned, and if so, how property interests in consumer information are to be determined. For one sample discussion of information ownership, see John Caher, *Privacy Initiative Aims for Consumer Protection*, N.Y. L.J., Jan. 24, 2000, at 1 (quoting New York Attorney General Eliot Spitzer, who stated that "'[e]verybody—on the left politically, in the middle politically, on the right politically—has come to an understanding that with technological changes, the capacity of an individual to maintain ownership of information about himself or herself is being diminished in a very significant way.'").

38. Jonathan Cox, *Senate, House Plan to Address Net Privacy*, CHI. SUN-TIMES, July 12, 2001, at 54 (noting companies are creating policies and practices to ensure privacy protections for users of the Internet).

39. "Personal information" usually refers to information that can be associated with a particular individual—*i.e.*, information that is tied with a person's name—rather than to information that would be considered highly confidential. This means that information that might be obvious, such as gender, would be considered personal, and that information not ordinarily considered sensitive is also included.

40. Stephen R. Bergerson, *Electronic Commerce in the 21st Century: E-Commerce Privacy and the Black Hole of Cyberspace*, 27 WM. MITCHELL L. REV. 1527, 1554-55 (2001) (explaining that while opt-in policies provide stronger protection to consumers, they do come with potential disadvantages, including costliness and impracticality for businesses).

41. Opt-in policies and opt-in legal requirements can be fashioned to prohibit any or all of these activities. A weaker opt-in policy or law might prohibit only sharing

information has expressly agreed to these activities.[42] Under an opt-in policy, the default assumption is that every consumer expects privacy.[43] The assumption can be rebutted only through voluntary and affirmative consumer consent. Opt-out policies prohibit businesses from collecting, using, or sharing[44] personal information only after a consumer has taken the initiative to inform the appropriate person or entity of objections to the relevant activities.[45] In contrast to opt-in policies, the default assumption in opt-out policies is that a given consumer does not have privacy expectations regarding relevant activities, such as collecting, using, or sharing the data.[46] To trigger the privacy protections that are automatic under an opt-in policy, a consumer must take the initiative and follow the prescribed steps.[47]

In many instances, companies collecting data do not conspicuously inform individuals of their opt-out rights or provide them with instructions and contact information for exercising their rights.[48] In these cases, the consumer must be willing to investigate the procedure and the details of implementation in order to exercise their rights. It is likely that these dynamics impede the assertion of opt-out privileges in many cases. While consumers most concerned with privacy are more likely to go to the trouble, those who are moderately concerned are less likely to expend the resources necessary to exercise their opt-out rights. Even among consumers

---

prior to opt-in, whereas a stronger opt-in policy might prohibit all the enumerated activities.

42. Keith Rodgers, *Telecoms Media Technology: Out of the Valley—The Battle Is On For Consumer Privacy*, INDEP. (London), Sept. 2, 2001, at 8 (describing opt-in policies as placing the onus on companies to get consumers' authorization before sharing data).

43. Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and Practice*, 7 J. INTELL. PROP. L. 57, 69 (1999) (observing that opt-in policies provide greater protection than opt-out policies because opt-in policies adopt non-use and non-disclosure as default assumptions).

44. *See supra* note 41 and accompanying text.

45. Allen E. Cooper, *Privacy Policies: Financial Information Shouldn't Be Shared*, MILWAUKEE J. SENTINEL, June 16, 2001, at 12A (noting that "[p]eople have been receiving customer privacy notices from the financial companies they deal with, and the notices state that customers must notify the companies if they do not want their personal information shared with other companies.").

46. Lawrence Jenab, Comment, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 667-68 (2001) (discussing opt-in and opt-out policies in terms of the default rules that they apply).

47. Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1497 (2001). "The amount of time, inconvenience, and cost of exercising an opt-out right is substantial." *Id.*

48. *See id.* at 1496-97 (explaining that many U.S. consumers are unaware of their opt-out rights, and that there are few incentives for companies to provide conspicuous notice of rights or other forms of opt-out related disclosure).

with high privacy-concern levels, some will be too busy or distracted to pursue an interest that they consider very important.

Some commercial interests and opponents of privacy advocates counter that opt-in and other aggressive policies add unnecessary or even prohibitive costs to doing business.[49] Anti-regulation arguments are bolstered by data suggesting that theoretical privacy concerns may not be very important to real consumers. For example, when New York Telephone enabled customers to opt out of a mailing list it intended to share with direct marketers, only 800,000 of 6.3 million customers exercised the option.[50]

Of course, privacy advocates can challenge the significance of this information on at least four grounds. First, 800,000 is a large number in absolute terms, and even as a proportion it is not a trivial percentage of offerees. Second, some of those who did not opt out in this case might do so in another case. For example, they might have considered the particular terms of the marketing practices proposed by New York Telephone to be either personally desirable or innocuous, yet would opt out under other circumstances. Third, the distribution of opt-out decisions may be a poor proxy for whether consumers consider the choice itself to be important. One may decide in a particular case not to opt out, but still view the right to make the decision as fundamental. Finally, privacy rights cannot be measured strictly quantitatively. A minority can consider their privacy to be a very precious thing. The possibility that some do not share the concerns of the minority should not detract from the legitimacy of that concern.

In short there are privacy advocates and there are opponents of privacy advocates—not surprising, given the tradeoffs between use of information and abuse of information. Privacy advocates emphasize the price of information-sharing; opponents emphasize the benefits of information sharing.

The "benefit-at-a-price" model of information processing applies to many of Internet innovations. For example, on-line medical data can be an enormous boon to individuals, who now can provide doctors around the world with instant access to their medical histories in the event of an emergency.[51] Globe-traveling patients also can communicate quickly and inexpensively with their own doctors via e-

---

49. Dale E. Ramsey, Letter to the Editor, KAN. CITY STAR, July 22, 2001 (writing that "[w]hen Congress attempted to deal with privacy and financial institutions, the 'opt-in' approach—where individuals would initiate giving permission for use of their private information—was discarded under pressure from business. The argument? Too costly for business.").

50. ANNE W. BRANSCOMB, WHO OWNS INFORMATION? 15 (1994).

51. Jane E. Allen, *ER Doctors Often Face a Shortage—of Patient Info*, L.A. TIMES, May 15, 2000, at S1 (noting the ability of information systems to improve emergency health care by giving providers important treatment information regarding the patients they serve).

mail.[52] In the words of the M.D. Anderson Center's Chief Information Officer, "The Internet will fundamentally transform the way we conduct health care in this country and the world."[53]

When on-line personal medical information gets into the wrong hands, however, the intended beneficiary of data processing can become a casualty, as in employment or insurance discrimination.[54] On-line financial data bear similar benefits and risks, as desirable facilitation of financial transactions is countered by possible undesirable flow of information to unauthorized recipients.[55]

The down-side of the information revolution is troublesome both in its own right and because of its broader implications. Potential privacy violations are obviously disturbing in both their intrusiveness and their ability to harm individuals.[56] Moreover, the prospect of privacy violations can have negative economic effects, impeding the development of e-commerce if consumer mistrust undermines adoption of the Internet for commercial transactions.[57]

Like many other policy challenges posed by the Internet,[58] today's privacy concerns were not as compelling a decade ago, because the technology is so new and powerful, and is changing so quickly.[59] More than ever, the speed of innovation and attendant social change[60] deprives lawmakers and regulators around the world of time

---

52. For a discussion of this phenomenon and the privacy challenges it poses, see Allisa R. Spielberg, *Online Without a Net: Physician-Patient Communication by Electronic Mail*, 25 AM. J.L. & MED. 267 (1999).

53. Laura Goldberg, *Doctors, hospitals find multiple uses for e-Information*, HOUSTON CHRON., May 21, 2000, at 38, *available at* 2000 WL 4301089 (quoting Mitchell Morris, chief information officer at M.D. Anderson Cancer Center).

54. Allen, *supra* note 51, at S1. "High-tech solutions that link personal medical histories to the Internet or scannable cards that reveal sensitive data could compromise careers or insurance if the information fell into the wrong hands." *Id.*

55. Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 481 (1999) (noting, in the context of government surveillance, the possibility that financial data may flow to "unauthorized third parties").

56. *See generally* CAI Elec. Comm. Advisory Council, *Protecting One's Privacy*, E-COMMERCE REP., *at* http://www.e-commerce.ca.gov/1e_privacy.html (discussing an array of consumer privacy interests in the context of the Internet).

57. Chris Tolhurst, *Big Brother Fears Fuel Net Reluctance*, AUSTRALIAN FIN. REV., Sept. 20, 1999, at 40, *available at* 1999 WL 19339664 (calling privacy-related consumer mistrust the greatest drawback for e-commerce businesses).

58. Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1205 (2000) (observing that the idea of Internet regulation in general began only in the 1990s, once the technology began to serve as a society-wide medium for communications).

59. Editorial, *Construct Politics with an Eye to the Future*, DAILY YOMIURI (Tokyo), Jan. 10, 2001, at 6, *available at* 2001 WL 3965175. "The nation and its people are confronted by a host of great changes due to the accelerated pace of globalization, rapid progress in the information technology revolution and the development of new technologies." *Id.*

60. Julia M. Fromholz, *The European Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 461 (2000) (tying growing concern about protection of personal data to

for careful, deliberate consideration of the implications of new technology and the best ways to address those implications. This pressure is exacerbated by the international character of globe-spanning technologies, which increase the number of stakeholders as well as the complexity of policy-making.[61] Despite these sub-optimal conditions for creating rules of the game, the modern proliferation of the media, largely fueled by Internet technology, heightens the pressures placed on lawmakers to respond, perhaps more quickly than ever before.[62]

No one has responded more quickly or more vigorously to modern privacy challenges than the European Union. The section that follows describes the philosophical differences between the European and U.S. approaches to contemporary privacy challenges.

