9-1-2003

The Future of Online Privacy: A Proposal for International Legislation

Joann M. Wakana

The Future of Online Privacy: A Proposal for International Legislation

I. INTRODUCTION

A revolution in data exchange and data processing has led to the creation of a new, popular forum for communication called Cyberspace.[1] Cyberspace is maintained through the Internet, which is an "internationally linked system of computer networks on which data flows."[2] Today, the Internet plays an important role in social and economic life, and therefore, concerns over online privacy have become a major issue for the millions of people who use the Internet daily.

Recently, both the United States and the European Union have addressed privacy concerns with regard to the Internet. In the United States, "much of current computer privacy law is found in laws [and statutes] . . . targeting specific records for regulation."[3]

In contrast to the U.S.'s diverse and targeted approach, the EU has a more common omnibus approach. The EU has worked to create comprehensive privacy regulations regarding controls over the collection and use of personal data transferred over the Internet.[4] In 1995, the European Parliament and the Council of the European Union adopted the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive), designed to protect the privacy of personal data and increase the security of data flow among the fifteen member states.[5]

The United States is concerned that the EU Directive prohibits online data transfer between its fifteen member states

---

1. RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 389 (West Group 2d ed. 1999).
2. *Id.*
3. TURKINGTON & ALLEN, *supra* note 1, at 429.
4. *See* HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 57 (Facts on File Inc. 1999).
5. Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

and other countries that do not provide *adequate* privacy protection.[6] While the concept of privacy is deeply ingrained in American tradition and the U.S. Constitution, enforcement of privacy rights in the United States is fragmented and much weaker than privacy laws in most European nations. In 2000, in response to the fact that the EU Directive could potentially interrupt transfers of personal information between Europe and the United States, the U.S. Department of Commerce developed a safe harbor framework that allows U.S. organizations to satisfy the EU Directive's requirements while ensuring that personal data flowing to the United States would continue uninterrupted.[7]

In creating the *Safe Harbor Privacy Principles* (Safe Harbor), the U.S. Department of Commerce wanted to bridge the differences between the EU and U.S. approaches to privacy protection while simultaneously ensuring adequate protection for the personal information of EU citizens.[8] The standards contained within the Safe Harbor do not sufficiently remedy global, and more specifically, the EU's concerns about the adequacy of private data protection. Today, there is debate between the United States and the EU about what constitutes adequate protection.

This Comment will discuss why the current U.S. approach to privacy protection is insufficient, and will propose a new international model of privacy data protection legislation which satisfies both EU and U.S. concerns. Part II presents a background on the current approaches taken by the EU and United States in addressing the issue of personal data privacy. It will also examine the privacy guidelines set forth by the Organization for Economic Cooperation and Development (OECD) and the Council of Europe Convention, both of which served as a model and basis for the EU Directive and the Safe Harbor. Part III analyzes arguments for and against an omnibus legislative response in addressing privacy concerns, and discusses the unavailing nature of current U.S. self-regulatory schemes. Finally, Part IV proposes a new international model for privacy protection legislation, and discusses how this type of overreaching international legislation can be successfully implemented and enforced.

---

6. *Id.* art. 25.

7. *See* U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR OVERVIEW, *available at* http://www.export.gov/safeharbor (last visited April 2, 2004).

8. *See id.*

II. BACKGROUND

A. The OECD and the Council of Europe

The OECD "is an international organization that promotes economic and social welfare"[9] by supporting progressive efforts on behalf of developing nations. The United States is a member of this organization.[10] In the late 1970s, the OECD started creating guidelines for data protection, and in the 1980s, it adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines).[11]

The OECD Guidelines are "based on the general principle of fair information practices,"[12] and apply to both automated and non-automated processing of personal data.[13] The OECD Guidelines did not create binding law upon any of its signatories, including the United States.

The Council of the European Union works to promote a greater degree of collaboration among the democratic states of Europe. Beginning in the late 1960s, the Council was already reviewing questions about the effects of technology and privacy. In February 1980, the Council promulgated the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (the Convention).[14] For the most part, the content of the Convention was similar to that of the OECD Guidelines. Unlike its U.S. counterpart, however, the Convention placed more emphasis on the "importance of data protection to protect personal privacy,"[15] and it was legally binding on the member

---

9. Robert Gellman, *Conflict and Overlap in Privacy Regulations: National, International and Private, in* BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 255, 264 (Brian Kahin & Charles Nesson eds., Harvard College 1997).

10. *Id.*

11. OECD, *Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980), *reprinted in* 20 I.L.M. 422 (1981) [hereinafter OECD 1980].

12. Gellman, *supra* note 9, at 265.

13. *See id.*

14. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Council of Europe, Eur. T.S. No. 108 [hereinafter 1981 Convention].

15. FRED H. CATE, PRIVACY IN THE INFORMATION AGE 34 (Brookings Institution Press 1997).

states that joined.[16] The Convention, which took effect in 1985, was only ratified by some of the twenty-nine member states.[17]

Although both the OECD Guidelines and the Convention share similarities, having been developed at approximately the same time and with similar motivation, there are nevertheless significant differences in the scope and application of the OECD Guidelines and the Convention.

First, the OECD Guidelines apply to both automated and non-automated processing of personal data, whereas the Convention is limited only to the automated processing of data.[18] Second, just as the name implies, the OECD Guidelines are recommendations and not legally binding to countries that have signed on. The Convention, on the other hand, is legally binding to the countries that have ratified it.[19] Neither the OECD Guidelines nor the Convention specifies details on practical application of the established standards, and both contain only very general provisions on how to enforce those standards.[20] Therefore, neither the OECD Guidelines nor the Convention can be considered a sufficient model of international privacy data legislation.

B. The EU Approach to Online Data Protection

European institutions are at the forefront of data protection rules and policies. European privacy legislation reflects the apparent "consensus within Europe that privacy is a fundamental human right which few if any other rights equal."[21] The amalgamation of these concerns led to the adoption of the EU Directive in October 1995.[22] While much of the EU Directive is based on the 1981 Council of Europe Convention and the 1980 OECD Guidelines, in many areas the Directive goes further.[23]

---

16. *See* 1981 Convention, *supra* note 14, at 319.

17. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 24 (Brookings Institution Press 1998).

18. *See* OECD 1980, *supra* note 11, ¶¶ 34-36.

19. *See* OECD 1980, *supra* note 11, at 422.

20. Gellman, *supra* note 9, at 265.

21. CATE, *supra* note 15, at 48.

22. *See* Council Directive 95/46/EC, *supra* note 5.

23. PRACTISING LAW INSTITUTE, FIRST ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH TECH AND CHANGING REGULATORY ENVIRONMENT 181 (Practising Law Institute 2002).

