# THE EUROPEAN UNION DATA PRIVACY DIRECTIVE

*By Julia M. Fromholz*

In an increasingly wired world, even our mundane daily transactions leave permanent records. What brand of toothpaste do we buy? Ask the supermarket's marketing department, which maintains a database of our "discount card" purchases. What stores do we frequent? Check with the credit card company, which tracks our every purchase. Which movies do we rent? Tap into the video-rental store's computer, and retrieve the records in an instant. With the omnipresence of the computer, coupled with the interconnectivity of the Internet, not only can such individual firms keep and analyze detailed records about us, but they can also spread such information quickly and easily anywhere in the world.

The ubiquity of computers and the growth of networks have made the collection, analysis, and dissemination of personal data inexpensive and easy. This growth has also led to a heightened concern about the level of protection afforded to personal data. National boundaries no longer present a barrier to data flows; therefore, a regulatory regime with traditional, territory-based rules can have only a limited effect. Some countries seeking to protect the privacy of their citizens' data have done so in ways that extend the reach of their data privacy laws into other countries. Conflict over such reach is virtually inevitable and, if serious, will likely impede the growth of worldwide electronic commerce.

In the European Union ("EU"), governments have moved aggressively to regulate the use of personal data. In the United States, on the other hand, the government has largely refrained from such regulation, instead allowing companies and associations to regulate themselves, save for a small number of narrowly drawn regulations targeting specific industries.[1]

---



1. American and European approaches to data protection are fundamentally different. European privacy statutes tend to protect information proactively and broadly, while American privacy statutes tend to stem from reactions to specific crises. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 5 (1996). This book, commissioned by the EU to give an overview of U.S. data protection law, provides a comprehensive analysis of data protection law in several fields in both the public and private sectors. The authors identify medical and direct marketing data as being particularly loosely protected by U.S. government regulation. *See id.* at 154, 308-09.

These divergent responses to the challenge presented by the proliferation of electronic data can best be explained by different cultural mores and the different legal approaches to privacy in general.[2]

The EU's aggressive regulation of the use of personal data originating in its fifteen member countries is embodied in its Directive on the Privacy of Personal Data 95/46/EC ("the Directive"), which took effect on October 25, 1998.[3] The Directive embodies the principle that privacy is a fundamental human right.[4] It also serves the purpose of equalizing the level of data privacy protection guaranteed in each EU member country so as to decrease transaction costs for entities that operate across national borders.[5] The Directive provides a high level of protection for the privacy of personal data, and it extends that protection beyond the EU by prohibiting the transfer of data to third countries[6] unless those countries can guarantee a vaguely defined "adequate" level of data protection.[7] Although some Americans have long called for stronger regulation, it seems unlikely that the U.S. will pass comprehensive data privacy legislation in the near future.[8] Such an absence of an overarching privacy law seems to be the primary reason that the EU has already concluded that the U.S. does not provide adequate protection, as defined in the Directive.[9] American firms

---

2. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 153 (1998). The authors state that while Americans "have a strong suspicion of government and a relatively strong esteem for markets and technology," Europeans "have given government a more prominent role in fostering social welfare but have placed more limits on unfettered development of markets and technology." *Id.*

3. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [hereinafter Directive]. The Directive is available at *Community Legislation in Force* (visited Dec. 1, 1999) ⟨http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html⟩, as well as in FRED H. CATE, PRIVACY IN THE INFORMATION AGE 133-76 app. A (1997), and in SWIRE & LITAN, *supra* note 2, at 213-46 app. A.

4. *See id.* at art. 1(1); James Harvey, *An Overview of the European Union's Personal Data Directive*, COMPUTER LAW., Oct. 1998, at 19.

5. *See Data Protection: Background Information* (visited Aug. 27, 1999) ⟨http://europa.edu.int/comm/dg15/en/media/dataprot/backinfo.htm⟩.

6. The term "third countries" refers to countries outside the EU.

7. Directive, *supra* note 3, at art. 25.

8. *See infra* Part III.A.

9. *See Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government* (visited Aug. 28, 1999) ⟨http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp15en.htm⟩ ("[T]he Working Party takes the view that the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied

must therefore figure out how to comply with the Directive's privacy standard, perhaps by exploiting what little flexibility it allows, or else face the prospect of having the flow of data from Europe cut off at the source. While individual firms, trade associations, and government entities are well aware of the problem and are working to avoid such a blockage, any solution to the immediate challenge posed by the EU Directive will likely not satisfy the need for a more certain privacy protection standard in the U.S., and indeed throughout the interconnected world.

## I. DEFINITIONS OF PRIVACY AND COSTS OF PROTECTION

Citizens and governments of both the U.S. and Europe have long debated the appropriate level of privacy protection and have come to varying conclusions. Before discussing "privacy," however, it is necessary to define the term with some precision and to acknowledge both the costs and benefits of protecting it. The Directive attaches great import to the privacy of personal information, at least as compared to the standards of other countries today. Yet protecting privacy is not a pure and unquestioned good.

### A. The Meaning of "Privacy"

The theoretical basis of a right to privacy is not always clear,[10] especially in an age in which the computer is ubiquitous.[11] The literature ex-

---

upon to provide adequate protection in all cases for personal data transferred from the European Union."). Article 29 of the Directive created the Working Party, and Article 30 authorizes it to advise the European Commission on matters related to implementation of the Directive, including data protection standards in third countries. *See* Directive, *supra* note 3, at arts. 29, 30.

10. In 1890, Louis D. Brandeis & Samuel D. Warren wrote the seminal article on privacy, basing their analysis on the "right to be let alone." Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). One contemporary view of the privacy problem today is that it does not concern just disclosures of embarrassing facts, but that it "involves disclosures that threaten control." Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990*, 80 CALIF. L. REV. 1133, 1146 (1992).

