Vanderbilt Journal of Transnational Law

Volume 35
Issue 1 *January 2002*

Article 6

2002

The EU Privacy Directive and the Resulting Safe Harbor

Angela Vitale

The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet

ABSTRACT

The rapid growth of the Internet and the importance of international business operations have thrust the issue of Internet privacy into the center of domestic and international political debates. Varying definitions of privacy have led to numerous—often inconsistent—legislative schemes to protect privacy on the Internet. These inconsistencies have made it difficult for companies to penetrate foreign markets and to maintain international operations. Of primary concern to U.S. companies is the EU Privacy Directive. The Directive requires U.S. companies that attempt to interact with potential customers or their own employees in the European Union either to qualify for a "Safe Harbor" or reach an individual compromise with each country from which data will be extracted. Not only do these requirements place additional costs on U.S. companies, they also place U.S. companies at a competitive disadvantage. More ominously, it appears that in the haste of the United States to implement privacy legislation, legislators are mimicking the EU Directive without considering the differences between the U.S. and EU legal systems, the historically different treatment of privacy as a fundamental right in the European Union, or shortfalls in the Directive itself.

TABLE OF CONTENTS

I. INTRODUCTION

The information superhighway has made geographic boundaries virtually obsolete.[1] The free flow of electronic data across borders has contributed to the growth of the "Information Age" and the global economy.[2] Internationally, however, governments have begun to restrict Internet use for various reasons, from political to religious to economic.[3] The protection of privacy on the Internet is one area in which the European Union has been a trendsetter. In an attempt to protect the rights of its citizens, the European Union has passed comprehensive legislation to protect personal data and privacy[4] on the Internet. The United States appears to be following the lead of the European Union.[5]

As of yet the United States has no comprehensive privacy legislation. The current political debates raging in the United States suggest, however, that it is only a matter of time before Congress will pass such legislation.[6] One reason for the heated debates at both the federal and local level is the proactive stance the European Union has taken.[7] The fact that the EU Privacy Directive[8] is far more

---

1. *A Web of Thought Control*, CHI. TRIB., Jan. 13, 2001, at N22.
2. Letter from Susan D. Pinder to David L. Aaron, Undersecretary for International Trade, Department of Commerce (Apr. 5, 2000), *at* http://www.ita.doc.gov/td/ecom/Comments400/NatBusCoalonEcomComments.htm [hereinafter Letter to Aaron].
3. *See id.*; *A Web of Thought Control*, *supra* note 1 (detailing government restrictions on Internet use in countries such as China, Saudi Arabia, and Singapore).
4. Throughout this Note, privacy and data collection refer to consumer information obtained for commercial purposes. Privacy will not be used to refer to the more narrow issues such as health information, information on children, government collection of information, or identity theft.
5. Anna E. Shimanek, Note, *Do You Want Milk With Those Cookies?: Complying With the Safe Harbor Privacy Principles*, 26 IOWA J. CORP. L. 455, 476 (2001).
6. *Id.* at 476-77.
7. Stefani Geraci, *Congressional Hearings Focus on Privacy Issues*, 18 PRIVACY 8 (No. 4, 2001).
8. Council Directive 95/46/EC, 1995 O.J. (L 281) [hereinafter Privacy Directive].

restrictive than any measures taken by the United States has dramatically impacted the U.S. approach to privacy regulation.[9] The Directive prohibits the transfer of information to and from countries not in compliance, and has therefore caused the United States to propose regulation to mirror the legislation of the European Union. Upon first impression, this creates a uniform standard for Internet operation.[10] Although a uniform standard may help to create bright-line rules, it ignores important differences between the EU and U.S. legal systems, their respective treatment of privacy, and the cultures that have developed around the Internet. Furthermore, as this Note argues, uniform standards may lead to unanticipated increased costs for global companies and anti-competitive effects for U.S.-based companies.

In the United States, both sides of the privacy legislation debate have strong arguments. Prior to the EU Directive, the United States took a "sectoral" approach to privacy issues, crafting narrow policy laws that only applied to specific industries or types of information.[11] Because the European Union was the first to craft a privacy policy, the United States was forced to act hastily to ensure that U.S. companies had access to the European market and to their own EU-based subsidiaries or parent companies. During the last six months of 2000, Internet penetration of households in Europe increased fifty-five percent.[12] The pressure to ensure that U.S. companies would not be at a competitive disadvantage in the European market hastened the development of a U.S. plan to comply with the Directive.

The solution to this need for haste was to create the Safe Harbor.[13] The perceived need for haste forced the United States to craft legislation without negotiation or debate. Consequently, the process failed to take into account the differences between the U.S. and EU legal systems and their different treatments of privacy issues. Furthermore, the fear—now justified—was that the Directive would not only keep U.S. companies from accessing European consumers, but would also hamper U.S. companies with European offices from engaging in trans-Atlantic communications.[14] U.S.

---

9. Henry H. Perritt, Jr. & Margaret G. Stewart, *False Alarm?*, 51 FED. COMM. L.J. 811, 814 (1999) (arguing that a multinational corporation "has a strong incentive to pressure the federal government to bring U.S. law into harmony with that of the European Union . . .").

10. *Id.*

11. Ron N. Dreben & Johanna L. Werbach, *Senators Versus Governors: State and Federal Regulation of E-Commerce*, COMPUTER LAW., June 2000, at 3.

12. Steve Gold, *EU Gives Green Light on E-Commerce Legislation*, NEWSBYTES (Dec. 1, 2000), *at* http://www.newsbytes.com/news/00/158859.html.

13. The text and requirements of the Safe Harbor will be the primary focus of the remainder of this Note and will be discussed extensively.

14. U.S. Dept. of Com. Website, *Welcome to the Safe Harbor*, *at* http://www.export.gov/safeharbor.

legislators and companies were and remain primarily concerned with avoiding interruptions in business dealings, protecting U.S. companies from prosecution in the short term, and protecting the estimated $125 billion per year in trade between the United States and the European Union over the long run.[15] U.S. legislators and companies have failed to negotiate with the European Union to formulate a means of compliance that will foster the long-term growth of the Internet.

This Note explores why the Directive and the resulting U.S. Safe Harbor are likely to prove injurious to the growth of the Internet in the United States. This Note argues that the Directive and Safe Harbor will inefficiently regulate a medium that would otherwise develop effective self-regulatory capabilities. The Note first considers the differences between the EU and U.S. treatment of privacy. These differences ultimately require different approaches to regulation.

The history of the Directive and the resulting Safe Harbor is then traced. The Directive and Safe Harbor prove to have profoundly affected the treatment of privacy on the Internet in the United States. Prior to the Directive, the United States relied on self-regulation and market regulation. These types of regulation take time to develop and were in the process of perfecting themselves prior to the EU Directive and the resulting push for government regulation.

Finally, the effects of the Safe Harbor will be considered. Public choice theories of agenda setting and herding support the argument that later U.S. regulations will mirror the Directive and Safe Harbor without considering differences between the United States and European Union or the different expectations of their respective citizens. Furthermore, the Directive, Safe Harbor, the activities of the Federal Trade Commission (FTC), and the resulting legislation will have negative effects on U.S. companies that have neither seriously contemplated their treatment of personal data and privacy, nor are capable of implementing the procedures and processes necessary to satisfy privacy regulation requirements.