The EU Directive contains a complex set of rights, restrictions, and exemptions, which are not found in the OECD Guidelines or the Convention. The expressed intention of the EU Directive is twofold: (1) to ensure uniform levels of protection between EU member states "to remove any obstacles to the free flow of personal data"[24] between the fifteen member states; and (2) to protect the fundamental rights and freedoms of individuals, "notably the right to privacy."[25]

First, in terms of scope, the EU Directive applies to the processing of all personal data, subject to exemptions found in Article 3. Article 3 of the Directive exempts from regulation the processing of "public security, defense, State security, and criminal law activities of the State," as well as data processed by a natural person "in the course of a purely personal or household activity."[26] Second, under Article 4, each member state is required to apply the national provisions it adopts where: (1) the controller is located on the territory of the member state; (2) the controller is located where the national law of the member state applies; or (3) processing equipment is situated on the territory of the member state, unless the use of such equipment is transitory.[27] Third, Article 6 lays out the *Principles of Data Quality*, which limits the collection of data to "specified, explicit and legitimate purposes," prohibiting the processing of data if it is incompatible with those purposes.[28] Furthermore, data must be "adequate and, where necessary, kept up to date."[29] Reasonable steps must be taken to ensure that inadequate data is "erased or rectified," and the data can only be kept for as long as is necessary to satisfy the purpose for which the data was initially collected.[30]

Fourth, Article 7 of the EU Directive generally prohibits the processing of data unless the data subject gives consent in an unambiguous manner. There are exceptions to this, however. Unambiguous consent is not needed under two circumstances: (1) when the processing of data is necessary for "compliance with a legal obligation" to "protect the vital interests of the data

---

24. *Id.*
25. *Id.*
26. Council Directive 95/46/EC, *supra* note 5, art. 3(2).
27. *Id.* art. 4.
28. *Id.* art. 6.
29. *Id.*
30. *Id.*

subject . . . for entering into or performing a contract with the data subject," or (2) when the processing of data is "necessary for performance of a task in the public interest."[31]

Additionally, Articles 10, 11, and 12 refer to the subject's right to know the identity of the collector of the information, and the purpose for the collection of the information. Also, the subject has a right to edit, erase, or intercept the processing of data that fails to comply with EU Directive requirements.[32]

Article 25 is the most significant to the United States. As stated in Article 25, transfer of personal data to a non-European country may take place only if the country ensures an adequate level of data protection.[33] The EU and United States debate over what constitutes adequate protection. The lack of comprehensive national data privacy legislation in the United States and the ad hoc nature of state privacy laws raise serious questions about whether the transfer of data from EU member states to the United States violates Article 25.[34] "Where there is not adequate protection, personal data transferred from [the EU] to the U.S. [is] permitted only [by] one of the [narrow exceptions] in Article 26."[35]

Article 26 allows for exceptions, namely where the subject has given unambiguous consent to the proposed transfer or where the transfer is necessary for the performance of a contract made at the subject's request.[36] The EU has adamantly voiced its concerns regarding the adequacy of the level of data protection the United States provides, and continues to apply consistent pressure on the United States to enact more stringent privacy protection regulation.[37]

---

31. *Id.* art. 7. Under Article 8, the EU Directive applies stricter *consent* rules to data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership" and data "concerning health or sex life." *Id.* art. 8.

32. *See id.* art. 10-12. In addition, if it does not require a "disproportionate" effort on the part of the collector, the collector must notify third parties to whom data has been disclosed or exchanged about any changes. *Id.* art. 12(c).

33. *Id.* art. 25. "This Article is designed to prevent the creation of data havens by third countries that would frustrate the purpose of the Directive." TURKINGTON & ALLEN, *supra* note 1, at 440.

34. *See* Scott Foster, *Online Profiling is on the Rise: How Long Until the United States and the European Union Lose Patience with Self-Regulation?*, 41 SANTA CLARA L. REV. 255, 266 (2000).

35. *Id.*

36. Council Directive 95/46/EC, *supra* note 5, art. 26.

37. *See* HENDERSON, *supra* note 4, at 36.

C. The U.S. Approach to Online Data Protection

In contrast to the comprehensive EU approach, the protection of information privacy in the United States is a "fractured, episodic, recorded targeted patchwork of laws,"[38] which leaves the majority of computerized data without legal regulation. To begin with, there is no precise constitutional guarantee of the right to privacy in the United States.[39] In addition, all constitutional rights apply only against the government, not private actors.[40] Moreover, all of the federal and state privacy laws and regulations currently in place apply only to specific categories of information use.[41] Furthermore, none of the laws currently in effect are comprehensive enough to provide adequate informational privacy across the board.[42] Finally, although the common law of privacy recognizes four basic types of privacy rights under the law of torts, none of these tort actions really offer protection for informational privacy.[43]

The U.S. response to the EU Directive was not the enactment of comprehensive federal data privacy legislation, but rather the creation of the ineffective international Safe Harbor Principles, which require U.S. entities to voluntarily cooperate with the EU Directive.[44] The Safe Harbor framework is supposed to bridge the

---

38. TURKINGTON & ALLEN, *supra* note 1, at 336.

39. Anna E. Shimanek, *Do You Want Milk With Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455, 465-66 (2001).

40. *Id.* at 466.

41. PRACTISING LAW INSTITUTE, *supra* note 23, at 14. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1994) (governs federal records systems); Freedom of Information Act, 5 U.S.C. § 552 (1998) (generally opens government records to the public, but contains medical, personnel, and "similar files"); Video Privacy Protection Act of 1988, 18 U.S.C. § 1681 (2000) (governs access to records of an individual's movie video rentals); Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (sets procedures for government access to newspapers, records and information); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (1998) (requires that Internet sites aimed at children under thirteen receive "verifiable" parental consent for the child's use of the web site).

42. TURKINGTON & ALLEN, *supra* note 1, at 429.

43. *See* Anita L. Allen-Castellitto, *Origins and Growth of U.S. Privacy Law, in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH & CHANGING REGULATORY ENVIRONMENT 9, 24 (Practising Law Institute 2001). The common law recognizes rights against: (1) intrusion upon seclusion; (2) publication of embarrassing private facts; (3) publicity placing a person in a false light; and (4) appropriation of name, likeness, and identity. *Id.*

44. U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES, *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm. (last visited April 2, 2004).

differences between the EU and U.S. approaches to privacy protection.

Voluntary compliance with the Safe Harbor creates a presumption of adequacy, and allows U.S. entities to be eligible to receive personal data from EU member states. Compliance with the Safe Harbor is satisfied where entities take one of the following measures: (1) joining a self-regulatory privacy program which adheres to the Safe Harbor, (2) developing self-regulatory privacy policies which conform with the Safe Harbor, or (3) being subject to other laws or rules which effectively protect personal privacy.[45] Thus, a U.S. entity's decision to comply with the guidelines is voluntary. Once they choose to comply, they have the option to self regulate, which gives them the leeway to enact low standards.