III. EUROPEAN VERSUS U.S. PHILOSOPHIES AND APPROACHES TO PRIVACY

Protection of personal data is an issue throughout the world, and all nations face similar challenges to some degree. The drama that has played out in Europe and the United States, while the most prominent example of the struggle between commercial interests and privacy interests, is far from the only one. In addition to nations grappling with legislative responses, non-governmental organizations such as the Organisation for Economic Cooperation and Development (OECD) have addressed data privacy issues.[63] What follows is a discussion of the most highly publicized international engagement with data privacy issues to date—discussions and negotiations between Europe and the United States.

Privacy is considered a fundamental right in both Europe and the United States.[64] Beyond this generalization, however, European

---

the rapid spread of computers and computer networks and the unprecedented capacity to collect, analyze, and disseminate data inexpensively and easily).

61. Leon A. Kappelman, *The Big Picture: Working in the Global Village*, INFORMATIONWEEK ONLINE, Mar. 20, 2000, *at* http://www.informationweek.com/778/78uwlk.htm (observing that each additional political boundary adds legal and other complexities to global information technology management).

62. Eric M. Reifschneider, Book Note, 3 HARV. J.L. & TECH. 253, 254 (1990) (reviewing M. ETHAN KATSH, THE ELECTRONIC MEDIA AND THE TRANSFORMATION OF LAW (1989)) (discussing the relationship between modern media, law, and social change).

63. Organisation for Economic Cooperation and Development, *1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *available at* http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

64. Nicole M. Buba, Note, *Waging War Against Identity Theft: Should the United States Borrow from the European Union's Battalion?*, 23 SUFFOLK TRANSNAT'L L. REV. 633, 641 (2000).

and U.S. approaches to privacy have differed historically.[65] According to policy analyst Ari Schwartz, European nations have a "vision" regarding privacy rights that is absent in the United States.[66] Privacy considerations that may be considered negligible in the United States are taken very seriously by the European Union.[67]

The European emphasis on personal privacy rights[68] may be attributable in part to Third Reich abuses in tracking its target groups with invasive data-collection methods.[69] Today, European nations are more likely to erect broad, prophylactic legislative protections, whereas the United States tends to protect privacy by reacting to crises.[70] The statutory privacy protections that do exist in the United States have historically focused on the public sector,[71] while the EU Data Privacy Directive extends to both public and private sectors alike.[72]

Much of the modern debate over data privacy has focused on self-regulation and technological solutions, rather than legal and regulatory responses.[73] Where the United States has favored self-regulation by business, Europe has preferred strict consumer-protection legislation that is capable of guarding privacy rights across

---

65. Editorial, *Privacy Here and Abroad*, WASH. POST, Oct. 31, 1998, at A16 (observing "sharp" differences between the two approaches).

66. James Evans, *Privacy Debate Rages*, INFOWORLD DAILY NEWS, July 12, 2000, *available in* LEXIS, Nexis Library, Allnws File (quoting Ari Schwartz, policy analyst for the Center for Democracy and Technology).

67. This difference is notable not only in comparing the EU Data Privacy Directive to less stringent U.S. protections, but also in other areas of privacy. Most recently, for example, the European Union has begun moving toward a unified opt-in policy in regarding to Spam, which would replace the less rigorous opt-out policies presently in place in a number of Member States. *See* Elizabeth De Bony, *EU Puts Brakes on Spam*, INFOWORLD DAILY NEWS, July 20, 2000, *available in* LEXIS, Nexis Library, Allnws File.

68. The European emphasis on privacy rights is not, of course, impervious to gaps and omissions. For example, one study recently found U.S. Internet businesses are more likely to post privacy policies than European Internet businesses. Specifically, ten percent of European sites examined posted privacy policies, whereas sixty-six percent of U.S. sites examined posted privacy policies. For a discussion on this issue, see *Tech Watch: Data Protection—For Your Eyes Only: Privacy on the Web*, TIME, Dec. 13, 1999, at 18.

69. Monahan, *supra* note 36, at 283.

70. Fromholz, *supra* note 60, at 462 n.1.

71. The Author does not suggest that the private sector is never subject to privacy laws, but rather indicates a general trend which may be changing as the United States begins to take privacy interests more seriously.

72. Heydrich, *supra* note 13, at 426 (observing that the EU Data Privacy Directive, which applies to both public and private sectors, provides greater protection than U.S. statutes which generally apply only to the public sector).

73. Peronet Despeignes, *Exorcising the Ghost in the Internet Machine*, FIN. TIMES, Feb. 28, 2001, at 14. "On one hand are high-technology companies promoting self-regulation and innovations that protect people's privacy; on the other, lawmakers determined to 'do something.'" *Id.*

international borders.[74] Not surprisingly, U.S. commentators are also more likely than European commentators to recommend market-based alternatives to legislation and regulation.[75] When the United States does decide to address privacy through laws, it usually applies a "sectoral approach,"[76] passing laws to cover particular industries or areas such as credit reporting,[77] education,[78] financial privacy,[79] telephony,[80] cable,[81] and video.[82] In contrast, Europe and nations such as Canada, Australia, and New Zealand have enacted omnibus data privacy laws, "covering the full spectrum of uses of personally identifiable information."[83] The legislation is broad and comprehensive, applying to both public and private sectors.[84] And unlike the United States, some European countries expressly guarantee privacy in their constitutions.[85]

Because Europe has taken the lead in the formation of ambitious, serious privacy legislation, EU law in this field is a fascinating subject for examination and analysis. The following section looks at the centerpiece of modern European privacy controls: the EU Data Privacy Directive.

---

74. *See* John R. Aguilar, *Over the Rainbow: European and American Consumer Protection Policy and Remedy Conflicts on the Internet and a Possible Solution*, 4 INT'L J. COMM. L. & POL'Y 1, 13-14 (1999) (describing the U.S. stance favoring development of internal business transparency mechanisms, and the European stance favoring formal laws ensuring protection of e-consumers).

75. *See, e.g.*, Paul Rose, Comment, *A Market Response to the European Union Directive on Privacy*, 4 UCLA J. INT'L L. & FOREIGN AFF. 445, 450 (1999). "[B]ecause of the deep U.S. commitment to self-regulation and to the Safe Harbor Principles, comprehensive privacy legislation is unlikely, and, as I argue, unnecessary. Although the *data* market has failed consumers, privacy concerns can still be resolved through market forces—through the creation of a *privacy* market." *Id.* (emphasis added).

76. Beth Givens, *Privacy Expectations in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 347, 348 (2000).

77. Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994).

78. Family Education and Privacy Rights Act, 20 U.S.C. § 1232(g) (1994).

79. Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22 (1994).

80. Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991).

81. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2780 (1984) (codified at 47 U.S.C. §§ 521-59).

82. Video Privacy Protection Act, 18 U.S.C. § 2710 (2000).

83. Givens, *supra* note 76, at 348-49.

84. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431 (1995).

85. Monahan, *supra* note 36, at 283 (stating that privacy rights appear in the constitutions of "many" European nations, and referring to Germany's constitution as one example).

IV. THE EU DATA PRIVACY DIRECTIVE

The EU Data Privacy Directive is built on a tradition of serious privacy protections. Comprehensive European data privacy legislation dates as far back as 1973, when Sweden passed early, groundbreaking legislation.[86] Trans-European initiatives began as early as 1981, when the Council of Europe solicited signatories to the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data.[87] Because this Convention was not self-executing, signature and subsequent ratification varied among European nations so that privacy assurances varied from one country to another.[88]

The European Union set a high global standard in data privacy protection when it forged its Data Privacy Directive,[89] which became effective in October 1998[90] and created a global model of a rigorous legislative approach to privacy.[91] More specifically, it has been described as "a top-down, mandated . . . approach to the issue of data privacy," in contrast to the U.S. "mix of legislation, regulation, and self-regulation."[92] Like all EU Directives, it is not in itself a law; rather, it directs each of the fifteen members of the European Union to enact its own implementing legislation, which need not be identical across Member States in many of its specifics.[93]

The Directive's origins may seem ironic today, considering the threat it poses to the flow of information from the European Union to

---

86. Patrick E. Cole, *New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws*, 17 N.Y.U. J. INT'L L. & POL. 893, 902-03 (1985).

87. *See* Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, European Treaty Series, No. 108.

88. *See* Fernand Keuleneer & Dirk Lontings, *Privacy Protection and Personal Data Processing in Belgium: Analysis of a New Law's Centralized Approach to Regulation*, 4 INT'L COMPANY & COM. L. REV. 344, 344-45 (1993) (noting Belgium's early failure to ratify the Convention, and subsequent criticism of its data privacy protections).

89. EU Directive, *supra* note 1.

90. Kendra L. Darko, *Someone's Watching*, AM. DEMOGRAPHICS, Aug. 1999, at 16.

91. *See, e.g.*, Dana James & Kathleen V. Schmidt, *Brazil Net: Growing Demand Tempered by Privacy Regulations*, MARKETING NEWS, Sept. 27, 1999, at 40 (reporting a privacy law proposal in Brazil similar to the EU Data Privacy Directive).

92. Sherman Katz & Edward Meyers, *The Threat to U.S. Companies Created by the EU Data Privacy Directive*, METROPOLITAN CORP. COUNSEL, Nov. 1999, at 4.