11. The current focus on privacy may be due to the explosive growth of computers and networks: the protection of personal data arguably "revived in the 1960s when computers began to take a prominent place in public awareness." Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 133 (1996). That argument is based on the idea that people started paying attention "when new physical, psychological and data surveillance technology applications transformed privacy into an issue that affected average consumers." *Id.* at 134 n.15. An example of such an application is 1800USSearch.com, where, for a nominal fee, anyone can run a search to find a person's

amining what privacy means and whence privacy interests spring is extensive.[12] Some theorists argue that personal information should be deemed a form of property; under this view, others have no more right to use our personal information without our permission than they do to drive our cars or enter our houses. This concept is intuitively appealing, as we may have a sense that we own information that is personal to us. On further reflection, however, a property right in personal information is a troublesome concept. Professor Arthur Miller has argued that a property right to privacy would protect far too much:

> The objective of protecting individual privacy is to safeguard emotional and psychological tranquillity by remedying an injurious dissemination of personal information; it was never intended to serve as a vehicle for defining the legal title to information or as a method for determining who has the right to control its commercial exploitation—typical functions of the law of property.[13]

A property right also seems not to fit the situation of the privacy of personal data because in order for the "information to be 'property,' . . . the owner must possess it. The difficult question[, however, is] how someone could 'possess' an intangible thing, like information, which [is] not subject to physical control."[14] A property right to privacy of personal data thus may not be justified on the basis that one person's use of the data makes the information less useful for others; data may be replicated many times over without losing any of its utility.[15]

---

current and past addresses; phone number; vehicle make, model, purchase price, and current value; debts; and other personal data. *See 1-800 U.S. Search—Instant Search* (visited Jan. 29, 2000) ⟨http://www.1800ussearch.com/fast6_credit.htm⟩.

12. One participant in this debate has compiled a fairly comprehensive list of distinct rights that are often referred to under the common rubric of "privacy":

> The right to individual autonomy; The right to be left alone; The right to a private life; The right to control information about oneself; The right to limit accessibility; The right of exclusive control of access to private realms; The right to minimize intrusiveness; The right to expect confidentiality; The right to enjoy solitude; The right to enjoy intimacy; The right to enjoy anonymity; The right to enjoy reserve; The right to secrecy.

DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 8 tbl.1 (1989). This Note focuses only on the right to control personal information in this discussion of the EU Directive and other possible ways to regulate privacy protection.

13. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 212 (1971).

14. Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 254 (1998).

15. *See id.*

## B. Costs and Benefits of Protecting Privacy

Though proponents of heightened privacy protection often speak as if privacy is an unquestionable individual and societal good, it must be acknowledged that privacy carries costs as well. Privacy allows people to act autonomously, providing them the "private space to develop, and reflect on, ideas and opinions," thereby strengthening a democratic government.[16] With privacy, people may also develop their individuality, apart from the groups to which they belong.[17] Privacy gives people the ability to decide what face they want others to see; such freedom allows people to set their own path to a greater degree than they would be able without it. But "privacy is not an absolute good because it imposes real costs on society."[18] In protecting some individual rights, a broadly defined privacy right not only fails to protect other individuals and society from the consequences of, but indeed promotes, "the dissemination of false information . . . [and] the withholding of relevant true information."[19] Privacy thereby imposes economic and social costs, as people are less able to acquire the information necessary to make fully informed decisions, such as whether a "child's babysitter had been convicted for child abuse" or whether a "physician had a history of malpractice."[20]

In seeking the appropriate level of protection for personal data, governments, industry groups, and companies must consciously balance these costs and benefits, rather than blindly hop on the privacy bandwagon. Achieving the proper balance is difficult because "[o]ne individual's privacy interests may conflict with another's, with the interests of society, or even with others of his own interests."[21] But it is clear that a system that unthinkingly elevates privacy above other interests will give insufficient regard to the costs privacy imposes on the very people it is intended to benefit.

---

16. CATE, *supra* note 3, at 24.

17. *See id.* at 25-26.

18. U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999) (invalidating FCC regulations concerning the privacy of telephone customers' personal information).

19. CATE, *supra* note 3, at 28.

20. *Id.* at 29.

21. *Id.* at 31.

## II. THE EU DIRECTIVE: BACKGROUND AND SCOPE

### A. Prelude to the Directive

European citizens and their governments view privacy as a fundamental human right and thus support strong protections against the unauthorized commercial use of personal data.[22] European governments have long debated the appropriate way to safeguard their citizens' personal information from improper exploitation; the Directive is only the latest development in this process, which has involved discussion outside the forum of the EU as well.

In 1980, the Organization for Economic Cooperation and Development ("OECD")[23] passed an international agreement concerning data privacy.[24] The guidelines promulgated by the OECD were intended as a response to the "danger that disparities in national legislations could hamper the free flow of personal data across frontiers."[25] The Guidelines set forth basic principles underlying data privacy protection; the OECD intended that these "principles . . . be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."[26] The OECD principles are largely mirrored in the Directive's principles.

Although the OECD Guidelines, which do apply to electronic data,[27] reflect a basic agreement on principles for data protection, they are not binding and do not set a maximum level of permissible protection,[28] the absence of which may hinder harmonization of national laws.[29] In addi-

---

22. *See* Directive, *supra* note 3, at art. 1(1).

23. The OECD consists of 29 member countries, including the United States and many European countries, as well as some in Asia. *See What is OECD* (visited Nov. 1, 1999) ⟨http://www.oecd.org/about/general/index.htm⟩; *OECD Member countries* (visited Dec. 1, 1999) ⟨http://www.oecd.org/about/general/member-countries.htm⟩.

24. *See* OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [hereinafter OECD Guidelines]. This document is available at *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (visited Nov. 1, 1999) ⟨http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM⟩.

25. *Id.*

26. *Id.*

27. *See Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet* (visited Nov. 1, 1999) ⟨http://www.oecd.org/dsti/sti/it/secur/prod/reg97-6e.htm⟩.

28. *See* OECD Guidelines, *supra* note 24.

29. *See* Jane A. Zimmerman, Comment, *Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism*, 4 J. INT'L L. & BUS. 601, 623-24 (1982) (stating that the Council of Europe Convention's failure to set

tion, because each member country must implement the Guidelines on its own, their implementation is not at all certain.

Although the OECD Guidelines may set forth principles on which all or most countries agree, the OECD does not have the power to enforce its recommendations, and it seems unwilling or unable to take on the contentious issue of how countries should work together to bridge their different standards of protection. The OECD does state that it will "[s]upport Member countries in exchanging information about effective methods to protect privacy on global networks, and . . . report on their efforts and experience in achieving the objectives of this Declaration."[30] But that is a far cry from a firm commitment to achieve a single international standard.

In another attempt at establishing data-protection guidelines, the Council of Europe, an organization of forty-one countries that focuses on "strengthen[ing] democracy, human rights, and the rule of law throughout its member states,"[31] promulgated a Convention on Personal Data.[32] This Convention provides consistent principles intended to inform national legislation on the protection of personal data.[33] The Council has largely failed to achieve uniform protection for personal data, however, because it could not force countries to implement its Convention through legislation.[34] Additional barriers to uniformity sprang from existing national data protection legislation and the Convention's failure to define key terms.[35] Although neither the OECD Guidelines nor the Council of Europe Convention resulted in uniformity of national data protection laws, they both set the stage for the broad and deep protection afforded by the Directive.