Substantively, under the Safe Harbor framework, organizations that decide to participate in the program must comply with the Safe Harbor's seven requirements,[46] and publicly declare that they do comply.[47] First, "organization[s] must inform individuals about the purposes for which it collects and uses information about them, [and give information on] how to contact the organization with any inquiries or complaints."[48] Also, organizations must give individuals the opportunity to opt out[49] before their personal information is disclosed to a third party or used for purposes other than those for which the information was originally collected. Furthermore, individuals must be given the opportunity to affirmatively or explicitly opt in[50] where personal information is sensitive.

Second, if an organization wants to transfer information to a third party, it must either ensure that the third party subscribes to the Safe Harbor, or that it is subject to the Directive, or some other adequacy finding. It may also enter into a written agreement with the third party requiring that the third party provide at least the same level of privacy protection as is required by the Safe

45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. "Opt out" means an entity can collect user information unless the user affirmatively indicates that they do not want their information collected. *Id.*
50. "Opt in" means an entity must obtain consent from users before they can collect information. *Id.*

Harbor.[51] Third, individuals must have access to any personal information collected about them, and be able to "correct, amend, or delete" information when inaccurate.[52]

Fourth, organizations are required to take reasonable precautions to protect an individual's data from "loss, misuse, and unauthorized access, disclosure, alteration and destruction."[53] Fifth, the Safe Harbor ambiguously states that "personal information must be relevant for the purposes for which it is to be used," without clarifying what constitutes a relevant purpose.[54] Sixth, in terms of enforcement, the Safe Harbor requires: (1) a "readily available and affordable independent recourse mechanism,"[55] (2) procedures for verifying organizations' adherence to and implementation of the Safe Harbor, and (3) an obligation to remedy non-compliance problems when they arise.[56]

Seventh, organizations must self-certify annually with the Department of Commerce by writing a consent agreement adhering to the Safe Harbor requirements and publishing it in its privacy policy statement.[57] In turn, the Department of Commerce maintains a list of all organizations that file the self-certification letters and make the letter, and a list of qualifying organizations, publicly available on its official web site.[58] To date, 175 businesses have voluntarily listed themselves on the Safe Harbor List,[59] and most of the businesses included are smaller businesses and not the Fortune 500 companies that truly make an impact on the world economy and international trade.

The Safe Harbor requirements fail to provide any kind of comprehensive federal regulation. On the contrary, not only is the decision to enter the Safe Harbor completely voluntary, the majority of the regulation and enforcement aspects are carried out

---

51. *Id.*

52. *Id.* An exception is made where "the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in question," or where someone else's rights would be violated by doing so. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. SAFE HARBOR OVERVIEW, *supra* note 7.

58. *Id.*

59. *See* U.S. Department of Commerce, Safe Harbor List *available at* http://www.export.gov/safeharbor (last visited Apr. 20, 2004).

by the private sector with federal enforcement supplied only on rare occasions.[60]

III. OMNIBUS LEGISLATIVE RESPONSE TO ONLINE PRIVACY CONERNS

A. Introduction

There is heated debate over how much regulation concerning online privacy is actually needed. Privacy advocates argue that self-regulation is inadequate due to the lack of enforcement mechanisms and the scarcity of legal options for harmed individuals. On the other hand, industry tends to rigidly favor self-regulation. From the industry's point of view, self-regulation results in efficient market-based solutions, while placing minimal burdens on affected businesses. Therefore, both sides of the debate merit attention.

B. Arguments for Comprehensive Regulation

As the overview on U.S. online privacy policies illustrate, many consumer advocates suggest that some legislative action is required to resolve the inconsistencies relating to privacy protections on the Internet. There are strong advantages to enacting comprehensive federal regulation similar to the EU Directive.

First, U.S. state, federal, and constitutional law simply do not speak to consumer privacy concerns against private actors in any inclusive way. Although the patchwork approach does a decent job of addressing specific categories of concerns regarding privacy, it does not adequately protect consumers from "the aggressive data gathering practices of online marketers."[61]

Therefore, privacy advocates argue, the only way to achieve an acceptable level of protection for online consumers is for Congress to create omnibus legislation that effectively secures consumer privacy rights and clearly sets forth methods for consumers to assert those rights.[62]

---

60. *Id.*

61. Shaun A. Sparks, *The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumer Personal Data*, 18 DICK. J. INT'L L. 517, 542 (2000).

62. *Id.*

Second, the fact that the EU continues to voice its frustration and concerns with the current U.S. standards may have dire consequences for future U.S.-EU trade relations. EU officials have explicitly made clear their view of the U.S. approach to private data protection, stating that it is generally inadequate. Furthermore, it has been a sticking point for long-running trade negotiations between the United States and Europe.[63]

EU data protection officials have some enforcement power regarding international transfers of private information, and this power includes the authority to block data exports by issuing a data embargo order, thereby forbidding or limiting international data export.[64] Such an embargo would have immediate and wide-ranging repercussions for U.S. businesses. Considering these tensions, it would make sense to create a streamlined standard, one that is acceptable for the United States and the EU, as well as for the rest of the world.

Although the EU currently recognizes the Safe Harbor as satisfying the data privacy requirements in the EU Directive,[65] it has become increasingly clear that the EU does not see the Safe Harbor as an adequate remedy to addressing consumer data protection, and it is likely that they will eventually reject the Safe Harbor in its current form. The European Commission's staff working paper concerning the Safe Harbor issued on February 13, 2002, noted the EU's concern that many organizations claiming to comply with the Safe Harbor are not "observing the expected degree of transparency as regards their overall commitment or as regards to the contents of their privacy policies."[66]

According to Professor Dr. Spiro Simitis, the EU may be unwilling to compromise its concerns regarding data protection because privacy is such a fundamental right in European countries.

---

63. Foster, *supra* note 34, at 266.

64. Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows,* 80 IOWA. L. REV. 471, 488 (1995).

65. *See* SAFE HARBOR OVERVIEW, *supra* note 7.

66. Commission Staff Working Paper: The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, SEC (2002) 196, Feb. 13, 2002, *available at* http://europa.eu.int/comm/internal_market/ en/dataport/adequacy/02-196_en.pdf.

As Simitis stated, it is simply "not a subject you can bargain about."[67]

Another argument for comprehensive legislation is that it increases electronic commerce by increasing consumer confidence in how data is handled.[68] Privacy advocates argue consumers will feel more confident in conducting business over the Internet if they know that their information is secure and protected. Although assessing the validity of this argument is difficult, at a minimum, there is overwhelming polling data that shows a widespread concern about online data privacy. A 1995 Equifax consumer survey revealed that 80 percent of "Americans agree consumers have lost all control over how personal information about them is circulated and used by companies."[69] Many people who shy away from electronic commerce for privacy concern reasons would likely otherwise engage in electronic commerce if privacy standards were improved by comprehensive legislation.