93. Jeffrey B. Ritter et al., *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87, 94-95 (2001) (explaining that the Privacy Directive creates minimum standards, and that national laws are allowed to vary, provided they meet these minimum standards).

nations deemed to be non-conforming.[94] According to its preamble, the Directive was born in part out of a desire to preserve rather than to inhibit data flows.[95] Specifically, the European Union was concerned that data flows within Europe could be hindered if the rules were not standardized across Member States.[96] If all EU Member States must adopt the same protections, then no Member State can "inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedom of individuals, and in particular the right to privacy."[97]

Europe recognized early that nations serious about protecting data privacy could not achieve their goals, given the global nature of the Internet, without controlling data use outside the legislating sovereignties.[98] Europe also understood the price of extraterritorial control: if the privacy rights of Europeans were to be meaningful rather than symbolic, any region or nation unable to ensure adequate privacy protections could not be guaranteed access to data flows. If serious regulatory privacy protections and free data flow are both of fundamental importance, regulatory uniformity is a natural solution, and perhaps the only one. By adopting the Directive, the European Union essentially shifted the privacy challenge from a European level to a global one.

This section briefly explains some of the more important components of the Directive. Because the Directive is a lengthy and detailed document, the discussion is intended not to be a comprehensive analysis, but rather to highlight the European approach to the management of data privacy.

A. *Restrictions on Collection and Use of Data*

The Directive protects only "personal data," defined as "any information relating to an identified or identifiable natural person."[99] The Directive then defines an identified or identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social

---

94. One commentator describes the Directive's threat as "a sword of Damocles." Steve Jarvis, *Their Way or the Autobahn?; U.S., EU Still Don't Agree on Data Handling*, MARKETING NEWS, Aug. 13, 2001, at 5.

95. EU Directive, *supra* note 1, pmbl.

96. *Id.* pmbl. (7) (suggesting that different levels of privacy protection across EU Member States regarding personal data processing might "prevent the transmission of such data from the territory of one Member State to that of another Member State . . . .").

97. *Id.* pmbl. (9).

98. *Id.* pmbl. (56).

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

identity."[100] This limitation means that European companies can freely develop and share demographic databases as in the United States, when they contain only abstract trends and information, and when no data can be associated with a particular person.

The Directive's restrictions apply to collectors who engage in personal data "processing," which is defined as operations or sets of operations that are performed on personal data, automatically or otherwise.[101] It includes, but is 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."[102] Processors of personal data are required to inform data subjects of the their identities, as well as the identities or categories of recipients of the data.[103] They are also required to explain the purposes for which the information is being collected.[104]

In instances where the data are not obtained from the data subject, these disclosure requirements may be inapplicable under the terms of a hardship provision, depending on the purposes for which the data are being used.[105] This potential disclosure exception applies "where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law."[106] When the disclosure exception applies, the Directive mandates Member States to provide "appropriate safeguards."[107]

A consumer who has been notified of personal data collection is protected in two important ways, through opt-in rights[108] and objection rights.[109] These two important areas are addressed in subsections below.

1. Opt-in Rights

The Directive's highly touted opt-in provisions[110] are more limited than a casual observer might realize because the pertinent

---

100. *Id.* art. 2(c).
101. *Id.* art. 2(b).
102. *Id.*
103. *Id.* arts. 10-11.
104. *Id.*
105. *Id.* art. 11(2).
106. *Id.*
107. *Id.*
108. *Id.* art. 7.
109. *Id.* arts. 14-15.
110. *See, e.g.*, Steve Jarvis, *Opt-In can't be stressed enough online*, MARKETING NEWS, May 21, 2001, at 6, *available at* 2001 WL 6706726 (discussing the effects of opt-

Article of the Directive contains what are, effectively, exceptions. The opt-in provision states the rule: "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent . . . ."[111] The rule is immediately followed by the crucial word "or," and five classes of exceptions, where consent is not required. These areas of exception protect a data collector's ability to serve either the data subject or the public interest at large. Exceptions that protect the data subject include data processing necessary to perform a contract with the data subject or the pre-contractual requests of the data subject,[112] and processing necessary to protect the data subject's vital interests.[113] Exceptions that protect the public interest include data processing necessary to meet a legal requirement[114] and data processing "necessary for the performance of a task carried out in the public interest."[115]

These are open-textured categories that seriously undercut the strength of the Directive's opt-in approach. They pale, however, in comparison with the final category, which dispenses with the data-subject consent requirement when

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).[116]

For numerous reasons, this final exception is likely to remove some forcefulness from the Directive's opt-in approach. The standard of "legitimate interests"[117] is a low threshold and presumably is easily met. The standard is also broad in its application, referring to both the interests of the data collector and third persons. Perhaps most importantly, the standard is very vague. Self-interested data collectors might easily interpret it in their own favor in a wide array of situations.

2. Access and Objection Rights

The EU Data Privacy Directive provides data subjects with access and objection rights. The rights are discussed in the following subsections.

---

in privacy policies on major research firms); Donna Gillin, *Opt in or opt out?*, MARKETING RESEARCH, July 1, 2001, at 6, *available at* 2001 WL 19284643.

111. EU Directive, *supra* note 1, art. 7(a).
112. *Id.* art. 7(b).
113. *Id.* art. 7(d).
114. *Id.* art. 7(c).
115. *Id.* art. 7(e).
116. *Id.* art. 7(f).
117. *Id.*

a. Access Rights

Article 12 of the Directive provides a set of guarantees to every data subject. Member States must assure that data subjects have a right of access to data being collected by data controllers.[118] It refers to data subjects' "right to obtain" the pertinent data "without constraint at reasonable intervals and without excessive delay or expense."[119] A right to obtain suggests that tendering need not be automatic—apparently, data controllers can require subjects to request the data in order to receive it.

Data subjects have the right to be told whether their personal data is being processed, and if so, for what purposes.[120] The also have the right to receive the data that is being processed, "in an intelligible form," as well as "any available information" regarding the source of the data.[121] If the processing of personal data is automated—and the Directive limits the conditions under which automated data processing is permitted[122]—the data subject has, at least at times,[123] the right to know "the logic involved" in the automated processing.[124]

Data subjects also have the right to erase or block any data processing not in compliance with the Directive, especially if noncompliance is a function of the incompleteness or inaccuracy of the data.[125] If third parties have received the data prior to such erasure or blocking, the data subject has the right to notification of the rectification to third parties.[126]

---

118. *Id.* art. 12.
119. *Id.* art. 12(a).
120. *Id.*
121. *Id.*
122. Article 15(1) on "Automated Individual Decisions" provides:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Id. art. 15(1).

123. The Directive is unclear regarding the comprehensiveness of this right to access. The exact language of the provision guarantees data subjects' right to obtain "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)." *Id.* art. 12(a). One way to interpret the "at least" provision in this language is as creating a statutory threshold for EU Member State legislation. *Id.* A less satisfactory interpretation is that the "at least" provision is to be part of the Member State legislation itself. This interpretation is less desirable because of the vagueness it would create on the face of the statutes. For this reason alone, it seems likely that the former interpretation better reflects the intent of the Directive.

124. *Id.*
125. *Id.* art. 12(b).
126. *Id.* art. 12(c).

One important point, alluded to earlier in this subsection, bears elaboration. Article 12 is couched in terms of Member States guaranteeing certain rights to data subjects; therefore, implementing legislation arguably may not place automatic burdens on data controllers. For example, there are at least two ways to guarantee access to information. More strictly, data controllers may be required to send data subjects information automatically. More leniently, data controllers may only be required to send information upon request of the data subjects. The more lenient approach would be in compliance with a strict, literal interpretation of the right to obtain the data.

Similarly, implementing legislation technically could guarantee the right to rectification either by requiring automatic rectification of errors in all cases or by requiring rectification only upon the request of the data subject. In both of these examples, it is the data subject's rights to obtain the stated relief from the data controller that is guaranteed. This situation leaves room for an interpretation whereby the data subject must act in some substantial way to trigger such a right. Requiring data subject action could create complex and time-consuming procedures. Indeed, given the complex nature of much legislation and regulation, one might expect complexity of procedures. Complicated processes are likely to undermine the consumer interests that they are ostensibly created to protect.

b. Objection Rights

The Directive also creates a data subject's "right to object."[127] Like the rights previously discussed in this Subsection, the right to object is not always clearly delineated within the Directive. Article 14(a), for example, requires Member States to grant data subjects the right

> at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data . . . .[128]

What remains most uncertain here is where the boundaries would or should be drawn regarding "compelling legitimate grounds relating to [the data subject's] particular situation to the processing of data relating to him."[129]

The other curious aspect of Article 14(a) is its mandate to grant data subjects objection rights "at least in the cases referred to in

---

127. *Id.* art. 14.
128. *Id.* art. 14(a).
129. *Id.*

Article 7(e) and (f)."[130] Referring back to Article 7, this suggests that Member States must confer objection rights when "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed,"[131] and when

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1.[132]

In contrast, Article 14(a) suggests that Member States need not provide objection rights when data is being processed for any of the other authorized reasons. The logic behind this distinction is obvious in terms of the first basis for data processing, where "the data subject has unambiguously given his consent."[133] Unambiguous consent logically vitiates the value of and the need for objection rights—one can safely assume that the data subject does not object where there is express consent.

The logic in distinguishing the remaining categories of data processing is less clear; why should Member States not allow data subjects to object when data are being processed because "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"?[134] This exemplifies a class of cases that is defined by the data processor by employing an element of discretion and judgment, with which the data subject may well disagree. Likewise, data subjects may have problems with processing justified as "necessary for compliance with a legal obligation to which the controller is subject,"[135] or "necessary in order to protect the vital interests of the data subject."[136] In each case, the processor's assessment could easily be a contestable stretch. It is difficult to see why Member States must provide objection rights in some instances, but not in these.

The second provision for data subject objection is more straightforward and less troublesome. It requires Member States to grant data subjects the right

> to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal

---

130. *Id.*
131. *Id.* art. 7(e).
132. *Id.* art. 7(f).
133. *Id.* art. 7(a).
134. *Id.* art. 7(b).
135. *Id.* art. 7(c).
136. *Id.* art. 7(d).