## B. The Directive

Although the EU Data Privacy Directive has been approved by the EU itself, it is not self-implementing. Before taking effect in individual na-

---

maximum standards for data privacy protection will allow countries to refuse all data flows with other countries, even if all have agreed to and abide by the Convention).

30. OECD Working Party on Information Security and Privacy, Ministerial Declaration on the Protection of Privacy on Global Networks 5 (Oct. 1998), *available at* ⟨http://www.oecd.org/dsti/sti/it/secur/prod/reg97-6e.htm⟩.

31. *About the Council of Europe* (visited Dec. 1, 1999) ⟨http://www.coe.fr/eng/present/about.htm⟩.

32. *See* European Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, *cited in* Rosario Imperiali d'Afflitto, *Recent Development: European Union Directive on Personal Privacy Rights and Computerized Information*, 41 VILL. L. REV. 305, 305 (1996). The Convention became effective in 1985. *See* CATE, *supra* note 3, at 34.

33. *See* d'Afflitto, *supra* note 32, at 305.

34. *See* CATE, *supra* note 3, at 34.

35. *See id.* at 35.

tions, each of the fifteen EU member countries must pass its own implementing legislation.[36] As of the effective date, only five had done so.[37] And even now, the interpretation of some parts of the Directive, particularly those concerning the transfer of data to third countries, is still being clarified by the Working Party.[38]

The European Commission, which proposes legislation for the EU and monitors the implementation thereof, has identified several goals of the Data Privacy Directive. The explicit primary goal was to harmonize data privacy laws among the fifteen member states of the EU.[39] In an effort to reach that goal, the Directive sets a minimum level of protection; however, it does not set a maximum limit.[40] Linked to the goal of harmonization is the Commission's mandate to protect its citizens' fundamental rights, including the right to privacy.[41]

In order to achieve these goals, the Commission took a broad view of data protection. It established high levels of protection for personal data, requiring, with narrow exceptions, that entities collecting personal data get permission from individuals whose data they wish to exploit.[42] The Com-

---

36. *See Data Protection: Background Information*, *supra* note 5.

37. *See* Chris Nuttall, *Privacy Laws Protect Personal Data* (last modified Oct. 24, 1998) ⟨http://news2.thls.bbc.co.uk/hi/english.sci/tech/newsid%5F200000/200284.stm⟩. These countries were the United Kingdom, Greece, Italy, Portugal, and Sweden. *See id.* As of September 1999, Belgium, Finland, and Austria had also implemented the Directive, leaving seven of the fifteen member countries without implementing legislation, nearly a year after the "effective" date. *See Status of Implementation of Directive 95/46* (visited Dec. 1, 1999) ⟨http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm⟩.

38. *See, e.g.*, Letter from Ambassador David L. Aaron, United States Under Secretary of Commerce for International Trade, to industry groups (Nov. 15, 1999), *available at* ⟨http://www.ita.doc.gov/ecom/aaronmemo1199.htm⟩ [hereinafter Aaron Letter]. For an explanation of the mandate of the Working Party, see *supra* note 9.

39. *See Data Protection: Background Information*, supra note 5.

40. *See* d'Afflitto, *supra* note 32, at 310; *see also* Directive, *supra* note 3, at art. 26(1) (stating that, with some narrow exceptions, member countries shall not allow data transfers to third countries lacking "an adequate level of protection," except "where otherwise provided by domestic law governing particular cases"). As noted *supra* note 29, such an absence of a maximum limit can be as destructive of harmony as is a lack of a minimum limit.

41. *See* d'Afflitto, *supra* note 32, at 310.

42. *See* Directive, *supra* note 3, at art. 7. Those collecting data ("data controllers") may be public or private entities. Those whose data are at issue are called "data subjects." *See id.* at art. 2(d). The Directive limits its protection to "personal data," which it defines as "any information relating to an identified or identifiable natural person . . . [which is] 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 identity." *Id.* at art. 2(a). The Directive does, however, cover non-electronic data, as long as they are part of a "filing system." *Id.* at art. 3.

mission directed each member country to create an independent supervisory body to oversee the regulation of personal data[43] and established a right of redress for data subjects in order to ensure that its provisions are rigorously enforced.[44]

Because transferring data across national borders generally involves no more effort than sending it next door, the Commission also sought to make uniform the protection given to all data originating in the EU, regardless of the location of processing.[45] The transfer requirements in Articles 25 and 26 also seek to avoid the problem that "[d]ouble standards would inevitably not only affect the credibility of the Union's regulatory aspirations but also favor, if not incite, attempts to relocate the processing of personal data."[46] Article 25 requires that data be transferred only to countries that ensure a notably undefined "adequate" level of protection,[47] while Article 26 sets out some exemptions to the Article 25 rule.[48] The detailed exemptions in Article 26 are narrow but provide some flexibility by allowing firms and customers to individually contract for the protection of personal data.[49]

---

The EU gives different types of data different levels of protection: more rigorous rules than those imposed on most types of personal data are imposed on the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and . . . data concerning health or sex life." *Id.* at art. 8; *see also Data Protection: Background Information*, *supra* note 5.

43. *See* Directive, *supra* note 3, at art. 28. In addition, Articles 29 and 30 create the Working Party, which advises the Commission on matters regarding the Directive but does not enforce its provisions. *See* Directive, *supra* note 3, at arts. 29-30.

44. *See id.* at arts. 22-24.

45. *See id.* at art. 25.

46. Spiros Simitis, *Foreword* to SCHWARTZ & REIDENBERG, *supra* note 1, at vi.

47. Directive, *supra* note 3, at art. 25(1). "Adequacy" of the privacy protection afforded by non-EU countries is to be "assessed on a case by case basis 'in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations'." *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (adopted by Working Party on July 24, 1998) (visited August 28, 1999) ⟨http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp12en.htm⟩ [hereinafter *Transfers*] (quoting Directive art. 25(2)).

48. Article 26(1) includes exemptions for unambiguous consent of the data subject (paragraph (a)), contractual necessity (paragraph (b)), and public interest necessity (paragraph (d)), among others. *See* Directive, *supra* note 3, at art. 26(1).

49. *See* Directive, *supra* note 3, at art. 26(2) .