II. INTRODUCTION TO THE INTERNET

The Internet is "an appliance of everyday life"[16] and is accessible worldwide.[17] The Internet has changed business and economic

---

15. Stephen Lawson, *Former U.S. Trade Official: Privacy headaches linger* IDG NEWS SERV. (Mar. 27, 2001), *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59023,00.html.

16. The White House Website, *Read the Framework*, *at* http://whitehouse.gov/WH/New/commerce/read.html [hereinafter White House].

17. *Id.*

paradigms.[18] Entrepreneurs and traditional businesses alike see the Internet as a means to improve business and reach the global market. Companies operating on the Internet have invested millions of dollars in an effort to entice customers to use and trust their Internet services.[19] To capitalize on customer use of the Internet, companies began collecting personal information on individuals who visited their websites.[20] Recent advances in technology have made it easier and cheaper to collect, store, retrieve, and organize consumer information.[21] Companies can use this information to target and maintain customers, or can organize this information into customer lists to be sold to third parties.[22] These customer lists have become valuable resources for companies.[23] This information enables web advertisements to target potential customers more efficiently than traditional advertisements.[24] The use of this information, however, has become the subject of regulation; it remains to be seen whether Internet companies will be able to capitalize on their investment.

There are generally three methods used to collect information on the Internet: collection of personally identifiable information, cookies, and click trails. Personally identifiable information is information that can be traced back to an individual user,[25] and refers to data like the user's first and last name, home address, and e-mail address.[26] A cookie is a block of text placed on a user's hard drive by a website when the user visits the website.[27] These files are most commonly placed on hard drives through the use of banner advertisements.[28] These files track the user's online behavior but do not collect information such as name, address, or social security number unless

---

18. *Id.*

19. Henry Welt & Rebecca Wall, *Internet Privacy: Consumer Protection, Economics, or Marketing?*, COMPUTERWORLD (Oct. 17, 2000), *at* http://www.computerworld.com/storyba/0,4125,NAV47_STO52533,00.html.

20. *Id.*

21. *Testimony on Online Privacy Concerns: Before the House Subcomm. on Comm., Trade, and Consumer Protection*, 107th Cong. (2001) (statement of Paul H. Rubin, Professor of Law and Economics, Emory University) [hereinafter Rubin].

22. *See id.* (applying database technologies and statistical models to consumer information to form demographic and interest profiles creates consumer profiles compromising customer lists).

23. Welt & Wall, *supra* note 19.

24. Rubin, *supra* note 21, (noting that "[a] seller does not ask 'What can I sell Paul Rubin?' Rather, a seller asks an advertiser such as DoubleClick or 24/7 to 'Put my ad on 1,000,000 pages viewed on computers of persons more likely than average to want a new car.'").

25. TRUSTe Website, Privacy Glossary, *at* http://www.truste.org/partners/users_glossary.html [hereinafter Privacy Glossary].

26. Jacqueline Klosek, *How the New COPPA Rule Affects Online Data Collection Practices*, N.J. L.J., Nov. 6, 2000.

27. Privacy Glossary, *supra* note 25.

28. Rebecca Lynch, *What's All the Fuss About?*, CIO MAGAZINE, Oct. 1, 2000, *available at* http://www.cio.com/archive/100100/fuss.html.

the user volunteers this personally identifiable information.[29] Only then can the information gathered by a cookie be linked through software to personally identifiable offline data.[30] Cookies notify the website each time the user returns.[31] A click trail is a record of all the websites and pages within a website that a user visits.[32] Like cookies, this information cannot be traced to an individual user, unless the user volunteers personally identifiable information.[33]

III. PRIVACY ON THE INTERNET

Along with the rapid growth of the Internet have come numerous legal issues. One of the more controversial and persistently debated is privacy and the treatment of personal data. This section examines the treatment of privacy by the United States and the European Union and how the different treatment of privacy in general leads to differing views of how to treat privacy on the Internet.

A. *United States Treatment*

"Americans treasure privacy, linking it to our concept of personal freedom and well being."[34] Interestingly, although Americans may value their privacy, a right to privacy does not appear in the Constitution. In addition to this curious anomaly, the issue of Internet privacy creates special problems when considered within the traditional paradigms of privacy protection in U.S. law.[35] These problems are examined below.

Common law affords limited privacy right protections through invasion of privacy torts, including intrusion on an individual's seclusion or solitude, public disclosure of private facts, placing an individual in a false light highly offensive to the reasonable person, and nonconsensual use of a person's identity for private commercial gain.[36]

---

29. *Id.*

30. *Id.*

31. Mark E. Budnitz, *Privacy Protection for Consumer Transaction in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. REV. 847, 852 (1998).

32. Privacy Glossary, *supra* note 25.

33. Lynch, *supra* note 28.

34. White House, *supra* note 16.

35. *See* Owen D. Kurtin & Beth Simone Noveck, *Financial community fixes on online data*, NAT'L L.J., Jan. 24, 2000, at C12; *see generally* Roe v. Wade, 410 U.S. 959 (1973); Griswold v. Connecticut 381 U.S. 479 (1965).

36. Marie Clear, *Falling Into the Gap: The European Union's Data Protection Act and Its Impact on U.S. Law and Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 981, 992 (2000). The first treatment of privacy as a right came from an article written by Samuel Warren and Louis Brandeis. Samuel Warren & Louis Brandeis,

The Supreme Court has, with difficulty, crafted a workable definition of the right to privacy that fits within the framework of the Constitution. The Court interpreted the Bill of Rights, through its penumbras,[37] to include a personal right of privacy.[38] The Court's current definition of the right to privacy provides for an "expectations" test.[39] This right derives from an extension of the Fourth Amendment's right to be free from unreasonable search and seizures,[40] and an extension of the Ninth Amendment's "umbrella" protection.[41]

The Court's expectation test considers whether a person claiming a violation of privacy "has a legitimate expectation of privacy in the invaded place."[42] The Court has created a two-pronged test to analyze alleged constitutional invasions of privacy.[43] The claimant must first have "manifested a subjective expectation of privacy."[44] The subjective expectation must then be deemed "one that society accepts as 'objectively reasonable.'"[45]

The problem with the expectation analysis in the context of the Internet is that as soon as a person voluntarily discloses information to a third party, the "expectation of privacy" disappears, unless the website assures the user that privacy will be protected.[46] Anytime an individual provides personal information, either in completing an online survey or ordering goods online, they have voluntarily provided personal information and cannot rely on an "expectation of privacy."[47]

The Right to Privacy, 4 HARV. L. REV. 193 (1890). William L. Prosser then defined the right in terms of four causes of action. *See* IAN C. BALLON & KEITH M. KUPFERSCHMIND, INTELLECTUAL PROPERTY OPPORTUNITIES AND PITFALLS IN THE CONDUCT OF ELECTRONIC COMMERCE: PRACTICING LAW INSTITUTE, PATENTS, COPYRIGHTS, TRADEMARKS AND LITERARY PROPERTY COURSE HANDBOOK SERIES 563 n.78 (1999).

37. The Supreme Court first interpreted the Bill of Rights to include certain penumbral rights in *Griswold v. Connecticut*, 381 U.S. 479 (1965).

38. Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L. REV. 661, 668 (1999).

39. Clear, *supra* note 36, at 994.

40. *Id.* at 1018 n.72.

41. *See, e.g., Griswold*, 381 U.S. at 479.

42. U.S. v. Hambrick, 55 F. Supp. 2d 504, 506 (1999) (citing Katz v. U.S., 389 U.S. 347 (1967)).

43. Clear, *supra* note 36, at 996.

44. *Hambrick*, 55 F. Supp. 2d at 506 (citing California v. Greenwood, 486 U.S. 35, 39 (1988)).

45. *Id.*

46. Clear, *supra* note 36, at 995.

47. Tan, *supra* note 38, at 670. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Id.* (quoting *Katz*, 389 U.S. at 351-52). Individuals who send e-mail through the Internet, however, do retain an "expectation of privacy." Clear, *supra* note 36, at 995.

Several other paradigms of analysis—such as treating Internet privacy and personal data as an intellectual property right or a contractual right—have been suggested. These paradigms have serious flaws as models for privacy regulation.

Some scholars advocate treating personal data as an intellectual property right.[48] Intellectual property law is designed to create private control over publicly used commercial information.[49] Treating personal data as an intellectual property right, however, creates First Amendment problems.[50] Courts have recognized that the level of protection afforded "commercial speech" should extend to the sale of personal data to third parties.[51] The First Amendment protects commercial speech from unwarranted governmental regulation but accords a lower level of protection to commercial speech than to other forms of constitutionally guaranteed expression.[52] Commercial speech can be regulated only if the state has a substantial interest in regulating such speech and the challenged regulation is the least restrictive means to achieve the substantial state interest.[53] Without evidence of abuse of personal data, it is uncertain whether the state would have a substantial interest in protecting personal data. Furthermore, any regulation adopted by the state will inevitably be more restrictive than self-regulation and therefore not the least restrictive means. It is further unclear who deserves the protection, the consumers from whom the personal data is obtained or the websites that collect the data. If it is determined that consumers deserve protection, courts may be reluctant to find an intellectual property right absent a cost effective way to acquire authorization.[54] It will be difficult to overcome the fact that such transaction costs will likely be very high and will arguably not be the least restrictive.[55]

For the websites that do provide users with privacy policies, some scholars advocate treating privacy as a contractual right.[56] If gathered information is used inconsistently with the privacy policy, it

---

48. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041-42 (2000).

49. Rochell Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8, 11.

50. *Id.* at 33.

51. *Id.* ¶5 n.4.

52. Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 761-62 (1976) (reasoning that "if there is a kind of commercial speech that lacks all First Amendment protection, therefore, it must be distinguished by its content. Yet the speech whose content deprives it of protection cannot simply be speech on a commercial subject.").

53. *Id.* at 755-56.

54. Dreyfuss, *supra* note 49, at 36.

55. *Id.* (arguing that "it is difficult to think of effective ways for potential users to negotiate with rights holders").

56. Kurtin & Noveck, *supra* note 35.

would be considered a breach of contract by the website.[57] This treatment has several problems. In treating privacy as a contractual agreement between the website and the user, a breach by the website imposes costs upon the user.[58] To enforce a contractual right, the user may be required to obtain the services of a lawyer.[59] The harm suffered by the individual user may not be sufficient for the consumer to litigate the issue.[60] Furthermore, this analysis only works for those websites that choose to post privacy policies. If a website does not post a privacy policy, there is no contractual relationship. Furthermore, some websites explicitly state that the policy is not a contract, and consequently a contractual argument will not work with such a website.[61]

B. *European Union Treatment*

In Europe, privacy is considered a "fundamental human right."[62] The European Union makes data privacy protection the "right of the individual."[63] Furthermore, in the European Union, the treatment of personal data is clearly defined in the "mass of acts, directives, amendments, and the like that are currently being developed."[64] Data protection laws are commonplace in Europe, and many European countries have had data protection laws in place for the last two decades, long before any comprehensive action by the European Union.[65] In many European countries the state takes an active role in protecting the personal information of its citizens through legislation.[66] These laws generally address data collection, storage, use, and disclosure.[67] Commonly, a single piece of legislation governs both the private and public sectors; other laws addressing "narrow fields of processing activity" supplement the legislation.[68]

---

57. *See id.*

58. Budnitz, *supra* note 31, at 876.

59. *Id.*

60. *Id.* (noting that "[c]ontracts will provide a right, but no meaningful remedy").

61. *See, e.g.*, Privacy Statement, *at* http://www.weather.com/common/home/privacy.html. "This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights." *Id.*

62. Jon Baumgarten et al., Washington Watch, *SEC Proposes Automated Internet Surveillance*, 5 CYBER. LAW. 19 (2000).

63. Patrick Thibodeau, *'Safe Harbor' Deal Doesn't Fully Bridge Data Privacy Divide*, COMPUTERWORLD, Sept. 13, 2000, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO50149,00.html.

64. Clear, *supra* note 36, at 993.

65. *Id.* at 1013. For example, the German Data Privacy Act required companies to provide listings of third parties that receive an individual's personal information. *Id.* at 1014.

66. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 12 (1996).

67. *Id.* at 13.

68. *Id.*

Prior to the Directive, there was general agreement among EU Member States as to what constituted fair treatment of personal data.[69] This agreement focused on four elements: (1) establishment of obligations and responsibilities for personal information; (2) maintenance of transparent processing of personal information; (3) creation of special protection for sensitive data; and (4) establishment of enforcement rights and effective oversight for the treatment of personal information.[70] These elements provided a comprehensive approach that served as a backdrop for the Directive.[71] This background of agreement permitted the European Union to act more rapidly to design comprehensive privacy legislation. Arguably, this also forced the hand of U.S. lawmakers as well.

IV. EUROPEAN UNION DATA PROTECTION DIRECTIVE

To understand the EU Data Protection Directive, it is important to understand the make-up of the European Union. The European Union consists of a "complex weave" of organizations, including various associations, commissions, committees, and councils.[72] The three primary bodies are the European Commission, the European Council of Ministers, and the European Court of Justice.[73] The European Commission recommends policy to the European Council of Ministers, which enacts policy.[74] Enacted policies preempt any Member State laws that are inconsistent or interfere with the EU legislation.[75] If there is an alleged violation of an EU law, the European Court of Justice interprets and applies the law.[76]

The Data Protection Directive was meant both to standardize rules among participating EU Member States and to strengthen technology protections.[77] The EU Council of Ministers formally adopted the Directive on October 24, 1995, and each Member State had until October 24, 1998 to amend existing state laws to comply with the Directive.[78] The Directive was designed to enable individuals to control the dissemination of their personal information.[79] "The Directive applies to personal data processed wholly or partly by automatic systems," and to manual data held in

---

69. *Id.*
70. *Id.*
71. *Id.*
72. Clear, *supra* note 36, at 982.
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.* at 983.
77. *Id.*
78. Tan, *supra* note 38, at 676.
79. Clear, *supra* note 36, at 985.

filing systems that are organized by reference to individuals.[80]