> data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.[137]

This language is relatively clear, makes no counterintuitive or curious distinctions among what appear to be like situations, and addresses one of the primary contemporary concerns regarding data privacy—its use and distribution by direct marketers.[138]

B. *Restrictions on Data Flows to Countries Lacking Adequate Privacy Protections*

Among the most controversial aspects of the Directive is its potential effect on other nations that interact with or do business in Europe.[139] Under the Directive, EU Member States are to block the flow of information from Europe to nations lacking acceptable privacy protections.[140] Specifically, Article 25, Section 1 of the Directive states,

> Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with national provisions adopted pursuant to the other provisions of this Directive, the third country in question *ensures an adequate level of protection.*[141]

Article 25's limitation to "personal data which are undergoing processing or are intended for processing"[142] may seem to mitigate the provision's potential severity. Yet, in reality, Article 25 would affect virtually all personal data transmissions. This occurs because the definitions section indicates that "processing of personal data" includes a very broad array of activities, including "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."[143]

Article 25, Section 2 provides guidance in interpreting what exactly qualifies as "an adequate level of protection." Adequacy is to

---

137. *Id.* art. 14(b).

138. Bergerson, *supra* note 40, at 1528-29 (citing recent Harris poll results showing a dramatic increase, from the 1970s to the 1990s, in consumer concern regarding use of personal information).

139. In today's global market, entities in all nations are likely to interact or do business with Europe. Accordingly, the provision of the EU Directive restricting data flows is likely to have worldwide impact.

140. Raf Casert, *EU, U.S. Reach Deal on Data Privacy*, ASSOCIATED PRESS, Mar. 14, 2000, *available at* 2000 WL 16859024.

141. EU Directive, *supra* note 1, art. 25(1) (emphasis added).

142. *Id.*

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

be assessed by looking at all the circumstances that surround data transfer operations, with particular attention to

> the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[144]

Article 26 of the Directive does provide some potential relief from the severity of Article 25's data flow restrictions. Under Article 26, countries not ensuring adequate protection under the provisions of Article 25 may still receive personal data transfers under a disjunctive list of circumstances.[145] These circumstances are similar to those listed in Article 7, circumscribing when personal data may be processed in Member States.[146] The specific language of Article 26 is as follows:

> Derogations
>
> 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:
>
> (a) the data subject has given his consent unambiguously to the proposed transfer; or
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
>
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
>
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
>
> (f) the transfer is made 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, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
>
> 2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the

144. *Id.* art. 25(2).
145. *Id.* art. 26.
146. *See supra* notes 111-15 and accompanying text.

> exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
>
> 3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2. If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2). Member States shall take the necessary measures to comply with the Commission's decision.
>
> 4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.[147]

These exemptions mimic the vague exemptions of Article 7, and thus share some of that Article's ambiguities.[148] These ambiguities could create "wiggle-room" for U.S. and other non-EU businesses, potentially jeopardizing the Directive's efficacy.[149] Apart from potential ambiguities, the apparent intent here is to ensure that, even if a non-EU nation has not passed rigorous privacy protection laws, data flows are not restricted in particular instances where Europe's own rigorous requirements would have been met.

The Directive's data flow restrictions respond to the valid concern that the European legislation will be substantially undermined if it fails to account for use of personal data once it goes beyond EU borders.[150] This concern over international spillover effects[151] was recognized as early as 1980, when the OECD issued its Guidelines.[152] The Guidelines established principles for companies around the world to apply in the fair collection and use of personal information.[153] Unlike the OECD Guidelines, however, the EU

---

147. EU Directive, *supra* note 1, art. 26.

148. *See supra* notes 111-15 and accompanying text.

149. Stephen A. Oxman, Note, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?*, 24 B.C. INT'L & COMP. L. REV. 191, 198 (2000) (observing that vague provisions in the Directive jeopardize data-subject privacy protections).

150. Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law*, 95 AM. J. INT'L L. 132, 156 (2001). "[I]n recognition of the ease with which personal data on Europeans can be transferred electronically outside the EU, the directive sought to prohibit transfers to non-EU states unless those states provide an 'adequate' level of data protection." *Id.*

151. Spillover effects are "effects of conduct [that] extend beyond pre-established geographical boundaries—or 'spill over' into other jurisdictions . . . ." David G. Post & David R. Johnson, *The New Civic Virtue of the Net: Lessons from Models of Complex Systems for the Governance of Cyberspace*, 1997, ¶ 21 (STAN. TECH. L. REV., Working Paper), *at* http://stlr.stanford.edu/STLR/Working_Papers/97_Post_1/index.htm.

152. *See supra* note 63 and accompanying text.

153. Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1189-90 (1999).

Directive creates a palpable threat that nations with lax privacy protections will lose access to European data flows.[154]

If non-European nations are to avoid losing access to European data under the Directive, they will have to qualify by creating acceptable "Safe Harbor" provisions. These are the provisions that will specify what non-EU nations must do to qualify as adequately protecting privacy. During 1999 and 2000, the European Union and the United States negotiated a Safe Harbor agreement, and other nations are likely to follow suit to ensure that data flows from Europe remain unimpeded.[155] The subsections below discuss the development and negotiation of the U.S. Safe Harbor provisions.

1. U.S. Safe Harbor Provisions Development and Negotiation

In April 1999, the U.S. Commerce Department submitted a draft to the European Union of a proposed Safe Harbor agreement, called the International Safe Harbor Privacy Principles.[156] A purported goal of these Principles was to develop compliance standards that were predictable and unambiguous.[157] Although the European Union did not accept the original proposals, its Article 31 Committee on Data Privacy eventually approved a subsequent version.[158]

By March 2000, the European Union and the U.S. Commerce Department had forged a tentative Safe Harbor agreement,[159] subject to EU Parliamentary Comment and final EU approval.[160] Initial reports suggested that final approval of the pact would be a formality,[161] despite protests by consumer groups that the agreement failed to provide sufficient protection to European privacy

---

154. Deborah Hargreaves, *Experts Back Brussels and US Data Protection Deal*, FIN. TIMES, June 1, 2000, at 13 (discussing the Directive's potential threat to the flow of information to countries lacking adequate privacy protections).

155. *No peeping toms, please*, ECON. TIMES, Apr. 22, 2000, *available at* 2000 WL 16891228.

156. James Heckman, *Marketers waiting, will see on EU privacy*, MARKETING NEWS, June 7, 1999, at 4, *available at* 1999 WL 7723071.

157. *E-Commerce Developments of Note: U.S. Reaches Privacy Accord with EU on Data Protection*, E-COMMERCE, Apr. 2000, at 8 (identifying provision of "clear and predictable guidance" as a goal in drafting the ultimate Safe Harbor proposal).

158. Elizabeth de Bony, *EU Overwhelmingly Approves U.S. Data-Privacy Regulations; Should make conducting business in Europe easier*, COMPUTERWORLD, June 5, 2000, at 28, *available at* 2001 WL 2176532.

159. *U.S. and Europe Agree on Privacy*, N.Y. TIMES, June 2, 2000, at C4.

160. The European Commission, *Data Protection: Commission Adopts Decisions Recognising Adequacy of Regimes in US, Switzerland and Hungary*, July 27, 2000, *available at* http://www.europa.eu.int/comm/internal_market/en/dataprot/news/safeharbor.htm (discussing EU Parliamentary comment and EU approval) [hereafter *Adequacy of Regimes*].

161. *See, e.g.*, *Enterprise Systems*, COMPUTING, June 15, 2000, at 6 (indicating that the pact was expected to be "rubber stamped" by the Commission in late July 2000).

interests.[162] According to a consumers' forum called Transatlantic Consumer Dialogue, "the safe harbor system would not provide European citizens with the adequate level of protection that they are guaranteed under EU law."[163]

A majority of the European Parliament objected to the U.S proposal.[164] The vote was close: in July 2000, the EU Parliament rejected the proposed Safe Harbor provisions by a vote of 279 to 259, with twenty-two abstentions.[165] Italian Member Elena Ornella Paciott suggested that present U.S. privacy policy was not sufficiently developed to support current adoption of the negotiated Safe Harbor provisions.[166] The Parliament's Citizens' Rights Committee was also concerned that the Safe Harbor agreement "contained several loopholes."[167]

Implementation and enforcement were major concerns.[168] The European Parliament's resolution recommended an amendment to provide for an independent body that would be empowered to hear complaints regarding privacy abuses, as well as a mechanism by which victims of privacy abuses could receive damages.[169] Although the European Parliament's resolution did not bind the European Commission,[170] commentators suggested it would be impolitic for the Commission to ignore the resolution without in some way addressing

---

162. *EU Backs Data Privacy Act*, CHI. SUN-TIMES, June 5, 2000, at 57.

163. *No Safe Harbor For Data*, INTELLIGENT ENTER., June 5, 2000, at 11, *available at* 2000 WL 11677727.

164. *Why privacy matters—European Director General to speak out next week (March 23-24) at privacy open seminar in Brussels*, M2 PRESSWIRE, Mar. 16, 2000, *available at* 2000 WL 16125616.

165. Jennifer DiSabatino & Greg Stedman, *U.S./Europe Privacy Deal Sent Back for More Talks; European Parliament rejects proposal; safe harbor agreement in question*, COMPUTERWORLD, July 17, 2000, at 24.

166. Elizabeth de Bony, *Europeans Pan U.S. Privacy Plan*, INFOWORLD DAILY NEWS, July 6, 2000, *available in* LEXIS, News Library, Allnws File (quoting European Parliament Member Elena Ornella Paciott, "The Parliament takes the view that the adequacy of the U.S. system cannot be confirmed and, consequently, the free movement of data cannot be authorized until all the components of the safe harbor system are operational and the United States authorities have informed the Commission that these conditions have been fulfilled . . . .").