Finally, as the Federal Trade Commission's May 2000 Privacy Report illustrates (2000 FTC Report),[70] the U.S. self-regulation approach is failing in its current form. According to the survey taken by the FTC, in a random sample of 335 web sites collecting personal information, only 20 percent of web sites implemented all of the fair information practice principles.[71] This is common under the current Safe Harbor framework, since most of the enforcement is carried out by the private sector itself. Thus, there is little incentive for companies to comply with the standards set forth in the Safe Harbor Principles.

Although the FTC has the power to seek injunctive relief and civil penalties against a private entity which fails to abide by the Safe Harbor, it is clearly not enough of a threat to make these private entities comply with those standards in any significant way.[72] Furthermore, there have been very limited instances where the FTC has actually punished private entities for noncompliance.

---

67. Fred Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L.R. 431, 439 (1995) (quoting Spiros Simitis, Unpubished Comments at the Annenberg Conference on Information Privacy and the Public Interest (Oct. 6, 1994)).

68. SWIRE & LITAN, *supra* note 17, at 79.

69. LOUIS HARRIS & ASSOCIATES AND ALAN F. WESTIN, EQUIFAX-HARRIS CONSUMER PRIVACY SURVEY 1995.

70. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS, (1998) *available at* http://www.ftc.gov [hereinafter PRIVACY ONLINE].

71. *Id.*

72. *Id.*

C. Arguments Against Comprehensive Regulation

On the other end of the spectrum, the market model, or the self-regulation model, defers to the free market to resolve these tensions concerning data privacy.[73] Market model advocates urge Congress to allow businesses to sort out the privacy issue on their own terms and in their own ways.[74] The FTC has basically encouraged a self-regulation approach to online consumer privacy.[75] Advocates of the market model approach argue that consumers will be concerned about online privacy issues as they become increasingly aware of the problem, and the private sector will eventually respond to these concerns because it will be essential for them to do so if they want to maintain their consumer base.[76]

Under the self-regulation model, "the incentives for industry to protect privacy are entirely financial."[77] The idea behind the self-regulation model is that consumers have the power to negotiate what information they wish to disclose to web sites.[78] If consumers care about privacy they will force industry to provide it since "bad publicity about [a] company's privacy practices can detract from the company's total reputation for quality."[79] In this sense, proponents of the market model assert that comprehensive consumer privacy regulation is unnecessary because the market will eventually work itself out.

Proponents of the market model also point out the legitimate and appropriate uses for data gathered through the Internet. One argument is that technology related to online profiling enhances and facilitates electronic commerce. For instance, cookies, small files that a web site's host computer places on a visitor's hard drive,[80] allow a web site to remember information provided by the

---

73. JOHN T. NOCKLEBY, DATA PROFILING INTRODUCTION, *at* http://eon.law.harvard.edu/privacy/Module2_Intro.html (last visited April 20, 2004).

74. Robert O'Harrow Jr., *Survey of Web Finds Gains on Privacy Issues*, WASH. POST, Mar. 28, 2002, at E2, *available at* http://www.washingtonpost.com.

75. Foster, *supra* note 34, at 266.

76. *Id.* at 267.

77. Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm (Sept. 8, 1997).

78. NOCKLEBY, *supra* note 73.

79. Swire, *supra* note 77.

80. "Cookies" are a mechanism that allows a web server to save small packets of data called cookies in a visitor's web browser. The cookie returns with the request each time

visitor, such as her password, email address, credit card number, and mailing address.[81] This means that a consumer will not have to reenter the data on her next visit, saving her time and needless hassle.[82]

Additionally, cookies can also be used to track a consumer's purchasing habit, monitor the pages on a site they view, monitor viewing duration, and learn other information about a consumer's preferences while they surf on the web.[83] Web sites commonly collect information such as a user's social security number, age, sex, date of birth, shopping preferences, health information, financial information, martial status, and hobbies, in order to compile this information into comprehensive user profiles.[84] This information can then be used to customize a site with a consumer's preferences, and offer shoppers suggestions consistent with their needs and tastes.[85]

Accordingly, there are cost and time efficiency benefits to data collection by web sites when used to customize or personalize consumer needs. The warehousing of personal information in the hands of trustworthy third parties can dramatically simplify electronic commerce transactions for the user.

Finally, proponents of the market model point out that privacy concerns about online profiling and other Internet-based data gathering are still very vague, and have not been clearly identified. Consequently, these proponents argue that it would be premature to enact any kind of comprehensive regulation concerning consumer data privacy.[86] As one commentator points

---

the visitor accesses the same web site. Cookies can be used to maintain a list of items a customer has purchased, to store user preferences, or as a means to track the pattern of a visitor's behavior when visiting a web site. Most browsers allow users to disable cookies, however, disabling cookies denies access to some web sites. Charles L. Kerr & Oliver Metzger, *Online Privacy: Emerging Issues, in* PRACTISING LAW INSTITUTE, FIRST ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH TECH & CHANGING REGULATORY ENVIRONMENT 29, 61 (2000).

81. Rita Heimes, *Internet Privacy Law, Policy, and Practice: State, Federal, and International Perspectives*, 54 ME. L. REV. 95, 95 (2002).

82. *Id.*

83. *Id.*

84. ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND CONSUMER PROFILING, *at* http://www.epic.org/privacy/profiling (Oct. 8, 2003).

85. Heimes, *supra* note 81, at 95.

86. *See* Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV., at ¶ 10 (2000), *at* http://stlr.standford.edu/STLR/articles/00_stlr_2.

out, there is currently a "remarkable coming together of various forces pushing for extreme solutions to vaguely identified problems at unknown costs."[87] For instance, in the 2000 FTC Report, the FTC noted "significant consumer privacy concerns" arising from "the prevalence, ease, and relatively low cost" of gathering and processing personal data, and conceded that self-regulation was inadequate to address online privacy issues.[88] In response, the FTC dramatically reversed its prior favorable position on self-regulation and called for federal comprehensive privacy legislation.[89] In the 2000 FTC Report, however, there is absolutely no consideration for costs and benefits of any proposed regulation, nor is there any explanation as to how this unclear and overbroad mandate will be enforced.[90]

Furthermore, it remains unclear whether it is necessary to make a distinction between online and offline privacy concerns and regulations. For instance, catalog companies and supermarket price clubs have mined data contained in consumer responses to surveys and purchases for years without regulation.[91] What is the difference between mining information through surveys and purchases, and mining for data through online profiling mechanisms? First, some argue that there is a difference between online and offline data collection, because the Internet facilitates the ability to "create a digital trail like nothing we've had so far in history."[92] Online data collection involves the accumulation of incomprehensible volumes of information at amazing speeds. The sheer volume, speed, and flexibility of the gathered and processed data is what distinguishes it from its offline counterpart. Second, the "surveillance of users on the Internet is cheap, and its product (profiles) is extremely valuable."[93] Accordingly, there is more economic incentive to engage in online data profiling and collection, and thus, "what might have been economically justified only for targets of extraordinary investigations is now justified for

87. *Id.* at ¶ 12.