The Directive requires all EU Member States to implement the following personal data policies: (1) personal data must be processed fairly and lawfully;[81] (2) data must be collected and possessed for specified and legitimate purposes and cannot be used in a manner inconsistent with those purposes;[82] (3) data must be adequate, relevant, and not excessive for the purposes for which it is collected;[83] (4) data must be accurate and kept up to date;[84] and (5) data must not be kept any longer than is necessary to achieve the purpose for which it was collected.[85]

The Directive mandates the following data requirements be satisfied before information can be processed: (1) the data subject must have clearly given his or her consent;[86] (2) the processing of the data must be necessary to complete a contract to which the data subject is a party or is a necessary step for entering a contract which the data subject is requesting;[87] (3) the processing of the data is necessary to satisfy a legal obligation;[88] (4) the processing is necessary to protect the vital interests of a data subject;[89] or (5) the "[p]rocessing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection."[90]

Article 8 regulates the processing of certain categories of data.[91]

---

80. Dreben & Werbach, *supra* note 11. Personal data is any information relating to an identified or identifiable natural person. *See id.* Also, subject to some exceptions, the Directive forbids the processing of information about racial or ethnic origin, political affiliation, religious faith, union membership, health status, or sexual orientation. *See id.*

81. Council Directive 95/46, art. 6(a); *see also* Tan, *supra* note 38, at 677.

82. Council Directive 95/46, art. 6(b); *see also* John D. Woodward, Jr. & Gary Roethenbaugh, *Fact Sheet on the European Union Privacy Directive, at* http://www.dss.state.ct.us/digital/eupriv.html.

83. Council Directive 95/46, art. 6(c).

84. *Id.* art. 6(d). Every effort must be taken to ensure that data that is inaccurate is destroyed or erased. *Id.*

85. *Id.* art. 6(e).

86. *Id.* art. 7(a).

87. *Id.* art. 7(b).

88. *Id.* art. 7(c).

89. *Id.* art. 7(d).

90. *Id.* art. 7(e).

91. The Directive states, in part:

> 1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
>
> 2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Id. art. 8.

Article 10 specifies the information that the data subject is to be given when personal information is gathered.[92] Article 12 ensures that data subjects have a right to access the data collected.[93] The Directive then provides that those gathering data must ensure its confidentiality and security and provide the necessary procedures to take if a breach of confidentiality or security occurs.[94] Articles 22 through 24 specify remedies provided to individuals when there is an infringement of an individual's right to privacy.[95] Articles 25 and 26

---

92. The Directive states, in part:

> Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
>
> (a) the identity of the controller and of his representative, if any;
>
> (b) the purposes of the processing for which the data are intended;
>
> (c) any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Id. art. 10.

93. The Directive states, in part:

> Member States shall guarantee every data subject the right to obtain from the controller:
>
> (a) without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);
>
> (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
>
> (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Id. art. 12.

94. *See id.* arts. 14-21.

95. The Directive states, in part:

> Article 22 Remedies
>
> Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior

are of special significance to U.S. companies, because they prohibit the transfer of data to countries the European Union does not consider to be secure.[96] Article 25 allows transfer to non-Member

---

to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23 Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

Id. arts. 22-24.

96. The Directive states, in part:

Article 25 Principles

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

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 or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2. If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2). Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer

States only if that country ensures an "adequate level of protection."[97] The definition of "adequate" is flexible and looks to the laws in force in the non-member country.[98]

In addition to the Directive, the European Union has launched the eEurope Initiative on Brussels Regulation, which outlines procedures for cross-border disputes.[99] The initiative provides that European consumers may sue non-EU businesses in their own national courts.[100]

V. THE SAFE HARBOR

On November 1, 2000 the Safe Harbor agreement went into effect in response to the Data Protection Directive.[101] Designed to ensure a means of compliance for U.S. companies, the Safe Harbor was the culmination of two years of intense negotiation between the European Union and the Unites States.[102]

From the time of its passage, U.S. companies were concerned with the possible ramifications of the Privacy Directive, particularly with Article 25 of the Directive.[103] Until they could guarantee an adequate level of protection to European citizens, U.S. companies could not receive credit card information or other types of data, including employee information, from European Union citizens.[104]

Historically, the United States has taken a different approach from the European Union to provide privacy protection.[105] As noted in Part III.A, the United States used a combination of legislation, regulation, and self-regulation to regulate privacy. Keeping within

---

sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

Id. arts. 25-26.

97. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 32 (1998).

98. *See id.*

99. Gold, *supra* note 12.

100. *Id.*

101. Electronic Privacy Information Center, *EPIC Alert*, vol. 7.20, § 6 (Nov. 14, 2000), *at* http://www.epic.org/alert/EPIC_Alert_7.20.html [hereinafter *EPIC Alert* 7.20].

102. *Id.*; FRIED, FRANK, HARRIS, SHRIVER & JACOBSEN, *Data Protection v. Privacy: United States and EU Come to Terms on a Safe Harbor*, 21st Century Money, Banking & Commerce Alert No. 2000-04-20 (Apr. 20, 2000), *reprinted in* 5 CYBER L. 14 (2000).

103. Julie M. Fromholz, Berkeley Technology Journal Annual Review of Law and Technology, Foreign & International Law, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 469 (2000).

104. Clear, *supra* note 36, at 988-89.

105. *See generally* U.S. DEPT. OF COM., SAFE HARBOR PRIVACY PRINCIPLES (2000), *at* http://www.export.gov/safeharbor [hereinafter SAFE HARBOR].

this framework, the U.S. Department of Commerce crafted the Safe Harbor agreement to provide a level of protection to Europeans sufficient to permit U.S. companies to transfer data between individuals within EU Member States and the United States.[106] This requires that the U.S. privacy policy must be deemed adequate upon consideration of "all the circumstances surrounding a data transfer operation"[107] and the legislative provisions, both general and sectoral, in force.[108] In crafting such a standard, the Safe Harbor was designed to provide adequate protection, while maintaining a certain amount of flexibility to prevent the Safe Harbor from being overly cumbersome or costly.[109]

Under the Safe Harbor, a company receiving personal data from the European Union must abide by the following seven criteria: notice,[110] choice,[111] onward transfer,[112] security,[113] data integrity,[114]

---

106. *Id.*

107. Deborah M. McTigue, *Marginalizing Individual Privacy on the Internet*, 5 B.U. J. SCI. & TECH. L. 5, ¶ 40 (1999) (quoting Ian Lloyd, *An Outline of the European Data Protection Directive*, J. INFO. L. & TECH., Jan. 31, 1996, *at* http://www.elj.warwick.ac.uk/elj/jilt/dp/intros/default.htm).

108. *Id.*

109. *See id.* ¶ 41. Those companies that cannot comply with the Safe Harbor may do business in those EU Member States with which the company has entered a special contract permitting the export of personal data from that country to the company's country. Lawson, *supra* note 12. These contracts must generally be negotiated country by country and may take as long as two months to reach an agreement. *Id.*

110.

> NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

SAFE HARBOR, *supra* note 102.

111.

> CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.
>
> For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other

access,[115] and enforcement.[116] These criteria are based largely upon

---

than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

Id.

112.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have know the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

Id.

113.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Id.

114.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Id.

115.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Id.