167. Robert MacMillan, *Parliament Pauses on EU-US Privacy Plan—Update*, NEWSBYTES, June 30, 2000, *available in* LEXIS, News Library, Allnws File.

168. *Adequacy of Regimes*, *supra* note 160 (reporting that the July 5 EU Parliament Resolution found individual remedies in the event of privacy breaches to be lacking in the Safe Harbor provisions).

169. DiSabatino & Stedman, *supra* note 165.

170. The Parliament's rulings concerning whether the Commission followed proper procedures are binding; in this instance, the Parliament voted by a margin of five votes against a finding of procedural flaws. The Parliament's findings regarding the substantive adequacy of an EU Commission action is not binding, and the Commission is not required to adhere to those findings. For a discussion, see Juliana Gruenwald, *European Parliament Says "No" to Safe Harbor*, NAT'L J. TECH. DAILY, July 13, 2000, *available in* LEXIS, News Library, Allnws File.

the Parliament's concerns.[171] Nonetheless, the Commission approved the Safe Harbor agreement on July 26, 2000,[172] stating to the EU Parliament that the arrangement did indeed provide "adequate protection."[173] A subsequent corrigendum verified that the Commission was acting within the scope of its authority in its approval.[174]

2. The Nature of the Safe Harbor Principles

Companies that intend to comply with the principles certify themselves by notifying the U.S. Commerce Department of their intent to do so.[175] To become a self-certified organization qualified to receive data, an entity must "unambiguously" and "publicly" disclose its commitment to comply with the Safe Harbor Principles.[176] To be eligible for this self-certification process, the organization must be subject to a U.S. government body "empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles."[177]

The enumeration of the actual guidelines themselves is very informal. The Federal Register lists and briefly explains Safe Harbor Principles, upon which it elaborates in a set of "frequently asked questions," or FAQs.[178] The Safe Harbor Principles cover rights of data subjects regarding notice, choice, onward transfer, security, data

---

171. de Bony, *supra* note 166.

172. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce. Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7 [hereafter Commission Decision].

173. *Telecommunications and Information Technology,* BUS. GUIDE TO EU INITIATIVES, ch. 9, 2000/2001 (reporting the public declaration of Commissioner Frits Bolkestein before the EU Parliament's Committee on Citizens and Civil Rights).

174. Corrigendum to Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46/EC of European Parliament and of the Council on the adequacy of protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the Department of Commerce. 2001 O.J. (L 115) 14 ("The Commission . . . concluded that although the European Parliament expressed the view that certain improvements needed to be made to the 'Safe Harbor Principles' and related FAQs before it could be considered to provide 'adequate protection', it did not establish that the Commission would exceed its powers in adopting the decision.").

175. Commission Decision, *supra* note 172.

176. *Id.* art. 1(2)(a).

177. *Id.* art. 1(2)(b).

178. Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000) [hereafter Principles] (modified in part by Issuance of Safe Harbor Principles and Transmission to European Commission; Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534, Sept. 19, 2000). The FAQs also are available at on the EU's web page, *at* http://www.europa.eu.int/comm/internal_market/en/dataprot/news/safeharbor.htm.

integrity, access, and enforcement.[179] If they remain in compliance with their own self-regulatory privacy policies,[180] certified parties remain eligible to receive data from the European Union and are shielded from EU Data Privacy Directive sanctions.[181] European organizations that want to send data to the United States can verify Safe Harbor compliance registration via an updated web page.[182] If a self-certified company fails to comply with the principles, Member States can suspend data flows to an organization under stipulated conditions.[183]

The U.S. development of Safe Harbor Principles demonstrates its acknowledgement of a need to respond to the Privacy Directive's data flow provisions. However, the voluntary registration process in the Principles is one of "self-certification,"[184] which has led some observers to question whether the United States is making real concessions or simply shielding its traditional self-regulation posture behind a smoke-screen of illusory changes.[185]

Purported implementation deficiencies under the Safe Harbor agreement added to concerns that U.S. concessions were mere

---

179. *Id.*

180. *See infra* note 189 and accompanying text (elaborating on the self-regulatory nature of the development of privacy policies that comply with the Safe Harbor agreement).

181. Cheryl Rosen, *European Parliament Nixes Safe Harbor*, INFORMATIONWEEK, July 10, 2000, at 40.

182. Safe Harbor List, *available at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

183. Article 3(1) of the Commission Decision permits such cessation of data flows by Member States under the following conditions:

> (a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or
>
> (b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

Commission Decision, *supra* note 172, arts. 3(1)(a)-(b).

184. Ron N. Dreben & Johanna L. Werbach, *Senators Versus Governors: State and Federal Regulation of E-Commerce*, COMPUTER LAW., June 2000, at 3, 11 (stating that U.S. companies would become Safe Harbor eligible under the proposed agreement by "self-certifying" their willingness to abide by the agreement's privacy principles).

185. *U.S. Companies Fail European Personal Data Privacy Requirements*, PRECISION MARKETING, Aug. 31, 2001, at 1, *available at* 2001 WL 11462796 (citing a report claiming that U.S. companies are not doing enough to guard personal data, despite the Safe Harbor Principles).

window-dressing.[186] Monitoring and enforcement to police the agreement in the United States technically would fall under the aegis of the Federal Trade Commission and the U.S. Department of Transportation.[187] The degree and rigor of monitoring and enforcement are unclear, so that the self-certification process remains a stumbling block for some distrustful critics.[188] Indeed, the text of the Commerce Department's November 1999 proposal clearly demonstrates that, despite potential actions for unfair or deceptive practices, Safe Harbor procedures are largely self regulatory:

> Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the principles must comply with the principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self regulatory privacy program that adheres to the principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self regulatory privacy policies provided that they conform with the principles. Where in complying with the principles, an organization relies in whole or in part on self regulation, its failure to comply with such self regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.[189]

Note that, under this language, potential liability for Safe Harbor violations obtains as a result of failure to do what a company says it is going to do, within the bounds of its own privacy policies. Determining what those privacy policies actually are is the responsibility of the self-certifying company. In the absence of some pre-certification external review or scrutiny of the policies themselves, sanctions triggered solely by a company's violation of those policies are weak. A certified company that meticulously complies with its own poorly developed policies can easily fall short of providing meaningful privacy protection.

This result is a potentially enormous efficacy gap in the Safe Harbor Principles. Nevertheless, attempted good-faith compliance with Safe Harbor Principles could require many U.S. firms to reassess their present data-sharing and data-retention procedures

---

186. *Safe harbour creates a transatlantic storm*, PRECISION MARKETING, Apr. 13, 2001, at 11, *available at* 2001 WL 11461787 (noting the opinions of some industry experts that the Safe Harbor agreement is just another "vain attempt to curb the EU's obsession with paperwork and get a model contract signed and sealed.").

187. Rosen, *supra* note 181.

188. *Consumers Highly Critical of EU/United States Data Protection Agreement*, EUR. REP., Apr. 5, 2000, *available at* 2000 WL 8841413. "U.S. consumer organizations have little confidence in the effectiveness of the self-regulatory system for protecting personal information." *Id.*

189. Draft: International Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce, Nov. 15, 1999, *available at* http://ita.doc.gov/td/ecom/Principles1199.htm.

and to make substantial changes to current practices.[190] If the U.S. Safe Harbor program does confer any incremental privacy protection within the European Union, it will likely be scattershot, given efficacy holes in the self-certification process.

Commentators disagree about whether the United States gave away too much or too little in the Safe Harbor agreement. In the United States, privacy advocates who would generally applaud the spirit of the Directive wonder how and why the United States will now confer greater privacy protection to Europeans than to U.S. citizens.[191] Other non-European critics have voiced concern over the Safe Harbor Principles on a number of grounds. Some believe that the approach is "excessive," extending protections "beyond consumer concern," and suggest that such stringent restrictions could harm international trade generally and the European economy specifically.[192] David Flint observes that, "[F]or many, the impact of the European Union directive on data protection is likely to have a severely constraining effect on the cross-continental sharing of important data . . . . [S]ince the law on data protection is drawn quite tightly, there are few, if any, non-EU countries that meet its standards."[193]

These concerns are exacerbated by the character of the guidelines for determining the adequacy of data protection. As was just observed, assessors of data protection measures are to look not only at a nation's policies and practices, but also at institution-specific variables.[194] The directive suggests a case-by-case compliance assessment on top of the nation-by-nation Safe Harbor principles assessment, increasing the potential drag on international commerce.[195]

---

190. Patrick Thibodeau, *Europe and U.S. Agree on Data Rules*, COMPUTERWORLD, Mar. 20, 2000, at 6 (noting that Safe Harbor compliance could require some companies to make painful changes, particularly in regard to the transfer of data to third parties).

191. This concern arose during negotiations of the Safe Harbor Principles. Keith Perine, *Not Enough Privacy?*, INDUS. STANDARD, July 3, 2000, *available at* 2000 WL 31584023 (noting privacy advocate Jason Catlett's concern that U.S. firms are now to give better privacy protections to Europeans than to Americans).

192. Stan Beer, *US Marketer Attacks EU Privacy Code*, AUSTRALIAN FIN. REV., Aug. 8, 1998, at 23.

193. David Flint, *EU and the Rest of the World Divided Over Data Protection*, SCOTSMAN, Sept. 24, 2001, at 20, *available at* 2001 WL 27630394.