## III. THE U.S. PERSPECTIVE ON PRIVACY AND ON THE DIRECTIVE

### A. U.S. Perspective on Data Privacy

Americans and Europeans conceive of data privacy in fundamentally different ways. In fact, the language Americans and Europeans use in discussing the issue reflects this deep disparity: Americans tend to use the term "privacy," while Europeans discuss "data protection."[50] In the U.S., "privacy" can refer to anything from a woman's right to abortion, to a resident's right to be free from the gaze of a "peeping Tom," to an individual's ability to choose whether he wants his name included on a telemarketing list.[51] Europeans, on the other hand, tend to speak more precisely of "data protection," referring to the narrower issue of regulating the collection and processing of personal data, rather than of "privacy" in general.[52]

#### *1. Constitutions and statutes*

Government regulation of data privacy in the United States starts with the U.S. Constitution, which protects, in a variety of ways, freedom from government intrusion into private affairs.[53] The Constitution circumscribes government regulation of private relationships and promotes the transparency of government itself.[54] Therefore, American privacy statutes regulate the government's use of personal data far more broadly and strictly than the private use of such data.[55] A European model of personal data protection would therefore be a jarring change from the norm of protection in the U.S.

---

50. *See* Gellman, *supra* note 11, at 132.

51. *See* SCHWARTZ & REIDENBERG, *supra* note 1, at 5-12; *see also* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995).

52. *See* Gellman, *supra* note 11, at 132.

53. *See* CATE, *supra* note 3, at 49-52; SCHWARTZ & REIDENBERG, *supra* note 1, at 6-7.

54. *See* SCHWARTZ & REIDENBERG, *supra* note 1, at 6 ("This emphasis [on freedom from government intrusion] creates a basic philosophy that favors the free flow of information, though restrictions on public power also oblige the state to set limits on its own use of personal information.").

55. Compare the Privacy Act of 1974, 5 U.S.C. § 552a (1994), with sectoral laws regulating private use of personal data, such as the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (Supp. IV 1998), the Cable Television Consumer Protection and Competition Act of 1992, 47 U.S.C. §§ 551-554 (1994), and the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994). *See infra* notes 66-71 and accompanying text.

Beyond providing the general structure for privacy protection in the U.S., the Constitution includes specific protections that may pose obstacles to the implementation of European-style data privacy regulation. The First Amendment's free-speech guarantee imposes limits on the ability of the government to regulate the flow of information, including personal data.[56] Indeed, it is the very protection of one kind of privacy embodied in the First Amendment that limits protection of other varieties of privacy.[57] As one commentator points out, "the First Amendment—perhaps the most significant protection for privacy in the Constitution—restrains the power of the government to control expression or to facilitate its control by private parties in an effort to protect privacy."[58] The First Amendment therefore must be considered in any attempt to regulate the use of personal data as broadly as does the Directive.

Cultural standards also shape the U.S. approach to data privacy. Traditionally, Americans have been less likely than Europeans to turn to the government to regulate private enterprise, instead relying on the market or new technologies to address public concerns about commercial activity.[59] The relatively narrow scope of U.S. privacy law, based as it is on the Constitution and cultural mores, seems unlikely to change in the near future, particularly when the impetus for change comes from a culture that takes a very different view of both privacy and the role of government.

One major problem for the EU—one that many Europeans perhaps hoped the Directive would remedy—is that the U.S. does not have a single, overarching privacy law.[60] Federal privacy-protection statutes exist in certain industry sectors,[61] and state laws provide protection in various areas as well.[62] U.S. privacy legislation tends to be reactive;[63] that is, "gov-

---

56. *See, e.g.*, U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224 (10th Cir. 1999) (invoking the First Amendment to invalidate FCC regulation restricting phone company use of customer data for marketing purposes).

57. *See* CATE, *supra* note 3, at 55 ("Just as the First Amendment protects the privacy of every person to think and to express thoughts freely, it also fundamentally blocks the power of the government to restrict expression, even in order to protect the privacy of other individuals.").

58. *Id.*

59. *See* Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L.J. 2024, 2024-25 (1999); *see also supra* note 1.

60. *See* Henry H. Perritt, Jr. and Margaret G. Stewart, *False Alarm?*, 51 FED. COM. L.J. 811, 812 (1999).

61. *See infra* notes 66-71 and accompanying text.

62. *See* CATE, *supra* note 3, at 66-68, 88-89 (discussing state constitutions, which regulate government activities, and state statutes, which regulate private behavior through

ernment tends to intervene only when a specific problem is identified."[64] Moreover, privacy legislation tends "to be narrowly tailored to deal with a specific type of information maintained by a particular sector of the economy."[65] For example, the Video Privacy Protection Act of 1988,[66] also known as the "Bork Bill,"[67] strictly regulates the use of individuals' videotape-rental data, and the Cable Television Consumer Protection and Competition Act of 1992[68] regulates disclosure of personally identifiable information on cable subscribers.[69] The Fair Credit Reporting Act[70] regulates consumer credit report information by, among other provisions, requiring credit bureaus to make certain disclosures to consumers and setting out procedures to be followed in case of disputes. The Children's Online Privacy Protection Act[71] requires operators of websites targeted at children to provide notice regarding personal information collected from children, as well as to obtain parents' consent before collecting such information. This sample of privacy statutes reflects the patchwork nature of American privacy legislation, and this "complex web of privacy laws"[72] means that there is "no single baseline" available by which to compare U.S. law with European standards.[73] Indeed, while some sectors of the U.S. economy would likely be judged to meet the standards set by the Directive,[74] there is little to no chance that other sectors would satisfy them.[75]

---

adoption of a general right to privacy, codification of common law privacy torts, or enactment of sectoral privacy legislation).

63. *See Options for Promoting Privacy on the National Information Infrastructure* (visited Nov. 6, 1999) ⟨http://www.iitf.nist.gov/ipc/privacy.htm⟩ [hereinafter *Options for Privacy*]; *see also* SCHWARTZ & REIDENBERG, *supra* note 1, at 10.

64. *Options for Privacy*, *supra* note 63.

65. *Id.*

66. 18 U.S.C. § 2710 (1994).

67. The statute is so known because it was passed in response to a newspaper's disclosure of Judge Robert Bork's video rental records after he was nominated to the Supreme Court. *See* SCHWARTZ & REIDENBERG, *supra* note 1, at 10.

68. 47 U.S.C. §§ 551-554 (1994).

69. *See id.* § 551.