116.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such

the Fair Information Practices principles developed by the FTC over the past three decades.[117]

Adherence to the Safe Harbor agreement is completely voluntary[118] and compliance can be achieved in a number of ways.[119] First, a company may implement all the restrictions of the Safe Harbor, notify the Department of Commerce that the company intends to comply with the Safe Harbor, and publicly declare compliance on its website.[120] A second route to compliance requires a company to develop its own self-regulatory policies, notify the Department of Commerce, and publicly declare its compliance.[121] This method of compliance may be achieved through complying with a safety seal program that notifies the Department of Commerce of the company's participation and ensures compliance.[122]

The U.S. Department of Commerce maintains the official list of U.S. companies that have agreed to abide by the Safe Harbor agreement.[123] If a website were to state that it complied with the Safe Harbor and then act contrary to the stated policy, the FTC has the power to challenge the practice.[124] This authority derives from Section 5 of the Federal Trade Commission Act, which prohibits

---

> mechanisms must include: (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by references to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Id.

117. *Prepared Testimony and Statement for the Record: Hearing on S. 809 Online Privacy Protection Act of 1999, S. 2606 Consumer Privacy Protection Act of 2000, and S. 2928 Consumer Internet Privacy Enhancement Act of 2000: Before the Senate Com. Comm.*, 106th Cong. (2000) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center) (explaining how Fair Information Practices resulted from the Fair Credit Reporting Act of 1970 which placed requirements on credit reporting agencies), *at* http://www.epic.org/privacy/internet/testimony_1000.html [hereinafter Rotenberg Testimony].

118. SAFE HARBOR, *supra* note 105.

119. *Id.*

120. *Id.*; *see also* FRIED, FRANK ET AL., *supra* note 102.

121. *See* FRIED, FRANK ET AL., *supra* note 102.

122. *TRUSTe Unveils European Safe Harbor Privacy Seal Program: World's Largest Privacy Certification Program Makes Landmark Move to Provide Global Online and Offline Dispute Resolution*, PR NEWSWIRE, Nov. 1, 2000, *at* http://www.truste.org/about/about_eu.html [hereinafter Privacy Seal Program].

123. *EPIC Alert* 7.20, *supra* note 101.

124. Letter from Robert Pitofsky to John Mogg, Director, European Commission 2 (July 14, 2000) (on file with author) [hereinafter Letter to Mogg].

"unfair or deceptive acts or practices" in or affecting commerce.[125] The FTC Act authorizes the FTC to obtain injunctive relief against future violations and to compensate injured consumers.[126] The FTC can seek redress for both U.S. and foreign citizens.[127] Anyone who does not comply with an injunctive order is subject to a civil penalty of up to eleven thousand dollars, with each day of violation constituting a separate violation.[128]

Currently the authority of the FTC is somewhat limited.[129] The FTC can only prosecute companies that misrepresent their purpose for collecting information. This provides companies with a loophole, because if they do not provide a privacy policy there is no misrepresentation.[130] Furthermore, the ability of the FTC to regulate in this area only covers unfair or deceptive practices if they are "in or affecting commerce,"[131] so information being traded without commercial purposes remains outside the power of the FTC.[132]

The FTC pursues law enforcement actions through active investigation and monitoring, and also through referrals received from regulatory agencies such as TRUSTe and BBBOnline.[133] TRUSTe, the Internet's leading privacy seal program, has launched an EU Safe Harbor Privacy Program.[134] By joining the TRUSTe program, U.S. companies fulfill the Safe Harbor requirements to self-certify to the Department of Commerce that they have complied.[135] U.S. companies can choose either to create their own program to satisfy the Safe Harbor or can choose to satisfy the criteria of TRUSTe. BBBOnline acts in the same way as TRUSTe.[136]

---

125. *Id.* A deceptive practice is a representation, omission, or practice that is likely to mislead reasonable consumers in a material fashion. A practice is unfair if it causes, or is likely to cause, substantial injury to consumers that is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n) (2001).

126. *Id.*

127. *Id.*

128. U.S. DEPT. OF COM., SAFE HARBOR ENFORCEMENT OVERVIEW: FEDERAL AND STATE "UNFAIR AND DECEPTIVE PRACTICES" AUTHORITY AND PRIVACY (July 14, 2000), *at* http://www.export.gov/safeharbor/enforcementoverviewfinal.htm.

129. *See* Letter to Mogg, supra note 124, at 6.

130. *See id.*

131. *Id.* at 7.

132. *See id.*

133. *Id.* at 2.

134. Privacy Seal Program, *supra* note 122.

135. *Id.*

136. BBBONLINE, Inc., *at* http://www.bbbonline.com (businesses can apply for reliability and privacy seals).

VI. EFFECTS OF THE SAFE HARBOR

The Safe Harbor was entered into to protect the interests of U.S. companies in transactions with EU Member States. This section analyzes whether that short-term goal was met and considers other unanticipated effects of the Safe Harbor.

A. *Effects on U.S. Privacy Policy*

While the Safe Harbor has permitted trans-Atlantic transactions between the United States and the European Union to continue, the Safe Harbor has also dramatically impacted the privacy policy debate in the United States. This section analyzes how the Safe Harbor legislation has had both herding and agenda setting effects on the U.S. privacy policy debate.

1. Herding

Herding is a culture-based theory.[137] The theory suggests that actors may rationally decide to follow the actions of others because they assume that previous actors had more information when they made their decision. Therefore, copying the previous decision is perceived to be the most efficient way to act.[138] Applying this reasoning to privacy, U.S. privacy law is likely to be similar to the Safe Harbor because the Safe Harbor is all that presently exists.[139]

There is evidence of this in Senate bill S. 2928, the "Consumer Internet Privacy Enhancement Act,"[140] House bill H.R. 89, the "Online

---

137. Eric Talley, *Precedential Cascades: An Appraisal*, 73 S. CAL. L. REV. 87, 90-92 (1999).

138. *Id. See also* Charles Sipos, Note, *Gun Control from Public to Private*, 55 VAND. L. REV. (forthcoming Apr. 2002).

139. Congress has taken a small step towards privacy legislation in its passage of the Children's Online Privacy Protection Act ("COPPA"), which only protects the privacy of children under the age of 13. 15 U.S.C. §§ 6501-06 (2001). COPPA requires: (1) posting prominent links providing how they collect, use, and disclose information collected about children; (2) notifying parents they wish to collect information and obtaining parental consent; (3) not limiting a child's participation on a website to the provision of information more than is reasonably necessary; (4) allowing parents to view children's information, have it deleted, and prohibit future collection; and (5) establishing procedures to protect the information collected from children. *Id.*; *see also* Orrin S. Shifrin & Lisa K. Liou, *COPPA: A Practical Guide to Compliance with the Children's Online Privacy Protection Act*, 5 CYBER L. 11 (2000). Although this preceded the Safe Harbor, it garnered its support from the fact that it protected children, not in its broad attempt to regulate privacy, as does the Safe Harbor.

140. Consumer Internet Privacy Enhancement Act, S. 2928, 106th Cong. (2000).

Privacy Protection Act of 2001,"[141] and Senate bill S. 2606, the "Consumer Privacy Protection Act."[142] The language within the proposed legislation reflects the objectives of the Safe Harbor and the EU Directive.[143] For instance, the "Consumer Internet Privacy Enhancement Act" makes it unlawful for a commercial website operator to collect personally identifiable information unless certain conditions are satisfied.[144] The website must provide the user with notice that includes: identification of the website operator, a list of the type of information that might be collected, how the information will be used, a list of possible recipients of the information, the steps being taken to protect the security of the information, and the steps users may take to stop use of their information by the website.[145] These requirements reflect the influence of the Safe Harbor and the FTC's Fair Information Practice principles.