194. EU Directive, *supra* note 1, art. 25(2).

195. Because each entity decides to certify under its own set of compliance procedures, there are potentially thousands of different versions of compliance, each of which would be evaluated and assessed individually. Both the number of entities and the variety of programs they use to comply with the Safe Harbor principles increase potential unwieldiness of EU monitoring and enforcement. At least two possible results arise—that the European Union will monitor aggressively, and may stall data flows in the process of the cumbersome challenge or that the burden of monitoring

As some domestic observers question whether the United States has given up too much, the concern of the EU Parliament is that the United States has given away too little.[196] Driven by fears that the Safe Harbor Principles lack meaningful enforcement mechanisms, the EU Parliament's fears seem to have some merit, given the slow pace at which U.S. companies have responded to the provisions. As of a March 2001 report, a mere two dozen or so U.S. companies had registered as Safe Harbor compliant.[197] By August 2001, the number had risen to about seventy,[198] a miniscule portion of all U.S. firms. Perhaps partially in response to concerns that meaningful data flow controls under the Privacy Directive may fizzle, the European Union is pressing implementation forward.[199]

One final note is warranted. The specifics of the U.S. Safe Harbor Principles are complex, and since they have been examined by others in detail,[200] and go beyond the scope of this Article, they will not be examined here.[201] Ironically, the importance of the provisions is now coming into question, as there have been few U.S. companies that have bothered to register with the U.S. Commerce Department as Safe Harbor compliant.[202] The final impact of the Directive's data flow restrictions is yet to be seen.

---

these thousands of entities will be unmanageable, and monitoring and enforcement will be nominal or nonexistent.

196. *See supra* notes 163-68 and accompanying text.

197. Marilyn Geewax, *Key Congressman says European Rules on Net Privacy Could Hurt U.S. Commerce*, ATLANTA J. CONST., Mar. 9, 2001, at 5C.

198. Jarvis, *supra* note 94, at 5.

199. *EC Ignores U.S. E-Trade Threat: The European Commission is Ignoring U.S. Requests to Slow Down the Implementation of its Data Privacy Directive Despite Fears that the Issue Could Spark an E-commerce Trade War*, GLOBAL NEWS WIRE (VNU), FIN. TIMES INFORMATION, May 8, 2001, *available in* LEXIS, News Library, Allnws File (discussing EU firmness in pressing forward application of the data flow provisions of the Privacy Directive).

200. *See, e.g.*, Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735 (2001).

201. Donna Gillin, *Safe Harbor Principles for the European Privacy Directive are Finalized*, MARKETING RESEARCH, Winter 2000, at 41 (describing briefly the basics of the Safe Harbor Principles).

202. Geewax, *supra* note 197.

V. THE EU APPROACH AND INTERNATIONAL RELATIONS

A. *The Challenge*

In terms of international relations, the Internet is truly a double-edged sword. In many ways, it has the potential to facilitate and improve relations between countries, to enhance human rights, and to support world peace.[203] Yet to realize and exploit this potential, nations must support a new technology that is more global than any that has preceded it, and efforts to create workable worldwide Internet policies can backfire, leading to short-term international strife.[204] Westbrook summarizes the situation aptly: "A new world is slouching toward New York and London, Beijing and Bangkok, to be born. If our planet and our values survive the secondary effects of that emergence, we may look forward to a humanity more prosperous and more integrated than at any time in human history."[205]

A brief examination of the two conflicting aspects of Internet technology, potentially enhanced international relations and potentially increased transitional strife, is warranted.

1. The Potential for Enhanced International Relations, Human Rights, and World Peace

Internet technology has the potential to be a powerful agent in affecting positive global change. By enhancing communications around the world, it supports transnational discourse in ways and to degrees previously unimaginable.[206] As the world continues to interact more frequently and regularly, the potential for the creation of a true global community grows.

---

203. Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1127 (1998). "The Internet, respectable commentators tell us, will foster tolerance, promote democracy, redistribute wealth, improve writing and reading skills, destroy trade barriers, and bring world peace." *Id.*

204. McTigue observes this potential, specifically in relation to globally conflicting privacy policies and philosophies. Deborah M. McTigue, *Marginalizing Individual Privacy on the Internet*, 5 B.U. J. SCI. & TECH. L. 5, 95, 112-13 (1999) (observing the potential for differing privacy approaches to result in discord among nations, due to the global collectivity of Internet networks).

205. Jay Lawrence Westbrook, *A Global Solution to Multinational Default*, 98 MICH. L. REV. 2276, 2276-77 (2000) (citations omitted).

206. For a discussion of characteristics and limitations of this discourse, see C. Edwin Baker, *An Economic Critique of Free Trade in Media Products*, 78 N.C. L. REV. 1357, 1425 (2000).

A global community may be a good thing or a bad thing, depending in part on the quality of the values that sustain it. A global community where human rights are respected, for example, is superior to one in which human rights are routinely abrogated. The very nature of Internet technology is likely to support rather than undermine human rights, because the Internet is a tool facilitating free speech, even in the face of attempted despotism.[207] By virtue of its unruliness, the Internet paradoxically may lead to higher quality rule because it allows dissident voices to be heard.[208] In a developing global arena, forces for human rights will always be strong, but to be galvanized, people must learn about the institutions that need changing. The Internet's inexorably open forum cannot help but facilitate the process.[209]

The Internet will be the foundation for a global discourse in which voices of reason cannot be smothered. While this is no guarantor of global harmony and peace, it is an infrastructure that is likely to help move the world in the right direction. The evolution of a global village suggests the decline of the symbolic power of sovereignty and the rise of a global ethos.[210] A move from "us versus them" to simply "us" can be a logical precursor to unification of interests and enhanced international relations.[211] Nonetheless, as will be seen in the next subsection, these ideal effects of technology are not so easily realized. The very nature of the Internet suggests that, on the way to this idealized world, technology may in fact increase, rather than mitigate, international frictions.

---

207. Gary Andrew Poole, *Despots Find Dissidents on Internet Hard to Muzzle*, USA TODAY, Jan. 26, 1999, at 15A (discussing difficulties in controlling dissident voices over the Internet in various countries around the world).

208. *See generally* John T. Delacourt, Recent Development, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207, 220 (1997).

209. For an elaboration of the Internet's inexorable value to dissident voices, see Delacourt, *supra* note 208, at 220.

210. This is not to suggest that sovereignty is either dead or moribund, but rather that it becomes increasingly troublesome as the world shrinks and global interactions escalate. Stephen Krasner provides an excellent analysis that addresses the functions and limitations of sovereignty as the working model for contemporary global governance. Stephen D. Krasner, *Pervasive Not Perverse: Semi-Sovereigns as the Global Norm*, 30 CORNELL INT'L L.J. 651 (1997).

211. This process will be expedited by a truly free Internet, and is impeded when nations attempt to censor the Internet to avert what are viewed as threats to national culture. Amy Knoll, Comment, *Any Which Way But Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275, 299 (1996) (suggesting that some Asian countries have controlled Internet information dissemination to ensure that it is aligned with their cultural norms).

2. The Potential for International Strife

In the short run, the Internet poses challenges that could create more international problems than it solves. This possibility results from the strains that volatile, globe-spanning technologies cannot help placing on international relations. These strains are a function of the dimensions of both time and space.

a. Time

Development of modern technologies and concomitant social change continue to accelerate.[212] It is harder than ever to foresee the technologies that will emerge within five- and ten-year horizons, much less to recognize the legal, social, and economic challenges such innovations will pose.[213] Consider a recording industry taken unaware by MP3 technology, or brick-and-mortar businesses unprepared for the competitive challenges of e-commerce threats in the 1990s. Less predictable technologies bring with them less predictable alterations in social and economic realities as well, and hence less predictable challenges to the legal systems that monitor and control those realities.[214] The deliberative processes of legal change are poorly equipped to respond rapidly and effectively to these fast-changing demands.[215] An unprecedented bad fit exists between the tasks law faces and the processes in which it engages. This bad fit creates strains on the legal system.[216]

---

212. Shamoil Shipchandler, *The Wild Wild Web: Non-Regulation as the Answer to the Regulatory Question*, 33 CORNELL INT'L L.J. 435, 444 (2000) (referring to the Internet as "rapidly changing").

213. Steven Bercu, Book Note, 4 HARV. J.L. & TECH. 299 (1991) (reviewing TOM FORESTER & PERRY MORRISON, COMPUTER ETHICS: CAUTIONARY TALES AND ETHICAL DILEMMAS IN COMPUTING (1990)). "Technological change penetrates society faster than we can form new attitudes, reach new consensuses, or adapt our legal and ethical codes. Adaptation must occur if we are to cope adequately with the new problems—or to recognize old problems in new garb—that the technologies bring." *Id.*

214. Both MP3 technology and e-commerce generally are examples of how shifts in technology bring about new social and economic challenges to the legal system. MP3 technology requires reexamination of copyright law, and particularly contributory infringement doctrine. E-commerce has raised questions of equitable sales tax policies, as well as the nature of the nexus requirement for out-of-state sales tax collection purposes.

215. Molly A. Holman & Stephen R. Munzer, *Intellectual Property Rights in Genes and Gene Fragments: A Registration Solution for Expressed Sequence Tags*, 85 IOWA L. REV. 735, 796 (2000) (observing that "if the law responds too slowly to rapid technological change, it is apt to be too slow in fostering norms that might respond to such change.").

216. A good example here is the problem of cybersquatting. Speculators began to cybersquat in the early to mid-1990s, coincident with the public's gaining widespread access to the Internet. Cybersquatting has been troublesome under

b. Space

Modern legal strains associated with time are exacerbated by further legal strains associated with space. Technology has sparked an increase in international transactions,[217] thereby also increasing the instances in which conflicting parties are likely to call on conflicting sovereignty-based legal systems. Comity and conflict of law issues are magnified when separate legal systems come head-to-head.[218]

Because the stakes are growing, sovereign nations can be expected to press their own interests and philosophies in the global marketplace of laws and customs.[219] Selling one's own legal doctrines globally is more than just an effort to gain influence for isolated purposes. It incorporates a recognition that a global technology ultimately seeks unified global policy solutions and that an aggressively pushed approach has the potential to become the dominant one, or even the only viable one. Within this legal "global scene,"[220] the negotiation of Internet-related laws and policies is likely to occur in a fiercely competitive arena.