88. PRIVACY ONLINE, *supra* note 70, at 33.

89. Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 396 (2002).

90. Walker, *supra* note 86, ¶ 10.

91. NOCKLEBY, *supra* note 73.

92. Edward C. Baig et al., *Privacy: The Internet Wants Your Personal Info. What's in it for You?*, BUS. WK., Apr. 5, 1999, at 84 (quoting Constance E. Bagley).

93. Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 KAN. L. REV. 641, 673 (2001).

the average Jane."[94] This unprecedented circumstance certainly constitutes a qualitatively and quantitatively different threat to consumer privacy than offline modes of data profiling and data mining, however, it is not completely clear whether offline laws are inadequate to regulate online data gathering activity.

IV. INTERNATIONAL LEGISLATION

A. Proposal for an Alternative Approach

There are many viable arguments for and against instituting comprehensive federal regulation to address online privacy concerns. Even assuming that proponents of the market model are correct in relying on the theory that market pressures will eventually force the market to address consumer privacy concerns, there is empirical evidence that shows that the self-regulation model in its current form is inadequate in the United States. To date, only 175 businesses have voluntarily listed themselves on the Safe Harbor List,[95] and according to the 2000 FTC Report,[96] the majority of those businesses are not in complete compliance with the standards set forth in the Safe Harbor.

Article 25 of the EU Directive, which requires adequate protection before data can be transferred from EU countries to the United States, highlights the necessity of consistency between national laws in this area.[97] The global nature of data transmissions made over the Internet and other digital networks have made privacy interests internationally relevant.[98] The current debate between the EU and United States over data privacy concerns suggests that the solution to the current dilemma is the creation of an international standard for information privacy. Consumers and service providers need a universally consistent standard. It is apparent that the lack of an international consensus on data privacy protection has serious costs and risks. As one scholar pointed out, "the lack of common principles burdens information users, compromises privacy protection for individuals, requires

94. Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 STAN. L. REV. 1193, 1261-63 (1998).

95. Safe Harbor List, *supra* note 59.

96. PRIVACY ONLINE, *supra* note 70, at 12.

97. Council Directive 95/46/EC, *supra* note 5, art. 25.

98. CATE, *supra* note 15, at 126.

greater national bureaucracies to administer national laws in multinational contexts, and threatens the deployment of new and valued services."[99]

Comprehensive legislation such as the EU Directive is not an adequate solution either. Effective international online consumer privacy legislation must take the realities of the Internet into account. As discussed earlier, the laws of economics are at work. Information cheaply and quickly collected on the Internet through online profiling and other online data gathering mechanisms has value, and like any other valuable commodity, will be bought and sold.[100] Furthermore, recognizing the idiosyncratic nature of the Internet is imperative. The decentralized nature of the Internet makes any type of comprehensive legislation very difficult to implement and to enforce;[101] however, effective legislation cannot be completely self-regulatory.

In the domestic forum, it is inevitable that mounting public perceptions of online privacy risks will increase demand for federal regulation. Internationally, it is inevitable that global pressures, spearheaded by the European Community, will continue and may eventually lead to the adoption of some kind of international privacy standard. These concerns illustrate the need for a new international model of online data protection legislation that takes a middle ground approach between consumer concerns and market model concerns. This proposed legislation, based on a consumerist model, balances the consumer interests of privacy and anonymity with the commercial interest in commodifying personal information.[102]

The following sections of this Comment will present some of the principles discussed in the Safe Harbor, and recommend ways in which it can be modified or supplemented to better address global and domestic consumer concerns regarding online privacy. The sections will also explore ways in which the market demands for the commercial accumulation and sale of online data can be simultaneously satisfied. The final section of this Comment will discuss how this proposed paradigm for international data privacy legislation can be effectively implemented and enforced.

---

99. *Id.* at 129.
100. HENDERSON, supra note 4, at 23-24.
101. *Id.* at 37.
102. NOCKLEBY, *supra* note 73.

B. The Consumerist Model Approach

The current Safe Harbor does not weigh consumer privacy concerns heavily enough. Accordingly, effective international online privacy legislation based on the consumerist approach requires the augmentation of five of the seven principles currently included in the Safe Harbor: notice, choice, onward transfer, access, and security.

1. Notice

A survey of over 1,400 web sites contained within the FTC's June 1998 Report to Congress (1998 FTC Report)[103] revealed that efforts to encourage *voluntary* adoption of basic and fair notice practices within the industry are failing. The FTC's survey shows that the vast majority of web sites collect personal information from consumers, yet only 14 percent of those web sites provide any kind of notice to consumers with respect to their information practices, and only two percent of those web sites "provide notice by means of a comprehensive privacy policy".[104] Although some companies back up their privacy statements with Seal Programs, such as TRUSTe or BBBonline (which hold web sites to some kind of baseline standard) the standards are minimal and it is questionable if these programs are truly effective.[105] This is a clear indication that the current Safe Harbor Principles' notice requirement is ineffective.

A consumerist model focuses on providing adequate notice to a consumer when online profiling is occurring. Within the consumerist model, debates take place over what constitutes adequate notice.[106] There are three approaches to notice. One approach is to require organizations to post clear and conspicuous notice regarding their data collection and disclosure practices.[107] A

---

103. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS ii-iii (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

104. *Id.* at iii.

105. Electronic Frontier Foundation, *EFF's Top 12 Ways to Protect Your Online Privacy*, (Apr. 10, 2002), *available at* http://www.eff.org/Privacy/eff_privacy_top_12.html. "TRUSTe" is a non-profit organization that provides monitoring and periodic reviews of over 1600 licensee web sites with regard to privacy; similarly, "BBBonline," a subsidiary of the Council of Better Business Bureaus, also provides monitoring of over 600 participant web sites to ensure compliance. BBBOnline, *at* http://www.bbbonline.com/consumer (last visited Feb. 3, 2004); Kerr & Metzger, supra note 80, at 38.