Section 2(d) of the Consumer Internet Privacy Enhancement Act—entitled "Safe Harbor"—is indicative of the influence the Safe Harbor has had on subsequent legislation.[146] The Section provides that a commercial website operator does not violate the Act if it complies with the self-regulatory guidelines of seal programs or representatives of the marketing or online industries.[147] As explained in Part V, the seal programs have adopted the regulatory schemes necessary to ensure compliance with the Safe Harbor to satisfy the Directive.[148] If a company satisfies the Safe Harbor, it automatically complies with the Act. The Act has therefore done little more than adopt the Directive's Safe Harbor as its own.

The herding effect can also be seen in the role the FTC plays in protecting Internet privacy. Prior to the EU Directive, the FTC advocated Internet self-regulation.[149] The Safe Harbor provided the FTC with an opportunity to increase its governing role and, perhaps as a result, the FTC appears to have changed its position towards Internet self-regulation. Apparently, the FTC concluded that

---

141. Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001).

142. Consumer Privacy Protection Act, S. 2606, 106th Cong. (2000).

143. *Id.*

144. S. 2928 106th Cong. §2(a), (2000). It is irrelevant for the purposes of this Note which bill, or version of any of the above bills, is actually passed. What is important for the purposes of this Note is that all three bills reflect the influences of the Directive and the Safe Harbor.

145. *Id.* § 2(b)(1)(A)-(G).

146. *See id.* § 2(d).

147. *Id.*

148. *See* http://www.truste.com/programs/pub_harbor.html; http://www.bbbonline.com/privacy/eu.asp.

149. *Hearing on Privacy in the Commercial World: Before the House Subcomm. on Com., Trade, and Consumer Protection and the House Comm. on Energy and Com.*, 107th Cong. (2001) (testimony and statement for the record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center) [hereinafter Second Rotenberg Testimony].

regulation was necessary because it realized that if the Safe Harbor were mimicked in legislation, the FTC would be incorporated into any new legislation,[150] because of its reliance on Section 5 of the Federal Trade Commission Act, which declares "unfair or deceptive acts or practices in or affecting commerce" to be illegal.[151] Furthermore, the Safe Harbor incorporates the FTC's Fair Information Practice Principles (FIPPs) and these FIPPs can be seen in resulting legislation.[152] For instance, the "Online Privacy Protection Act of 2001" requires the FTC to prescribe regulations to protect consumer privacy on the Internet.[153]

Due in part to the attention given to the issue of Internet privacy protection, it is now politically popular to advocate protecting privacy.[154] Legislators have warned, "if the private sector won't ensure consumers their privacy is protected on-line, then the federal government will step in and try."[155] The Directive and the resulting Safe Harbor give legislators the ability to make their threats a reality, and quickly.[156] They already have statutory language which they can "cut and paste" without much debate and without thoughtful consideration.

Events such as the bankruptcy of the web-based company Toysmart exacerbate the herding effect and encourage Congress to enact "cut and paste" legislation. After filing for bankruptcy, Toysmart sought to sell its consumer information list in violation of its own privacy policy.[157] The FTC reached a settlement with

---

150. *See id.* (noting that it was not until the year 2000 that the FTC concluded that regulation was required).

151. 15 U.S.C. § 45(a)(1) (2001).

152. Rotenberg Testimony, *supra* note 117 (stating that these FIPPs incorporated the responsibilities of the organization that collect personal information and the of those individuals that provide information).

153. H.R. 89, 107th Cong. (2001). There is a public choice argument that the FTC has acted to create a role for itself in regulating privacy on the Internet. Steven Hetcher, *The Emergence of Website Privacy Norms*, (Sept. 5, 2000) (unpublished manuscript, on file with author).

154. David McGuire, *Net Privacy Law Could Pass, Despite Congressional Rancor*, NEWSBYTES, Dec. 5, 2000 (quoting Andrew Shen, policy analyst for the Electronic Privacy Information Center, who stated that "privacy as an issue is much more bipartisan . . ."), *at* 2000 WL 27303518.

155. Tan, *supra* note 35, at 675.

156. Other countries have begun implementing privacy policies. This strengthens the argument of U.S. legislators who support a privacy policy when they allege that the United States provides inadequate privacy protection relative to other countries. For instance, on January 1, 2001 the Canadian Personal Information Protection and Electronic Documents Act became effective. Electronic Privacy Information Center, *EPIC Alert*, vol. 8.01, § 4 (Jan. 17, 2001), *at* http://www.epic.org/alert/EPIC_Alert_8.01.html. [hereinafter *EPIC Alert* 8.01]. The Canadian law establishes Fair Information Practice for personal data collected by private sector organizations. *Id.* The Act is enforced by the Office of the Privacy Commissioner of Canada. *Id.*

157. *Id.*

Toysmart, which eventually led to the sale of the list to Walt Disney—a majority owner of Toysmart—conditioned on a promise that Disney would keep the list confidential.[158] Nevertheless, the incident provides an example of the threat of abuse from which the Directive protects European consumers. It also provides an example of what U.S. consumers may expect companies to do upon bankruptcy, if personal data is not protected.[159]

2. Agenda Setting

Agenda setting is a public choice theory that states that the order in which alternative proposals are considered will influence the solution that is actually adopted.[160] Prior to the Safe Harbor, there were arguments for and against Internet privacy protection that fell everywhere along the political spectrum. Some urged absolutely no protection for personal data; others believed personal data should be treated as intellectual property. The Safe Harbor essentially determined how these preferences would be presented before Congress and the public.[161] After the Safe Harbor, any proposal that offers less protection to consumers than that offered by the Safe Harbor is likely to be dismissed. Yet, prior to the Safe Harbor, the leading argument was for self-regulation of Internet privacy.[162] The Safe Harbor essentially destroyed the self-regulation argument, and the "agenda" for policy legislation is currently based on various combinations of Safe Harbor and FTC language, which can be employed by the government to draft privacy protection legislation.[163]

The enactment of the Safe Harbor enabled those advocating legislative action for privacy protection to ask the politically powerful question, "Why are Europeans getting better privacy protection than Americans are?"[164] Because Europeans are already being protected under the Safe Harbor and the Directive, any legislation that provides less protection to Americans will be unacceptable. Due to

---

158. *Id.*

159. *Id.*

160. *See generally* Michael E. Levine & Charles R. Plott, *Agenda Influence and Its Implications*, 63 VA. L. REV. 561, 564-65 (1977) (discussing two ways in which agenda influences outcomes).

161. *See* Daniel A. Farber & Philip P. Frickey, *Legislative Intent and Public Choice*, 74 VA. L. REV. 423, 427 (1988).

162. *DMA Testifies on Privacy and Self-Regulation*, 62 DIRECT MARKETING ASS'N 8 (Sept. 1, 1999).

163. James Evans, *High-Tech Trade Group Unveils Net Privacy Principles*, IDG NEWS SERVICE, (Jan. 18, 2001), *at* http://www.idg.net/ec?go=1&content_source_id=13&link_id=400563 (noting that high-tech trade organizations which once lobbied for Internet self-regulation are now lobbying for federal legislation so as to avoid conflicting privacy rule from the 50 state governments).