70. 15 U.S.C. §§ 1681-1681t (1994).

71. 15 U.S.C. §§ 6501-6506 (Supp. IV 1998).

72. SWIRE & LITAN, *supra* note 2, at 43.

73. *Id.* at 43-44.

74. For example, wiretaps, video rental records, student records, and home telephone records "are more strictly regulated than in many European countries." *Id.* at 43.

75. *See id.*

### 2. *Agencies*

In stark contrast to the system established by the EU Directive, there is no single United States government agency that supervises privacy protection. Instead, authority over this issue resides in several agencies, including the Department of Commerce ("DOC"),[76] the Federal Trade Commission ("FTC"),[77] and the Office of Management and Budget ("OMB").[78] This dispersion of authority reflects the reactive and sectoral nature of U.S. privacy protection and also complicates European efforts to negotiate for stronger protection.

---

76. The International Trade Administration in the DOC has taken the lead in negotiations with the EU over a safe harbor approach to U.S. satisfaction of the Directive's adequacy standard. *See infra* Part IV.A. The National Telecommunications and Information Administration in the DOC has also joined the privacy protection fray, publishing privacy principles and reports. *See, e.g.*, *Discussion Draft—Privacy Principles* (visited Nov. 26, 1999) ⟨http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm⟩; *Privacy Study* (visited Nov. 26, 1999) ⟨http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm⟩.

77. Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." FTC Act § 5(a)(1), 15 U.S.C. § 45(a)(1) (1994). The FTC may seek administrative or judicial redress to protect consumers under this provision. *See* FTC Act §§ 5(b), 13(b), 15 U.S.C. §§ 45(b), 53(b) (1994). If the safe harbor, *see infra* Part IV.A, is approved, the FTC will be an active player in enforcing it: "The FTC has committed to reviewing on a priority basis referrals received from privacy self[-] regulatory organizations . . . and EU member countries alleging non-compliance with the safe harbor principles to determine whether Section 5 of the FTC Act . . . has been violated." *Draft Frequently Asked Questions (FAQs): FAQ 11: Dispute Resolution and Enforcement* (visited Nov. 26, 1999) ⟨http://www.ita.doc.gov/ecom/FAQ11DisputeRes1199.htm⟩ [hereinafter *Enforcement FAQ*].

78. The OMB's Office of Information and Regulatory Affairs is charged with monitoring implementation of the Privacy Act of 1974, which regulates only government use of personal information. *See supra* note 55 and accompanying text. In March 1999, the Administration appointed Professor Peter Swire as the OMB's Chief Counselor for Privacy (also known as the "Privacy Czar"); he sees his role as "coordinat[ing] the wide range of federal government agencies in their efforts to shape privacy issues." *Peter Swire Home Page* (visited Dec. 1, 1999) ⟨http://www.acs.ohio-state.edu/units/law/swire1/pshome1.htm⟩; *see also The Standard: News Briefs* (visited Dec. 1, 1999) ⟨http://thestandard.com/article/display/0,1151,3748,00.html⟩. Critics have called for a stronger central figure to oversee data privacy protection: "This is certainly a step toward [a data protection commissioner], but [Swire] doesn't have the resources, role, and authority that most countries' data protection commissioners have." Jason Catlett, Founder of Junkbusters.com, *quoted in* Courtney Macavinta, *U.S. to Appoint Privacy Adviser*, CNET.com, Mar. 3, 1999, *available at* ⟨http://news.cnet.com/news/0-1005-200-339497.html⟩.

## B. U.S. Perspective on the Directive

The European Commission attempted to extend the Directive's reach globally through Article 25, which requires countries receiving personal data from the EU to provide an "adequate" level of protection.[79] If strictly implemented, the Directive could prohibit mundane transactions such as the transfer of data from the European subsidiary of a multinational company to its American headquarters or the transfer of data between code-sharing airlines based in different countries. Although multinational companies "ordinarily expect to comply with local laws," those laws usually do not have extraterritorial effects.[80] However, in this case, the EU's goal—ensuring the same level of protection for data of EU origin no matter where the data are processed—necessarily reaches well beyond the borders of the fifteen member states.[81]

Although the Directive may affect the entire world, the fact remains that only fifteen countries agreed to it. A single, global privacy standard surely would enhance efficiency, but a unilateral decision by a small group of countries is not the most effective way to create a widely accepted standard. The Directive in effect forces the United States, along with all other non-EU countries, to abide by its regulations, to negotiate with the EU in order to win an interpretation that is more flexible than the words of the Directive suggest, or to suffer the ill consequences of not being able to transfer data out of the EU. In a world aspiring to seamless transnational electronic commerce, such a purely regional approach to regulation "jeopardize[s] the aspirations of free trade as codified in the World Trade Organization Agreement."[82] The U.S. might object to the Directive at the World Trade Organization ("WTO"), under which "laws that appear to prevent free trade in goods and services are carefully scrutinized."[83] The General Agreement on Trade in Services ("GATS"),[84] however, includes an exception that permits each member nation to set its own data protection laws without undergoing review by the international body.[85] Despite this likelihood that the Directive would survive WTO review, an agree-

79. *See* Directive, *supra* note 3, at art. 25(1).

80. SWIRE & LITAN, *supra* note 2, at 42.

81. *See id.* at 3 ("In the European view these effects [on third countries] are not extraterritorial because the Directive governs only the personal information of people in Europe."). Indeed, at least some in the EU hoped that third countries would enact new privacy legislation in response to the Directive. *See id.* at 154.

82. Perritt & Stewart, *supra* note 60, at 813-14.

83. SWIRE & LITAN, *supra* note 2, at 4; *see also id.* at 188-96.

84. The GATS is enforced by the WTO. *See id.* at 190.

85. *See id.* at 191.

ment among fifteen countries is not the most efficient or effective way to implement a broadly applicable law.

In addition to attempting to impose a foreign set of cultural values on American entities, the Directive also may be trying to impose rules that are not well suited to today's technology. Some scholars argue that the Directive could function well in a mainframe world, but not in a world of distributed processing.[86] For example, the Directive's use of the terms "controller" and "data subject" seems almost archaic in the world of laptop computers and the Internet.[87] "The entity running a Web site is often an individual or a small company—hardly worthy of the term 'controller.' The persons browsing may be equipped with a large variety of tools for protecting their privacy.... Such people are no longer passive and powerless."[88] Looking beyond the language to the application of the Directive, commentators also argue that

> mainframe computers may be easier to fit within the [Directive] than other forms of modern information technology [because] ... mainframes generally exist within major organizations, which are easily identified by regulators and have staff to devote to compliance efforts ... [and because] mainframe operations are a natural setting for self-regulatory measures such as contracts that can be approved by European authorities.[89]

In addition, the Directive requires so much oversight of even individual data transfers that the transaction costs of implementing a system that fulfilled the requirements for every transfer could be prohibitive.[90] It would seem to make little sense for the U.S. and other third countries to spend significant resources attempting to comply with a regulation that cannot realistically be enforced.