106. NOCKLEBY, *supra* note 73.

107. Jenab, *supra* note 93, at 673.

second approach is to require notice only after the data has been collected, allowing organizations to collect data without the consumer's knowledge.[108] The third approach is to make the notice requirement very flexible, and provide individual organizations with the choice to decide what kind of notice they want to provide to their consumers based on their underlying policies.[109]

The problem with all three current approaches to notice stems from the fact that there are no existing comprehensive standards, and the policy statements, if any are even provided, are confusing. The 2000 FTC Report noted that many web sites describe their policy in very general terms, then reveal exceptions to the general rule somewhere later in the same statement. This can be extremely misleading to consumers.[110] Web companies know consumers rarely read or understand their so-called privacy policies. These policies are inundated with legalese and impossible for the average consumer to understand.[111] A policy statement is useless and inadequate if it does not actually inform and advise the consumer.

Accordingly, it would make sense to create an international comprehensive notice standard that lays out exactly what must be included in a policy statement. Then organizations will be clear on what is required of them, and consumers have the opportunity to learn about the collection practices of an organization before deciding if they want to provide the organization with their information.

First, a privacy statement should list all information collected by the web site (e.g., purchases, surveys and polls, data collected at registration) and the collection or storage of that that information. If the site collects tracking data, that should also be disclosed.

Next, the policy statement should describe how the collected information is actually used (e.g., to complete a customer's registration, to send the user e-mail notices, to mine purchase preferences of a consumer). If the site supplies this information to third parties, even if the third party is an affiliate or co-brander,

---

108. *Id.*

109. *Id.*

110. PRIVACY ONLINE, *supra* note 70, at 24-25.

111. Paul Eng, *Privacy on the Web: Will New Standards and Laws Help Protect Sensitive User Data?*, ABC NEWS, *at* http://abcnews.go.com/sections/scitech/DailyNews/webprivacy020730.html (July 30, 2003).

the consumer should be notified of that practice and that web site should identify those third parties.

Third, the policy statement should include information on how to contact the organization if the user or consumer has any questions or problems. It should also explain how and to what extent the individual may limit the collection or use of their information. For instance, if the web site uses cookies or web bugs[112] to collect the information, the statement should describe what cookies and web bugs do, and include instructions on how to disable them, if possible.[113]

Finally, if web sites reserve the right to change their policy in the future, they should be required to notify consumers of any material changes in their data collection policy, and should be disallowed from applying new policies to previously collected information. In addition, it should be further mandated that the policy statement be posted somewhere on the web site where it is easily seen and accessible to visitors

2. Choice

Currently, the Safe Harbor requires an organization to give individuals the choice to opt out if their information will be disclosed to third parties (who can then use it for purposes incompatible with those for which it was originally collected); or opt in if their *sensitive* information will be disclosed to third parties.[114] This opt in versus opt out approach has dominated the debate over choice. Under an opt out approach, the collection and circulation of the user's information is acceptable, unless the user affirmatively indicates a rejection of that policy. On the other

---

112. "Web bugs," also known as "invisible gif" or a "1 x 1 gif," is an "image that is added to a web page that is located on a different site to inform the party running the site each time the page is downloaded. Web bugs are frequently used by advertising networks such as DoubleClick to measure the number of times a page containing an advertisement is downloaded." It can also be used to track a user from one site to another by recording the IP address from which the request is received. Phillip Hallam-Baker & Stephen S. Wu, *An Introduction to Privacy Technologies and Techno-Speak, in* PRACITISING LAW INSTITUTE, SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH & CHANGING REGULATORY ENVIRONMENT 89, 106-07 (2001).

113. You can block third-party cookies by using programs like "Cookie Crusher" or by setting your browser to override automatic cookie handling. Daniel Tynan, *How to Take Back Your Privacy*, PC WORLD (June 2002) *at* http://www.pcworld.com/resource/printable/ article/0,aid,92895,00.asp.

114. SAFE HARBOR OVERVIEW, *supra* note 7.

hand, under an opt in approach, companies must obtain a user's permission before collecting and using any personal information from a user. An August 2000 survey revealed that 86 percent of Internet users favored an opt in privacy policy.[115]

Any comprehensive international policy on the issue of choice should apply to both the collection of information and its disclosure (to any third parties). Furthermore, it should prohibit the collection and disclosure of all information unless the entity obtains affirmative consent in advance, which would take form of an opt in approach. The problem with the Safe Harbor's choice standard is that it tries to differentiate between sensitive and non-sensitive data without adequately defining those terms. Similarly, the EU Directive generally prohibits the collection or use of data identifying "racial or ethnic origin, political opinions, religious or philosophical beliefs [and data] concerning health or sex life." The EU directive requires that consumers have an opt in option for the data collection and processing activities applicable to this type of information only.[116] There is no consensus to date as to what constitutes sensitive information since the definition appears to depend on personal preferences.[117]

Rather than applying different standards for different types of information, it would make more sense to require an opt in choice for the collection and disclosure of all information. This seems to reflect the wishes of the majority of consumers.[118] In practical terms, an opt in requirement would mean that web sites would be required to leave permission boxes unchecked. Alternatively, the boxes that prohibit the collection and distribution of personal information should be pre-checked.[119]

The more complex question regarding choice understands the broad definition of the term. Does the right to choice mean that consumers should simply be given a mechanism whereby they may either grant or refuse permission for online profiling activity, and be afforded the opportunity to exit the site before the fact of their

---

115. Dylan Tweney, *The Rules for Writing a Privacy Policy* (Sept. 7, 2000), *at* http://www.ecompany.com/articles/web/0,1653,8297,00.html.

116. Council Directive 95/46/EC, *supra* note 5, art. 8.

117. Walker, *supra* note 86, ¶ 158 (citing CATE, *supra* note 15, at 117-18).

118. Tweney, *supra* note 115 (86% of Internet users favor an "opt in" privacy policy program).

119. An example of this is a check box that says, "No, you may not collect and sell my personal data to any other businesses."

visit becomes a part of their profile? Or does it encompass a broader right, whereby consumers may still obtain the same benefits whether or not they consent or refuse the collection and distribution of data? Self-regulation advocates argue that consumers who object to data collection should not have a "legally guaranteed right to 'free ride' on possible value and corresponding benefits made possible by the cooperation of those who do not object.[120]

The former right appears more in tune with the objective of the choice requirement and is consistent with the protection of public interests. It should be legal to reward users who consent to have their computer usage monitored in exchange for certain benefits. If a vendor wants to offer lower prices in exchange for this information, they should have the right to do so. Supermarket club or loyalty programs have applied the same standard for years. Supermarkets issue cards offering discounts for certain specially priced items exclusively available for their members in exchange for the collection of useful data such as purchasing habits and patterns, without extending those prices to customers who decline to use the card and have their information collected.[121] There is no regulation that prevents supermarkets from sharing the information that they collect with third parties.[122] Choice simply means that consumers should have an opportunity to decide whether they want to be profiled or not. It should not encompass any rights beyond that, and any comprehensive regulation should reflect that notion.