Escalating stakes and fierce competition over global laws and policies are a natural breeding ground for international strife.

---

trademark analysis because a true cybersquatter who does not use the relevant domain name creates no confusion, tarnishment, or dilution. Lawmakers addressed this problem after dozens of high-profile cases emerged, but they only enacted anti-cybersquatting legislation in 1999. By that time, much of the problem had already been solved, as businesses subsequent to 1999 are, of course, more knowledgeable and aware of e-commerce than were companies earlier in the decade. Reservation of domain names is second nature now; when it was not second nature, and the need for legal doctrines was greatest, businesses acted in a legal vacuum. There simply is not much time for legislators to recognize that a problem exists, identify the issues, identify possible solutions, debate the benefits and costs of those solutions, select an approach, and draft and rehash statutory language. P. Wayne Hale, *The Anticybersquatting Consumer Protection Act & Sporty's Farm L.L.C. v. Sportsman's Market, Inc.*, 16 BERKELEY TECH. L.J. 205 (2001) (discussing the 1999 anticybersquatting statute).

217. John Christopher Anderson, *Respecting Human Rights: Multinational Corporations Strike Out*, 2 U. PA. J. LAB. & EMP. L. 463, 467-68 (2000) (observing that the Internet will spawn an increase in international trade).

218. Joshua S. Bauchner, Note and Comment, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, 26 BROOK. J. INT'L L. 689 (2000) (discussing this problem as it relates to the EU Data Privacy Directive).

219. This is part of a broader phenomenon, which Alan Wright refers to as "trading nations . . . [jockeying] for globally competitive positions." Alan Wright, *The North American Free Trade Agreement (NAFTA) and Process Patent Protection*, 43 AM. U. L. REV. 603, 617 (1994).

220. Annelise Riles, *Wigmore's Treasure Box: Comparative Law in the Era of Information*, 40 HARV. INT'L L.J. 221, 223 (1999) (arguing that "[w]hen legal academics can agree about little else, they do agree that they are players in a global scene, whose theories and policy proposals are of global significance.").

Approaches that are consistent with a nation's culture and interests will be highly valued, and efforts to thwart these approaches can be threatening.[221] For these reasons, a nation or region that takes a dominating or aggressive approach in the forging of laws and policies may increase the potential for international discord.

B. *The EU Data Privacy Directive as an Approach to Internet Governance*

Two of its characteristics make the EU Data Privacy Directive an interesting example or model for Internet governance in the global environment of modern technology, as described in the preceding subsection. First, the Directive takes a strong position.[222] Its solid pro-privacy philosophy—in comparison to U.S. law, for example[223]—gives the Directive forcefulness. Second, the Directive's data flow restrictions are aggressive. They take a powerful global stand. It would hardly be an exaggeration to say that the data flow provisions are a threat to nations outside the European Union.[224] This fact is not to suggest that the provisions are pernicious, but rather that they confront, rather than appeal to, other nations and regions. The Directive limits global negotiations on the fundamental issue of consumer data privacy. Although the details of conformity are subject to some negotiation—some give and take, as seen with the U.S. Safe Harbor negotiations—the basic requirements applied to non-European nations are non-negotiable. The European Union forged fundamental privacy tenets for the world, then gave notice that failure to conform would imperil vital data flows.

Questions arise when these details are analyzed within the context of the preceding subsection: do the Directive and its aggressive approach threaten global harmony? Or do the Directive and its philosophy provide the world with a high-quality stance on data privacy, along with a strong impetus to comply, establishing the kind of unified global policy that contemporary technological society

---

221. Laws and legal culture obviously are a subset of a nation's larger, more overarching culture. The match between the rule of law and legal culture is an important one. Orna Ben-Naftali & Sean S. Gleichgevitch, *Missing in Legal Action: Lebanese Hostages in Israel*, 41 HARV. INT'L L.J. 185, 208 (2000) (discussing one instance of the quality of the match between Israeli culture and detention law).

222. Assey and Eleftheriou describe the Directive as "sweeping privacy legislation creating strong protections governing the collection and use of personal data." Assey & Eleftheriou, *supra* note 29, at 145.

223. Malla Pollack, *Opt-In Government: Using the Internet to Empower Choice—Privacy Application*, 50 CATH. U. L. REV. 653, 658 (2001) (referring to "pro-privacy Europe and consumer-beware United States").

224. This threat has been recognized since the early 1990s. *See, e.g.*, George B. Trubow, *The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow*, 13 NW. J. INT'L L. & BUS. 159 (1992).

will demand? To begin to address these questions, scholars need to examine whether the Directive is built on a solid global foundation of shared norms and values with regard to data privacy. They will also need to explore the implications of recent global events.

1. Does the Directive Capture a Global Perspective on Privacy?

Whether the initiative reflects a reasonable degree of global consensus is a central issue in assessing any aggressive, global legal initiative. If it does, then the risks of creating discord with a domineering posture are reduced, and the potential rewards in terms of forging a global philosophy are increased.[225] That is to say, the wisdom of attempts to force a global policy fit, in the interests of the expediency demanded by rapid technological change, increases when the global arena is already prepared for a unified approach.[226] The more that global players embrace similar ideologies, the greater is the chance that they will view efforts like the EU Data Privacy Directive as leadership rather than aggression.[227] Such differences in

---

225. This is similar to the issues that arise when nations try to impose their influence through extraterritorially applied laws, in areas such as antitrust and international bribery. The Author has addressed whether extraterritorial bribery legislation overreaches in light of cultural differences, in numerous previous articles. *See, e.g.*, Steven R. Salbu, *Information Technology in the War Against International Bribery and Corruption: The Next Frontier of Institutional Reform*, 38 HARV J. ON LEGIS. 67 (2001); Steven R. Salbu, *Transnational Bribery: The Big Questions*, 21 NW. J. INT'L L. & BUS. 435 (2001); Steven R. Salbu, *Battling Global Corruption in the New Millennium*, 31 LAW & POL'Y INT'L BUS. 47 (1999); Steven R. Salbu, *The Foreign Corrupt Practices Act as a Threat to Global Harmony*, 20 MICH. J. INT'L L. 419 (1999); Steven R. Salbu, *Extraterritorial Restriction of Bribery: A Premature Evocation of the Normative Global Village*, 24 YALE J. INT'L L. 223 (1999); Steven R. Salbu, *Bribery in the Global Market: A Critical Analysis of the Foreign Corrupt Practices Act*, 54 WASH. & LEE L. REV. 229 (1997).

226. The need for groundwork is commonly acknowledged. *See, e.g., Leaders Gather, Explore Solutions*, BUS. WIRE, May 22, 2001.

227. For example, industry activity may comprise a bottom-up approach (compared to government edict), whereby e-commerce companies could lead in the development of policies that eventually develop broad support, precisely because decentralized processes build on inputs from multiple constituencies. Decentralized processes also yield a variety of approaches that can then "battle it out" in the marketplace in order to achieve dominance, based at least in part on the superiority of the dominant approach. Such efforts could then channel in to transnational laws that are built on a reasonably uniform foundation. Ultimately, however, whether the forging of policies should be top-down (government-initiated) or bottom-up (industry-initiated), is controversial. Miller observes that "[g]overnments are asking . . . industry to actively lead e-commerce policy development. Leadership, however, flows from clear purpose and direction, not from dithering." Harris N. Miller, *On the Same Page?*, UPSIDE, Apr. 1, 1998, *available at* 1998 WL 30499950.

perception have obvious effects on international relations, as leadership is valued and aggression is resisted and resented.[228]

The question posed by the Directive, then, is whether it reflects a reasonable amount of international concurrence on privacy-related values. The answer, unfortunately, is not as simple as the question. Among hundreds of nations, the dichotomy between the European Union and the United States stands most dramatically in relief—in these two culturally-related regions, very basic commonalities[229] are overshadowed by very fundamental differences.[230]

Even the commonality is tenuous. Admittedly, both the European Union and the United States consider privacy to be important. Yet this statement itself hides two fundamental differences between the European Union and the United States. First, the "privacy" considered to be so important in the two places refers, to some extent, to different conceptions. Every law student in the United States learns that breach of privacy refers to numerous differing concepts. It can refer to misappropriation of personality, invasion of solitude, invasion of autonomy, or misuse of personal information, for example. The sacred privacies of the European Union and the United States often refer to very different concepts.

Fundamental European privacy rights are much more sprawling and all-inclusive, and certainly include data privacy. In the United States, the kinds of privacy that have been deemed a fundamental

---

228. This proposition that aggressive policies are resented when they cross borders is simply an extension of what one commonly see in other political, economic, or military arenas.

229. Kevin Bloss, Note, *Raising or Razing the E-Curtain?: The EU Directive on the Protection of Personal Data*, 9 MINN. J. GLOBAL TRADE 645, 646 (2000) (observing that "the EU and U.S. are not so diametrically opposed in their approaches to privacy regulation, as one would first assume.").

230. Jonathan M. Winer, *If the U.S. is from Mars and the EU is from Venus, What Do You Do in Cyberspace?*, 1 PRIVACY INFO. L. REP., at 8 (No. 8, 2001).