164. Keith Perine, *Not Enough Privacy?*, INDUS. STANDARD, July 10, 2000 (quoting privacy advocate Jason Catlett).

the Safe Harbor, those who once advocated self-regulation have been forced to change their position and use their resources to attempt legislation beneficial to the various organized industries operating on the Internet.[165] The Safe Harbor has, in essence, served as a substantial victory for those advocating regulation and has changed the focus of the debate.[166] Even though there is objective evidence that self-regulation was working, the change in focus has made such evidence moot.[167] The Safe Harbor has set a minimum standard by which all future privacy legislation is judged.

In practice, the Safe Harbor creates a positional conflict for U.S. companies opposed to such regulation.[168] To access the European market, companies must sign up for the Safe Harbor and, at the same time, try to argue that the laws are too cumbersome to implement in the United States.[169] Furthermore, those companies that do not sign up for the Safe Harbor and do not provide a policy are beyond the scope of FTC power. Under the Safe Harbor, the FTC possesses only limited power and cannot require that entities collecting information on the Internet adhere to a privacy policy.[170] This discrepancy has led the FTC to call for comprehensive privacy legislation.[171]

The debate now occurs between those who want strict privacy legislation, much like the EU Directive, and those who advocate achieving a balance between the interests of consumers and the "legitimate interest of business in operating efficiently and in using information to improve the quality, variety and cost-effectiveness of products and services."[172] With the Directive and the Safe Harbor

---

165. The AeA, the nation's largest high-tech trade association, released principles in an attempt to guide legislators in drafting privacy legislation. Marc Brailor, *AeA Unveils Federal Privacy Principles; Says Balanced Approach, Uniform Standards, Can Build Consumer Confidence, Boost Internet Growth*, *at* http://www.aeanet.org/pressroom/pret-privacyprinciples011801.asp. The principles were released in response to the attempts of state governments to regulate online privacy and to help legislators identify the technical and economic realities of the Internet. *Id.*

166. Businesses appear to have realized that some form of regulation is inevitable and have shifted lobbying efforts to promoting uniform regulation as opposed to a patchwork quilt of state regulation. Edmund Sanders, *Politicians, Industry Gear Up for Public Battle Over Privacy*, L.A. TIMES, Jan. 22, 2001, at C1. Two dozen states in 2000 tried to strengthen their privacy laws, but businesses were able to lobby successfully on the local level to prevent such legislation. *See id.*

167. *See* Rubin, *supra* note 21 (arguing that the ability of consumers to quit engaging with websites that may abuse consumer information is a powerful incentive for websites to respect the privacy rights of consumers, and evidence shows that when a company does something that is seen as harming its reputation with consumers, the company suffers a substantial loss in value).

168. *Id.*

169. *Id.*

170. Letter to Mogg, *supra* note 124, at 6.

171. *Id.*

172. Letter to Aaron, *supra* note 2.

available, those advocating more restrictive regulations have an agenda setting advantage. For instance, Senate bill S. 2928, the "Consumer Internet Privacy Enhancement Act," requires every website to satisfy four basic standards: notice, choice, access, and security.[173] There are a number of bills with variations on these principles, reflecting the influence of the Safe Harbor and the FTC.[174] There is likely to be little protest as the bill is currently drawing bipartisan support.[175] Instead, the debate will focus on the variations in the level of protection. The Safe Harbor, rather than self-regulation, will act as a minimum standard.

B. *Anti-Competitive Effects*

Although the Safe Harbor enables U.S. companies to continue to engage in trans-Atlantic transactions with the European Union, in the long-run the Safe Harbor may have a negative impact on U.S. companies. This section examines the European market, the timing of the Safe Harbor, and the costs imposed by the Safe Harbor and speculates that, over the long-run, the Safe Harbor will do U.S. companies more harm than good.

1. European Market

U.S. companies feared that the Privacy Directive would prohibit them from accessing the European online market,[176] projected to be worth $1.2 trillion by 2004.[177] Judging by the number of U.S. companies that have availed themselves of the Safe Harbor, the European market is extremely attractive to U.S. companies and is one to which they want to assure themselves access.[178] The Safe Harbor has created a "non-tariff trade barrier in that a U.S. person cannot do business with the European Union unless that U.S. person agrees to play by EU rules."[179] However, as discussed below, there is

---

173. *See, e.g.*, John F. Kerry & Carly Fiorina, *Congress Should Act to Boost Online Privacy*, BOSTON GLOBE, Oct. 21, 2000, *available at* http://kerry.senate.gov/`kerry/globe-net.html; Press Release, McCain, Kerry, Abraham, Boxer Unveil Internet Privacy Bill, (July 26, 2000), *at* http://www.senate.gov/~mccain/webprivate.htm.

174. Sanders, *supra* note 166 (discussing how both Democratic and Republican lawmakers are offering privacy bills).

175. *Id.*

176. Baumgarten et al., *supra* note 62.

177. Douglas F. Gray, *Euro Internet Economy Worth $1.2 Trillion by 2004, A New Study Predicts*, IDG NEWS SERVICE (Oct. 26, 2000), *at* http://www.idg.net/ec?go=1&content_source_id=13&link_id=347875. Germany and the United Kingdom will account for over fifty percent of European online revenue in 2004. *Id.*

178. Tamara Loomis, *Data Privacy: A Few Companies Have Complied with EU Law*, N.Y. L.J., Aug. 30, 2001, at 5.

179. Letter to Aaron, *supra* note 2.

evidence that the European Union is not enforcing the Directive. U.S. companies therefore face much greater costs to adhere to the Safe Harbor because they face potential litigation and sanctions from the FTC.[180]

The Directive achieves several victories for European companies. First, it keeps out a number of U.S. competitors. Second, it increases the costs for those U.S. companies that do try to penetrate the European market. Furthermore, the Directive has costly implications for companies with global operations, because companies must be careful of what data is collected and transferred from EU employees to computers located in the United States, as well as how that information is used. This permits the European Union to favor EU companies to the detriment of U.S. companies.

2. Timing

Internet commerce is new—no model of excellence exists and many companies are still trying to figure out how to become profitable.[181] Although many European companies may have considered the issue of privacy immediately, U.S. online companies were not prepared to comply with the Privacy Directive.[182] Even after the Europeans implemented the Privacy Directive, U.S. companies resisted any form of regulation and most made little progress in changing their privacy policies to qualify for the Safe Harbor.[183] U.S. companies may be eager to sign up for the Safe Harbor without considering whether they are technologically or legally prepared. For example, two companies whose websites carried the TRUSTe privacy seal and claimed to adhere to the TRUSTe criteria were selling personal information to a marketing company in violation of the privacy seal policies.[184]

In the two years between the enactment of the Directive and the adoption of the Safe Harbor, European companies had a competitive advantage over their U.S. counterparts and could build brand name recognition within the European Union. A well-known brand name

---

180. Joris Evers, *U.S. Beats Europe in Online Privacy Protection*, INFOWORLD (Jan. 24, 2001), *at* http://www.infoworld.com/articles/hn/xml/01/01/24/010124hnprivsur.xml.