## IV. RESOLVING THE CONFLICT BETWEEN U.S. AND EU PRIVACY PROTECTION

Although a third country will not be assured of receiving European data unless it meets the strict standard set out in the Directive, individual organizations in third countries may continue to receive personal data from Europe if they fall within certain exceptions spelled out in the docu-

86. *See id.* at 14.
87. *See id.* at 50.
88. *Id.* at 51.
89. *Id.* at 53.
90. *See generally id.* at 52, 58-59, 64 (discussing the difficulty of monitoring data protection in mainframe, client-server, and Internet environments).

ment. In Article 26, the Directive allows for both self-regulatory measures and contractual provisions to ensure the adequacy of an organization's data privacy protection. However, the U.S. and the EU seem close to agreement on a third alternative, one not explicitly mentioned in the Directive, but one that would provide a structure through which U.S. organizations would be deemed to provide adequate protection. This alternative, negotiated by the DOC and the European Commission, is known as the "safe harbor."

### A. The Safe Harbor Approach

The safe harbor approach would allow American firms to transfer data from EU nations provided that they sign on to a set of privacy-protection principles. Discussions regarding such an approach began in the fall of 1998, around the time that the Directive went into effect. Adherence to the guidelines would provide an American company or industry association a finding that it meets the adequacy standard for data transfers.[91] A safe harbor would fill in what the European Commission sees as gaps in United States privacy statutes, without requiring any legislative action. An organization that earns the presumption of adequacy would experience no blockages in its flow of data from the EU.[92]

After a year of negotiations and comments from interested parties, the European Commission and the DOC have recently reached a new agreement on the safe harbor principles; they are now awaiting further comment from industry groups in the U.S. and other interested committees in the EU.[93] Once the comment deadline has passed, the two sides will consider comments and possibly finalize the proposal.[94]

The safe harbor documents include a list of privacy principles, as well as frequently asked questions ("FAQs") to aid firms in their compliance efforts.[95] In order to qualify for the safe harbor and thereby satisfy the Di-

---

91. *See Draft International Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce* (Nov. 15, 1999), *available at* ⟨http://www.ita.doc.gov/ecom/Principles1199.htm⟩ [hereinafter Draft Safe Harbor of 11/99]. Under the previous draft safe harbor principles, promulgated in November 1998, a company adhering to the safe harbor would have earned only a presumption of adequacy. *See International Safe Harbor Privacy Principles* (visited Aug. 28, 1999) ⟨http://ita.doc.gov/ecom/shprin.html⟩.

92. *See* Draft Safe Harbor of 11/99, *supra* note 91.

93. *See id.*; Aaron Letter, *supra* note 38.

94. The EU has agreed not to disrupt data flows to the United States during the negotiations; that "'standstill'" will apparently continue as long as good faith negotiations are underway. *See* Aaron Letter, *supra* note 93.

95. *See id.*; *Draft Frequently Asked Questions (FAQs), available at* ⟨http://www.ita.doc.gov/ecom/menu.htm⟩.

rective's adequacy standard, a company may develop its own "self[-] regulatory privacy policies . . . conform[ing] with the principles," or it may "join a self[-]regulatory privacy program that adheres to the principles."[96] A company may also self-certify its adherence to the safe harbor if it is regulated by a body of law that provides sufficient protection for personal privacy.[97] The EU has highlighted two further requirements for protection by the safe harbor: "organizations must publicly declare their adherence to the Principles and . . . [they] must be subject to the jurisdiction of the Federal Trade Commission or another government body with powers to take enforcement action in cases of deception or misrepresentation."[98] The current safe harbor proposal envisions that "all enforcement [will] be carried out in the United States, subject to very limited exceptions."[99] The Enforcement FAQ identifies the FTC and privacy seal programs[100] as principal actors in the effort to ensure adherence to safe harbor principles.[101]

## B. Other Ways to Provide Adequate Protection

Article 26 and Working Party papers identify alternative ways third-country organizations may satisfy the adequacy standard if their home country is deemed inadequate: self-regulation[102] and private contracts.[103] Other options may be available as well, as the Working Party has acknowledged that the volume of personal data transfers would make impossible the case-by-case analysis of protection foreseen in Article 25.[104] It

96. Draft Safe Harbor of 11/99, *supra* note 91.

97. *See id.*

98. *Summary of the Main Operative Provisions of a Possible Decision on the Basis of Article 25.6 of the Data Protection Directive Concerning the U.S. "Safe Harbor", available at* ⟨http://www.ita.doc.gov/ecom/256summary1199.html⟩. However, in a footnote to that document, the U.S. asserts that this "condition applies only to participants in the 'safe harbor' relying wholly or partly on self-regulation." *Id.* at n.2.

99. Aaron Letter, *supra* note 38.

100. *See Enforcement FAQ, supra* note 77; *see also infra* notes 133-135 and accompanying text.

101. *See Enforcement FAQ, supra* note 77.

102. *See First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy* (June 26, 1997) (visited Nov. 13, 1999) ⟨http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp4en.htm⟩ [hereinafter *First Orientations*]; *Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?* (Jan. 14, 1998) (visited Nov. 13, 1999) ⟨http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp7en.htm⟩ [hereinafter *Judging Industry Self-Regulation*].

103. *See* Directive, *supra* note 3, at art. 26(2) (stating that "adequate safeguards . . . may in particular result from appropriate contractual clauses").

104. *See First Orientations, supra* note 102.

therefore has suggested two alternative ways of ensuring the requisite level of protection: a "White List" of acceptable third countries,[105] and a risk analysis using the level of risk to personal privacy posed by different types of processing and of data to "determine the precise nature of what is considered to be 'adequate protection.'"[106] But self-regulation and contractual provisions may well provide more certainty for the organizations involved than would the White List, which might apply to only a few countries, or the risk analysis, which might not apply to a company's most important data transfers.