> The divergent approach of the U.S. and the EU to regulating technologies that inherently do not respect borders has the potential to create a transatlantic legal labyrinth that can do great harm to global e-commerce. This is obviously true regarding the EU's approach, as the EU has to date shown little respect for alternative approaches to their heavily regulatory model. But it also is true on the U.S. side. Domestic companies exercising First Amendment rights in the U.S., with permanently established business locations solely limited to the U.S., operating under contracts that specify the U.S. for choice of law and choice of jurisdiction, may find themselves nevertheless subject to foreign laws, jurisdiction, liability and litigation over e-commerce matters. Even worse, in some cases the interplay between U.S. contract law and requirements of doing business in the EU may have the potential to create theories of liability for U.S.-based firms to U.S. persons, if those U.S. persons have an EU nexus to the transaction. Accordingly, those engaged in e-commerce involving both 'Mars' and 'Venus' may find their online transactions at some substantial risk from worlds in collision.

Id.

right tend to be related to autonomy—the right to decide whether to use birth control,[231] for example, or the right to choose an abortion.[232] The United States simply does not share Europe's extremely high levels of concern about data sharing.[233]

The second difference likely results from, or at the very least reflects, the first. That is, the European Union and the United States have adopted fundamentally different legislative and regulatory approaches to data privacy. Most glaring is the most basic decision about data privacy, whether to adopt an opt-in approach or an opt-out approach. The United States has always embraced an opt-out approach, presuming that data privacy often is not a serious concern, while the European Union has adopted an opt-in approach, presuming that data privacy generally is a serious concern.

The difference may reflect more than competing philosophies about privacy. In all likelihood, they reflect more fundamental differences regarding the role of the government in the maintenance of social order and the importance of minimizing the cost of doing business. Europe places a relatively high emphasis on government as a source of the public good, relative to the United States.[234] Contemporary U.S. policies have reduced the role of government, in the faith that unfettered businesses will thrive as costs and impediments are reduced[235] and that the marketplace will help resolve social issues that might be addressed by government in Europe.[236] This juxtaposition translates into a relatively "low interference/high freedom" culture in the United States,[237] consistent with weak legal and regulatory data privacy protections.

In light of these observations, the impact of European-style privacy protections may go well beyond their own specific limits, representing a more symbolic, all-encompassing faith in government

---

231. Griswold v. Connecticut, 381 U.S. 479 (1965).

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

233. *U.S. Government and EU split over Data Protection Directive*, NEW MEDIA AGE, Apr. 5, 2001, at 14, *available at* 2001 WL 11317678 (calling the U.S. view on data privacy incompatible with the EU view because the former are "more relaxed" than the latter).

234. Charles Kennedy, Comment, *European Leaders Should Be More Important to Us Than the U.S. President*, TIMES (London), Nov. 17, 2000, at Features (noting that "self-help" solutions are more common in the United States, compared with government solutions to social problems in the United Kingdom).

235. *Redefining the Government*, J. COMM., Sept. 4, 1997, at 8A (observing that U.S. efforts to reduce regulation are decades old).

236. Peter Grier, *In Europe, Bush Tries Easier Tack*, CHRISTIAN SCI. MONITOR, June 12, 2001, at 1 (contrasting the U.S. and EU approaches to government intervention in addressing social issues).

237. *Americans Have Adjusted Their Views on Government's Role Within the Context of Traditional Values: An Interview with Richard B. Wirthlin*, PUB. PERSPECTIVE, Feb.-Mar. 1998, at 25 (containing comments of Richard B. Wirthlin regarding "[t]oday's commitment to less government and more individual responsibility").

protections that surpasses what U.S. culture is presently prepared to accommodate. As such, the European privacy protections may demand a fundamental philosophical shift of U.S. values and norms—threatening in itself, but even more so when imposed from without.

2. The Future of the Data Privacy Directive's Outward Reach After September 11, 2001

In the latter half of the 1990s, when it attempted to forge global policy through the Data Privacy Directive, the European Union could not have foreseen the terrorist attacks of September 11, 2001[238] or their potential impact on global attitudes toward privacy generally, and U.S. attitudes toward privacy specifically. Nonetheless, these events and their aftermath could have an effect on the value that U.S. citizens place on privacy of all varieties, including data privacy. In the foreseeable future, the EU Data Privacy Directive's efforts to establish a global order in the realm of privacy could be further thwarted by terrorist events.

David Wessel points to September 11 as "a pivot point in American life," engendering major shifts in values.[239] After concerns over personal privacy had begun to grow in the United States on the heels of the Internet's power, September 11 shifted the focus away from privacy and toward security.[240] It is no surprise that unprecedented acts of terrorism should affect the cost-benefit analysis in the balancing of privacy and safety interests. Surveillance tools used by the military and intelligence branches of the government are no less potentially invasive to personal freedoms; yet some may be willing to sacrifice more of those freedoms if they believe that the payoff will be better government protection against future atrocities.[241] Indeed, immediately following the attacks, the U.S. Congress began examining anti-terrorist legislation that evoked concerns about civil liberties in general and privacy in particular.[242]

---

238. *See Planes Crash into World Trade Center and Pentagon, Possibly Terrorist Attacks*, NPR MORNING EDITION, Sept. 11, 2001, *available at* 2001 WL 9328799 (giving an early news report of the terrorist attacks on the World Trade Center in New York and the Pentagon in Washington, D.C. on September 11, 2001).

239. David Wessel, *Capital: A Pivot Point in American Life*, WALL ST. J., Oct. 4, 2001, at A1.

240. *Id.*

241. David Lightman, *Americans Want Both Privacy and Security; Terror in America*, HARTFORD COURANT, Oct. 4, 2001, at A3, *available at* 2001 WL 25325001 (discussing the privacy-security tradeoff, and suggesting that after September 11, 2001 people may be willing to trade some privacy rights for increased security, but with limitations).

242. Greg Miller, *Response to Terror*, L.A. TIMES, Oct. 4, 2001, at A3 (discussing such proposed legislation).

If there is a pendulum swing in the United States away from privacy rights that appear to impede the government's ability to protect against terrorism, it may widen the existing gap between U.S. and European privacy values. The question of its effect is a difficult one to answer, because there are forces acting in two different directions. On one hand, there are reasons to believe that U.S. retrenchment from growing privacy rights might not be matched by a parallel and equal retrenchment in Europe. For one, the terrorist acts of September 11 occurred in the United States, so it is possible that the U.S. reaction will be most severe.[243] Moreover, since substantial U.S. recognition of serious data privacy interests is so recent a phenomenon, it may not have the "legs" of more firmly entrenched, long-standing European pro-privacy values. Either of these dynamics could result in rapid U.S. renunciation of data privacy initiatives, without an analogous move on the part of Europe. Should this prove to be the case, the gap will grow, and the already aggressive EU Data Privacy Directive will potentially become more divisive.

On the other hand, the gulf between U.S. and European attitudes might remain unaffected by, or even be reduced by, the September 11 attacks. Since EU and U.S. political interests are largely aligned in the war against terrorism,[244] it is possible that the European Union will move closer to the United States as a result of the attacks, rather than the United States moving away from the European Union. To the extent that Europeans feel vulnerable as a result of terrorism, they may shift their emphasis away from data privacy and toward protective anti-terrorist surveillance programs.[245] Furthermore, since much of Europe confers upon government a stronger role in protecting the public welfare than has been true of the post-Reagan era United States,[246] Europe may in some ways be more receptive, rather than less receptive, to initiatives that strengthen the government's antiterrorist capabilities. This result

---

243. This is only one possibility. Given much of Europe's sympathetic alliance with the United States following the attacks, such as British Prime Minister Tony Blair's strong statements aligning the United Kingdom with the United States, it is possible that the threat is seen as being equally palpable in Europe, and therefore will have a similar effect on European desire for effective antiterrorist monitoring tools.

244. Geoff Meade et al., *EU Pledges to Join US Response to Terror Attacks*, PRESS ASS'N, Sept. 21, 2001, at Home News (noting a firm backing of European leaders of "a targeted American response to the terrorist atrocities in Washington and New York").

245. *Beating Terrorism Will Mean Sacrificing Some Freedoms*, EXPRESS (London), Sept. 20, 2001, at 12 (suggesting that the British must reassess their priorities in regard to personal freedoms in the wake of the terrorist activities of September 11, 2001).

246. Kennedy, *supra* note 234.

would reflect a more general emphasis on community welfare[247] in some European nations.[248] This theory could be consistent with Europe's traditional strong pro-privacy stance, especially to the extent that modern privacy concerns in Europe focus on breaches initiated by the private sector rather than the public sector.

VI. CONCLUSION

There can be no doubt that modern technology has heightened the world's interest, albeit to varying degrees, in the protection of data privacy. The European Union has taken an aggressive leadership position, and has elected to force the issue as a means of ensuring that its strong protections not be diluted or destroyed as soon as data pass beyond EU borders. This policy is but one example of a broad policy question facing the shrinking globe in the age of the Internet: how is an ever more integrated world to govern relations in light of historic limitations of sovereignty?

How question is answered is likely to affect international relations, and potentially the world, in the twenty-first century and beyond. The terrorist tragedies of September 11, 2001 certainly force the question to the world's immediate attention. The future success of the EU Data Privacy Directive could serve as an important proving ground for a position of aggressive regional leadership. But success is by no means guaranteed. Meanwhile, the fate of the Directive plays a critical symbolic role in the tension between coercion and colloquy in the future forging of global policy.

---

247. For detailed discussion of community in global capitalist markets, see Don Mayer, *Community, Business Ethics, and Global Capitalism*, 38 AM. BUS. L.J. 215 (2001).

248. Some Western European cultures, such as Germany, tend to embrace a more communitarian and less individualistic ethics than one sees in places like the United States. Timothy L. Fort & Cindy Schipani, *Corporate Governance in a Global Environment: The Search for the Best of All Worlds*, 33 VAND. J. TRANSNAT'L L. 829, 832 (2000) (discussing this distinction in terms of communitarian and contractarian models of corporate governance).

* * *