3. Onward Transfer

Onward transfer of data to third parties is the practice of vendors selling or transferring information to third party recipients or buyers.[123] Any comprehensive international legislation will have to ensure that third party recipients or buyers of information also

---

120. Walker, *supra* note 86, ¶ 153 (citing Statement of FTC Commissioner Thomas B. Leary Re: The Federal Trade Commission's May 2000 Report to Congress on Online Privacy Before the United States Senate Committee on Commerce, Science, and Transportation (May 25, 2000), *available at* http://www.ftc.gov/os/2000/07onlineprofiling.htm#LEARY [hereinafter Statement of FTC Commissioner Thomas B. Leary]).

121. *See* NOCKLEBY, *supra* note 73.

122. *See* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 84.

123. *See* SAFE HARBOR OVERVIEW, *supra* note 7.

conform to the same policies on notice and choice as described in the previous sections. There is the potential for abuse when private information is transferred to third parties. For example, when online consumer health site, DrKoop.com, went bankrupt in 2002, the company tried to sell their customer information to a similar type of web site called Vitacost.com.[124] The problem was that nearly one million visitors of DrKoop.com entered their personal and medical histories on the site, believing that such data would remain private.[125] Although the filing of a suit prevented DrKoop.com from selling medical information, this illustrates what could happen if onward transfer policies are too lax.[126]

The Safe Harbor includes a requirement that third party recipients of information apply the notice and choice principles of the Safe Harbor.[127] This requirement, however, becomes somewhat more complex in an international setting. As with Article 25 of the EU Directive, any multinational legislation would have to include a provision that provides that transfers to a third country be dependent on an adequate level of protection of data privacy by that third country. The Safe Harbor notes, however, that "[i]t is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization."[128]

The Safe Harbor sets out reasonable requirements for the onward transfer of data to third party agents. Where an organization wishes to transfer information to a third party that is acting as an agent, vendor, contractor, or consultant, it should be adequate that the third party complies with the standards set forth by the primary party, so long as that information is being used within the intended scope of the transaction.[129] Otherwise, it would be too difficult and costly for vendors to conduct business over the Internet. For example, it would make no sense to require FedEx workers to review and comply with different customer privacy

124. Eng, *supra* note 111.

125. *Id.*

126. In the end, Vitacost.com was only allowed to buy the DrKoop.com web site, its trademark, and the e-mail addresses of former DrKoop.com members. *Id.*

127. *Safe Harbor Principle*, *supra* note 44.

128. *Id.*

129. SAFE HARBOR OVERVIEW, *supra* note 7.

policies for different deliveries depending on the policy of the Internet vendor that took the order.[130]

4. Access

The access requirement in the Safe Harbor clearly states that consumers should have the right to "correct, amend, or delete that information where it is inaccurate."[131] The practical question is how much access is enough. Certainly, the same degree of access is not appropriate for all types of information. For instance, information used as a basis for granting credit or employment is much more important than information gathered for a consumer survey. As the Safe Harbor notes, burden and expense should be important, although not dispositive, factors to be taken into account in considering how much access should be granted.[132] International standards must also take burden and expense into consideration and apply a principle of reasonableness and proportionality. As Commissioner Thomas Leary of the FTC explains, a broad application of the access requirement could in many cases, lead to vast expense for trivial benefit.[133] It would make sense to apply different standards of access depending on the sensitivity of the information collected and the purposes for which it is gathered.

5. Security

There is no way to absolutely guarantee the security of personal information provided by consumers to a web site. There has recently been a string of successful hacks into major commercial and governmental web sites.[134] The reality is that "the Internet is the most surveillance-friendly environment there is," which means that there are ample opportunities for security breaches.[135] In addition to hackings, information leaks and

---

130. *See Safe Harbor Principles*, *supra* note 44.

131. *Id.*

132. SAFE HARBOR OVERVIEW, *supra* note 7.

133. Statement of FTC Commissioner Thomas B. Leary, *supra* note 120.

134. John B. Kennedy & Matthew H. Meade, Privacy Policies and Fair Information Practices: A Look at Current Issues Regarding Online Consumer Privacy and Business Practices, in PRACTISING LAW INSTITUTE, SECOND ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH & CHANGING REGULATORY ENVIRONMENT 321, 341 (2001).

135. Doug Bedell, *Many Find it's Hard to Hide from Trackers in Cyberspace*, SAN DIEGO UNION-TRIB., Dec. 2, 2002, at C-1.

technical glitches are also commonplace.[136] For instance, in November 2002, a glitch on the Victoria's Secret web site allowed people to view details of customer's private purchases and customer's name, address, and size.[137] The order status features on the Victoriassecret.com web site was temporarily shut down while company officials investigated the problem and fixed the glitch.[138]

Consistent with the Safe Harbor, the future international legislation can require organizations to take reasonable precautions to protect personal information from "loss, misuse and unauthorized access, disclosure, alteration and destruction."[139] In the United States, consumers already have the right to sue an organization whose system is hacked by alleging either negligence or the web site's failure to provide adequate security measures. The threat of legal action, coupled with the adverse effects of negative publicity generated by a breach in security, is the real incentive for meaningful security to any organization.[140]

In addition to the requirement of adequate precautions, it would make sense to require organizations to disclose the security procedures that they choose to employ. For instance, many web sites use encryption packages to secure their sites, which require updates on the encryption programs as technology advances. Organizations should be required to disclose what encryption packages they use and to note any material changes in encryption features. This will give consumers an opportunity to decide whether they feel the security measures taken by a web site are adequate before deciding whether they want to consent to the collection of their data.

C. Implementation and Enforcement

The current debate between Europe and the United States regarding the application of the EU Directive illustrates the need for an international standard for information privacy—the challenge is the implementation and enforcement of legislation. The implementation of an international standard is possible,

---

136. *See id.*

137. Bob Sullivan, *Victoria's Secret Customers Exposed: Glitch at Web Site Reveals Who Ordered What in Some Cases*, MSNBC NEWS, *at* http://www.msnbc.com/news/840596.asp?0cv=CB10 (Nov. 27, 2002).

138. *Id.*

139. *Safe Harbor Principles*, *supra* note 44.

140. Walker, *supra* note 86, ¶ 171.

however. As noted earlier, Europe and the United States already share many basic principles underlying information privacy contained within the EU Directive and the Safe Harbor. Where the EU and the United States diverge most sharply is on the role of the government in protecting privacy.[141] As discussed earlier, the EU member states believe that government should oversee the data processing activities of private parties and enforce the law when necessary. The United States, on the other hand, backs a self-regulatory scheme.[142] In light of the apparent failure of the U.S. self-regulation scheme, it is time for the U.S. government to take a more active role in overseeing data processing activities and enforcing privacy laws.