*1. Industry self-regulation*

Self-regulation allows for flexibility in that companies and associations that wish to comply with the Directive may do so entirely on their own, without delays or prolonged negotiations.[107] However, self-regulation may raise the problem of preemption, as industry regulations that provide adequate safeguards may not prevail over conflicting laws.[108] The variety of self-regulatory measures available, and the different standards they are likely to have, results in "a reasonable likelihood of a responsible company finding potential or real conflicts, or overlaps even at the voluntary level."[109] A company that adheres to a self-regulatory code in one country but does business in another might also run afoul of the second country's laws, as different countries are likely to have divergent codes and laws.[110] If self-regulatory codes are unable to assure certainty of enforcement in situations such as these, such codes are unlikely to be widely developed and used.

a) The Directive Approach

If a third country is not in compliance with the Directive, its industries can choose to provide an adequate level of protection by writing and adhering to industry codes that do provide sufficient data privacy protec-

105. *See id.* Although such a list would be an efficient means of ensuring that a country provides adequate protection, it would likely be complicated by factors such as sectoral differences in privacy protection in third countries and a difficulty in deciding who should determine the composition of the list. *See id.*

106. *Id.*; *see also* SWIRE & LITAN, *supra* note 2, at 167-69.

107. *See* SWIRE & LITAN, *supra* note 2, at 157.

108. *See* Gellman, *supra* note 11, at 143.

109. *Id.* at 144.

110. *See id.* at 145.

tion.[111] One advantage of self-regulation is that the process is likely to move more quickly than would governments seeking to pass legislation.[112]

The Working Party has stated that one of the key factors in assessing industry self-regulation is determining the "degree to which its rules can be enforced."[113] On this point, the Working Party focuses more on the sanctions the industry group can impose than on the size of the group, although it also states that the latter may inform the analysis of the former.[114]

According to the Working Party, self-regulation must achieve the basic principles of the Directive.[115] By assessing an industry code's effectiveness in achieving these principles, one can determine whether the code will provide "a good level of general compliance[,] support and help to individual data subjects[, and] appropriate redress (including compensation where appropriate)."[116] The Working Party states that this analysis is an objective matter and therefore should not be difficult to perform.[117] Some factors may make the analysis easier; for example, punitive sanctions and mandatory external audits are, in the Commission's view, effective ways to gauge whether an industry code will afford adequate protection.[118]

b) U.S. Industry Views

Most U.S. businesses strongly prefer self-regulation to the alternative of state-imposed mandates. Companies have taken several different routes, none mutually exclusive, to regulate themselves: industry codes, organi-

111. *See* Directive, *supra* note 3, at art. 25(2) ("The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation; particular consideration shall be given to . . . the professional rules and security measures which are complied with in that country."); *see also Judging Industry Self-Regulation*, *supra* note 102.

112. *See* SWIRE & LITAN, *supra* note 2, at 157.

113. *Transfers*, *supra* note 47. In this document the Working Party defines industry self-regulation as "any set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned." *Id.* The Working Party acknowledges that this definition is a broad one, encompassing a wide range of codes. *See id.*

114. *See id.*

115. *See First Orientations*, *supra* note 102.

116. *Judging Industry Self-Regulation*, *supra* note 102.

117. *See id.*

118. *See id.*

zations such as the Online Privacy Alliance,[119] and third-party privacy seal programs.[120]

Many industry groups, including the powerful Direct Marketing Association ("DMA"), vehemently favor self-regulation over government regulation, as this approach allows them to establish the limits of protection.[121] The DMA has promulgated a "Privacy Promise" for consumers[122] and established a "Privacy Task Force," but it has also hired lobbyists to promote its cause among those who will make decisions on behalf of consumers.[123] On their own, the promise and the task force can do little more than set expectations for DMA members; enforcement authority must accompany such steps if they are to provide real protection. The DMA does "issu[e] quarterly reports on members who are being disciplined for violating DMA codes of conduct,"[124] but such action may not be enough of a deterrent to protect consumers. Industry groups such as the DMA will have to overcome a "perceived . . . intrinsic conflict that occurs when data users promulgate their own data protection codes of conduct"[125] if they are to be able to provide the "adequate" privacy protection mandated by the EU Directive.

In 1998, the Online Privacy Alliance ("OPA"), a group of more than eighty global corporations and associations that have organized to promote and lobby for industry self-regulation,[126] announced privacy-protection guidelines somewhat similar to those in the Directive.[127] Notably, how-

---

119. *See Online Privacy Alliance* (visited Nov. 15, 1999) ⟨http://www.privacyalliance.org⟩.

120. *See, e.g., BBBOnline* (visited Nov. 6, 1999) ⟨http://www.bbbonline.org⟩; *TRUSTe: Building a Web You Can Believe In* (visited Nov. 6, 1999) ⟨http://www.truste.org⟩.

121. *See* SCHWARTZ & REIDENBERG, *supra* note 1, at 309.

122. *See The DMA Privacy Promise Information for Consumers* (visited Dec. 1, 1999) ⟨http://www.the-dma.org/pan7/conspri.shtml⟩. The Privacy Promise includes commitments to notify customers that they may opt out of having their personal data shared among companies and to honor such requests. *See id.*

123. *See* SCHWARTZ & REIDENBERG, *supra* note 1, at 309 & n.5.

124. CATE, *supra* note 3, at 107.

125. *Id.* at 108.

126. *See Online Privacy Alliance: Who We Are* (visited Nov. 15, 1999) ⟨http://www.privacyalliance.org/who/⟩. Members include companies and associations in a variety of industries, including 3Com, Bank of America, Bell Atlantic, Dell, Dun & Bradstreet, eBay, Ernst and Young, Microsoft, Procter & Gamble, Time Warner, Xerox, American Advertising Federation, Business Software Alliance, Direct Marketing Association, and Motion Picture Association of America. *See id.*

127. *See* Directive, *supra* note 3; *First Orientations*, *supra* note 102; *Online Privacy Alliance: Privacy Policy Guidelines* (visited Nov. 15, 1999) ⟨http://www.privacyalliance.org/resources/ppguidelines.shtml⟩.

ever, the OPA's enforcement principle is markedly different.[128] As a voluntary organization, the OPA does not have the authority to enforce its guidelines; instead, it relies on agencies such as the FTC, third-party privacy seal programs, and state privacy statutes to ensure that its members adhere to their commitments.[129]