At a minimum, the U.S. government should articulate domestic principles for information privacy. In the end, it should work with other countries towards promulgating basic, multinational principles on privacy and data protection. The creation and implementation of international privacy protection legislation, like the legislation proposed here, will not be easy. [Any such legislation will have to take into account the fact that different countries assign value to privacy in varying ways and how these unique systems will affect the overall market and economy.] In light of the proliferation of computers, networks, the Internet, and the increase in electronic data exchange, it is inevitable that concerns about digital data will eventually lead to the creation of an international standard for privacy protection.

In addition, the failure of the self-regulation model in the United States can be partially attributed to the fact that there are no adequate dispute resolution bodies in place under the Safe Harbor framework to effectively and efficiently resolve problems that arise,[143] and the FTC appears to lack "the statutory authority, the resources, and the reporting requirements that are required to operate effectively on privacy issues."[144] Although the FTC is

---

141. HENDERSON, *supra* note 4, at 130.

142. *Id.*

143. Currently, the Deptartment of Commerce has chosen six organizations to operate as dispute resolution bodies: BBBOnline, TRUSTe, the Direct Marketing Safe Harbour Program, Entertainment Software Rating Board Privacy Online EU Safe Harbour Programme, the Judicial Arbitration and Mediation Service, and the American Arbitration Association. Application of 520/2000/EC, *supra* note 66.

144. Marc Rotenberg, *Consumer Privacy in the E-Commerce Marketplace*, *in* PRACTISING LAW INSTITUTE, SECOND ANNUAL INSTITUTE ON PRIVACY LAW:

under-equipped, it does have resources at its disposal to take action against companies in violation of the Safe Harbor requirements. The FTC's strongest weapon is Section 5 of the Federal Trade Commission Act (FTCA),[145] which protects a consumer's informational privacy when "a company collects or disseminates personal data in an unfair or deceptive manner."[146] For example, in 1998, the FTC brought its first online privacy case against GeoCities[147] for misleading its members on how the company used the information it gathered. In its complaint, the FTC alleged that GeoCities falsely represented that the mandatory information that members provided would not be released to third parties without their consent, when in fact a third party collected and maintained that information.[148] In the end, the FTC was successful in persuading GeoCities to prominently disclose what information it was collecting, for what purpose, to whom it was to be disclosed, and how members could inspect or remove their personal information from the databases of third parties.[149]

Although the FTC was successful in its suit against Geocities, there are simply "too many complaints, too little adjudication, and too little oversight" for the FTC to handle enforcement effectively at this point.[150] In addition, Section 5 of the FTCA simply does not provide the FTC with jurisdiction to enforce the Safe Harbor. By its own terms, Section 5 establishes extensive exceptions to the FTC's authority over unfair or deceptive acts or practices with respect to financial institutions, telecommunications and interstate transportation common carriers, air carriers, packers, and stockyard operators.[151] For instance, in January 2000, DoubleClick, the world's largest provider of Internet-based advertising, was sued in a series of lawsuits that challenged DoubleClick's effort to

---

STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH-TECH & CHANGING REGULATORY ENVIRONMENT 303, 311 (2001).

145. Federal Trade Commission Act, 15 U.S.C. § 45 (2000).

146. Complaint, In the Matter of GeoCities, No. C-3850, 1999 WL 69866 (F.T.C.).

147. Debra A. Valentine, *Privacy on the Internet: The Evolving Legal Landscape,* Remarks Before Santa Clara University (Feb. 11, 2000), *available at* 2000 WL 222524 (F.T.C.).

148. *GeoCities*, 1999 WL 69866.

149. Valentine, *supra* note 147.

150. Rotenberg, *supra* note 144, at 311.

151. U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR OVERVIEW: FEDERAL AND STATE "UNFAIR AND DECEPTIVE PRACTICES" AUTHORITY AND PRIVACY, *at* http://www.export.gov/safeharbor/ENFORCEMENTOVERVIEWFINAL.htm (last visited July 14, 2000).

tie its database of customers' offline purchasing histories with customers' online activities.[152] Although the FTC initially launched an inquiry into DoubleClick's business practices, the FTC eventually closed its investigation, acknowledging that DoubleClick's practices were legitimate under the current lenient privacy law standards.[153] As illustrated here, effectively implementing international privacy legislation requires the FTC to have more authority to execute and enforce the legislation. The FTC must have the ability to send the message that there are real penalties for violating privacy policy agreements, and that the FTC has the power to sanction organizations when they are in violation.

V. CONCLUSION

The policy statement posted on the FTC's web site poignantly summarizes the current dilemma facing the topic of online privacy:

> [A]dvances in computer technology have made it possible for detailed information about people to be compiled and shared more easily and cheaply than ever. That has produced many benefits for society as a whole and individual consumers. . . . At the same time, as personal information becomes more accessible, each of us—companies, associations, government agencies, and consumers—must take precautions to protect against the misuse of our information.[154]

It remains to be seen what kind of precautionary measures the FTC is willing to take in the future to ensure against misuse and abuse of information. It is clear that there is a dire need for comprehensive, multinational legislation that addresses online data privacy concerns. As the FTC has conceded, the U.S. self-regulation model has failed in its current form and the EU places increasing pressure on the U.S. government to get involved in the creation and implementation of a standard that is comparable to the EU Directive. Effective online privacy legislation must address both consumer privacy concerns and market interests in the commercial accumulation and sale of online data. The current U.S. Safe Harbor Principles can meet both of these demands through

---

152. Charles L. Kerr & Oliver Metzger, *Online Privacy: Current Developments in* PRACTISING LAW INSTITUTE, REPRESENTING TECHNOLOGY COMPANIES IN THE NEW BUSINESS ENVIRONMENT 563, 683 (PLI 2001).

153. *Id.*

154. FEDERAL TRADE COMMISSION, PRIVACY INITIATIVES INTRODUCTION (2004), *available at* http://www.ftc.gov/privacy.

modification and supplementation. Recalibration and modification of the principles based on consumerist principles can create a cohesive template for international privacy legislation.

*Joann M. Wakana**

* J.D. Candidate, Loyola Law School, Los Angeles, 2004; B.A. Political Science, University of California at Los Angeles, 2000. I dedicate this Comment to my partents and Jenny for all of their love and encouragement. Thanks especially to Jason for his support throughout law school. Special thanks to Professor John Nockleby for bringing much needed perspective to my Comment and for his invaluable input. Finally, I am grateful to all of the members of the *Loyola of Los Angeles International and Comparative Law Review* for their tireless assistance in preparing this Comment for publication.