Support for self-regulatory measures is seen across business organizations, whether based in the U.S. or in Europe. For example, the TransAtlantic Business Dialogue ("TABD") is an organization of U.S. and EU companies and industry associations that discusses and develops trade-policy recommendations.[130] Given the character of the TABD's members as multinational corporations and associations, it is not surprising that the group strongly favors self-regulation to protect data privacy and ensure an uninterrupted data flow among countries.[131]

Third-party privacy seal programs hold the possibility of providing a less biased, and therefore more trustworthy, level of protection than do industry groups.[132] As the best known seal programs today, BBBOnline[133] and TRUSTe[134] award seals to websites that meet their standards for privacy protection.[135] The programs also promise to monitor the sites they license to ensure their continued adherence to the seals' commitments,[136] but such monitoring has yet to prove broadly effective in securing privacy protection. For example, two TRUSTe licensees, RealNetworks and Microsoft, have been accused of using their software to transmit customers' personal data without consent.[137] But because the privacy breach was effected through software, not through the websites bearing the privacy seal,

---

128. *See Online Privacy Alliance: Effective Enforcement of Self-Regulation* (visited Nov. 15, 1999) ⟨http://www.privacyalliance.org/resources/enforcement.shtml⟩.

129. *See id.*

130. *See TransAtlantic Business Dialogue* (visited Sept. 12, 1999) ⟨http://www.tabd.org/tabd.html⟩.

131. *See TransAtlantic Business Dialogue* (visited Sept. 12, 1999) ⟨http://www.tabd.org/resources/content/apr98.html⟩.

132. These programs apply only to consumers and companies doing business online, not to other sorts of electronic data collection.

133. *See BBBOnline*, *supra* note 120.

134. *See TRUSTe*, *supra* note 120.

135. *See BBBOnline Privacy Program* (visited Dec. 1, 1999) ⟨http://www.bbbonline.com/businesses/privacy/index.html⟩; *TRUSTe: for Web Users* (visited Dec. 1, 1999) ⟨http://www.truste.org/users/users_how.html⟩.

136. *See How BBBOnline Protects Your Privacy* (visited Dec. 1, 1999) ⟨http://www.bbbonline.com/consumers/protectsprivacy.html⟩; *TRUSTe: for Web Users*, *supra* note 135.

137. *See* Alex Lash, *TRUSTe Goes Easy on RealNetworks*, THE STANDARD, Nov. 8, 1999, *available at* ⟨http://www.thestandard.com/article/display/0,1151,7536,00.html⟩.

TRUSTe was not able—or perhaps not willing—to enforce the companies' privacy commitments.[138] Privacy seal programs have the potential to solve the enforcement problem, as they are less beholden to data collectors than are other entities, yet they provide more flexibility than does government regulation. But in order to provide real protection, they will have to determine the proper scope for their work as well as ways to avoid even the appearance of providing special treatment to some companies.

*2. Contractual provisions*

Article 26 provides the possibility of flexibility for U.S. businesses by allowing contractual provisions to satisfy the adequacy standard. Article 26(2) contains the first mention of contractual provisions, stating that "adequate safeguards may in particular result from appropriate contractual clauses."[139] In Article 26(4), the Commission stated its further acceptance of "standard contractual clauses" to provide adequate safeguards.[140] Although these provisions may add some flexibility to the Directive's requirements, as is the case with self-regulation, the Working Party's goal for the use of contractual provisions is to export the level of data protection guaranteed in the EU.[141]

Contractual provisions that are used to provide the adequate protection missing in the third country's laws will be judged by the same criteria that would apply to laws and industry self-regulatory codes.[142] The Working Party stated that "[f]or a contractual provision to fulfil this function, it must satisfactorily compensate for the absence of a general level of protection, by including the essential elements of protection which are missing in any given situation."[143] An early Working Party document downplayed the applicability of Articles 26(2) and (4), stating that contractual solutions are "appropriate only in certain specific, and probably relatively rare circumstances."[144] A later document, however, seems to envision wider use of contractual clauses.[145] The Working Party does, however, see

---

138. *See id.*

139. Directive, *supra* note 3, at art. 26(2).

140. *See id.* at art. 26(4).

141. *See Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries* (Apr. 22, 1998) (visited Nov. 13, 1999) ⟨http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp9en.htm⟩ [hereinafter *Preliminary Views*].

142. *See Transfers*, *supra* note 47.

143. *Id.*

144. *First Orientations*, *supra* note 102.

145. The Working Party's *Preliminary Views* states that "there will be some situations in which a contractual solution may be an appropriate solution, and others where it

practical limits on the use of such provisions; in particular, the contract must be "detailed and properly adapted to the data transfer in question," and the data subject must have redress in case of a problem, even if the data processor is in a third country.[146] Therefore, the Working Party concluded, contractual solutions are "particularly suited to situations where data transfers are similar and repetitive in nature [and] . . . where the parties to a contract are large operators already subject to public scrutiny and regulation."[147] Some commentators believe that these limitations mean contractual provisions will be most effective for firms that use mainframes, especially where the processors are large or multinational companies transferring data to branches within the same organization.[148]

## V. CONCLUSION

As industry and government leaders approach a consensus regarding the safe harbor approach to compliance with the EU Directive, the urgent threat of blockages in the data flow appears to have subsided. However, the disparity between U.S. and European data privacy protection laws remains, and thus this negotiated settlement is unlikely to serve as a permanent solution to the problem. Unilateral action, such as the implementation of the EU Directive, will only stir international resentment. Only if a wide array of nations, possibly acting through a body such as the WTO or the United Nations, arrives at an agreement on the appropriate level of data protection will a truly global solution be possible.

Although the U.S is unlikely to enact comprehensive data privacy legislation anytime soon, firms appear willing to establish non-governmental bodies to regulate themselves. The existence of such entities should foster transnational electronic commerce by making public those companies' privacy standards and by creating a structure for enforcement. The private bodies will be hampered in their efforts to self-regulate, however, by a conflicting patchwork of laws. The U.S. may never have a single, national privacy agency or an over-arching privacy statute, but a clearer federal data-protection policy is necessary in order for U.S. companies to continue to function globally. The U.S. is a long way from arriving at such a comprehensive answer; until we reach such resolution, we will be forced

---

may be impossible for a contract to guarantee the necessary 'adequate safeguards'." *Preliminary Views*, *supra* note 141. Although perhaps not a ringing endorsement of contractual solutions, this statement does seem to allow a wider use of them than did *First Orientations*.

146. *Id.*

147. *Id.*

148. SWIRE & LITAN, *supra* note 2, at 164, 173.

merely to react to the standards set by other players in this interconnected world.