181. Lynch, *supra* note 28.

182. Baumgarten et al., *supra* note 62.

183. Kevin Featherly, *U.S. Cos. Don't Make 'Safe Harbor' Privacy Grade*, NEWSBYTES (Aug. 16, 2001), *at* http://www.newsbytes.com/news/01/169115.html. "American companies doing business overseas electronically have generally failed to implement minimum data privacy protections for their customers . . . ." *Id.*

184. Rebecca Lynch, Analysis, *E-Privacy Debates Faces Long Road Ahead*, CIO (Oct. 4, 2000), *available at* http://www.cnn.com/2000/TECH/computing/10/04/privacy.fuss.idg/index.html.

undoubtedly helps bring traffic to websites.[185] In order to build brand name recognition on the Internet, consumers must be made aware of a website and the services offered. U.S. companies hoping to carry over brand name recognition from the traditional marketplace to the Internet may not be able to do so as easily in Europe, where they lack pre-existing name recognition. These companies often hope to target potential customers by e-mail with promotions for their website.[186] The Directive, however, prohibits U.S. companies from accessing information on European consumers, and those companies who have not signed up for the Safe Harbor cannot contact Europeans, regardless of whether or not they intend to collect personal data.[187] This creates an obstacle to developing brand name recognition among Europeans. The Directive hurts U.S. companies because the websites that develop brand name recognition are the ones that do well.[188]

In some niches of the Internet it is important to capitalize on the first mover advantage.[189] The online-auction business is one such example.[190] eBay was the first to develop brand name recognition in this industry, and while others like Yahoo! and Amazon have tried to compete, eBay has continued to grow and dominate in the online-auction industry due in large part to its first mover advantage and the large mass of users it obtained before its competitors.[191] U.S. companies have lost this advantage in the European market to European companies, who were able to act in the two years between the enactment of the Directive and the creation of the Safe Harbor. Those U.S. companies that are unable to comply with the Safe Harbor are at a disadvantage relative not only to their European competitors, but also to their U.S. counterparts that can comply.

An additional timing problem applies to both the Safe Harbor and any resulting U.S. legislation. "Change is the normal state of

---

185. MARC BRAUNSTEIN & EDWARD H. LEVINE, DEEP BRANDING ON THE INTERNET: APPLYING HEAT AND PRESSURE ONLINE TO ENSURE A LASTING BRAND 26 (2000).

186. *Id.* at 117 (the most successful marketing tool on the Internet is e-mail).

187. SAFE HARBOR, *supra* note 105.

188. Interview by Jack Cafferty with Micheal Exstein, Retail Analyst, Credit Suisse First Boston, *Before Hours* (CNNFN television broadcast, Apr. 6, 2000); *see also FTD.COM Fiscal Fourth Quarter and Year 2000 Results Showcase Strong Gains in Key Operating Metrics*, BUS. WIRE, Aug. 8, 2000 (noting that "[t]he primary driving force behind our growth is the 96% awareness of the FTD brand name among consumers. This brand name recognition continues to fuel our growth as Internet shoppers are increasingly migrating to strong brands with proven distribution capabilities.").

189. Adam Cohen, *eBays Bid to Conquer All: For All the Dotcom Disasters, Here's One Company That's Redefining E-Commerce*, TIME, Feb. 5, 2001, at 48. "The lore among Internet strategists was that whoever nabbed Web space early would have a commanding commercial . . . lead." *Id.*

190. *Id.*

191. *Id.* "Attempts by other companies to replicate eBay have bombed. eBay controls more than 80% of the online-auction market, with Yahoo and Amazon lagging far behind." *Id.*

affairs for the Internet."[192] Regulation is a "cumbersome, inflexible tool" and regulation could "freeze some aspects of the Internet in their current state."[193] Unlike the Internet, which changes and adapts easily, a poorly constructed regulatory scheme will be very difficult to change once in place, due to the U.S. political structure.[194] The United States should not lock itself into a regulatory scheme without ensuring that it will be equipped to support the growth of the Internet. This issue is not of such grave concern for the European Union because directives, unlike regulations, "'are binding as to the result to be achieved' . . . [but] the choice of the method is left to the state concerned."[195] This provides EU Member States much more flexibility in accounting for the growth of the Internet than does U.S. legislation.

3. Increased Costs to Companies

Trying to adopt privacy policies after years of operating without them is proving to be an expensive endeavor for many U.S. companies. To comply with the Safe Harbor or similar U.S. legislation, some U.S. companies' costs for privacy policies may increase from zero to the full cost of compliance.[196] It remains unclear what the actual costs of compliance with the Safe Harbor will be, as there exists no serious study of the cost or "technological feasibility" of implementing the Safe Harbor.[197]

Some of the costs of compliance are foreseeable—and quite considerable. Some websites will have to invest time and money to create privacy policies to satisfy notice requirements, while others will have to adapt their pre-existing privacy policy to satisfy the Safe Harbor.[198]

Arguably, requiring websites to post privacy policies is unnecessary.[199] Consumers who are concerned about privacy can choose to avoid sites that do not post their privacy policies. Websites that choose not to post policies will "choose" to lose these

---

192. Rubin, *supra* note 21.

193. *Id.*

194. *Id.*

195. D. LASOK & J.W. BRIDGE, LAW & INSTITUTIONS OF THE EUROPEAN COMMUNITY 137 (5th ed. 1991).

196. SWIRE & LITAN, *supra* note 97, at 43.

197. Letter to Aaron, *supra* note 2.

198. Letter from Charles A. Prescott, Vice President, International Business Development and Government Affairs, Direct Marketing Ass'n to Ambassador David L. Aaron, Undersecretary for International Trade, Department of Commerce (Apr. 4, 2000), *at* http://www.ita.doc.gov/td/ecom/Comments400/DMAComments.htm.

199. *NCC's Privacy Group Cautions Against Hasty Pledges That May Harm Consumers*, U.S. NEWSWIRE, Feb. 12, 2001 [hereinafter *NCC's Privacy Group Cautions*].

customers.[200] Requiring privacy "legalese" forces all websites to pass costs on to the consumers, and may have the effect of forcing some smaller businesses out of the market.[201]

Likewise, there are costs associated with compliance with the access component of the Safe Harbor. Providing a system where individuals can access the information gathered about them is expensive and cumbersome.[202] Increasing the ease with which consumers can access their own personal data leads to greater security risks, which in turn leads to increased costs for preventing security breaches.[203] Furthermore, compliance with the Safe Harbor requires hiring new employees to ensure information gathered is relevant and to address any concerns raised by individuals.

For smaller online companies, or those experiencing financial difficulties, the privacy requirements may be insurmountable.[204] Most costs associated with privacy protection are fixed. Therefore it is more difficult for such costs to be borne by a small company, because the costs do not depend on the size of the company.[205] A small children's site, Zeek.com, estimated that it would cost approximately $200,000 a year to comply with privacy requirements.[206] Such costs will deter small companies from setting up Internet commerce operations, depriving the market of new start-up companies that have historically served as a source of valuable innovation and growth.[207]

The Safe Harbor also creates enormous inefficiencies for global companies. If the human resource department of a global company wants to maintain records for all of its employees, it must be careful with the data it collects from EU employees and ensure that the data

---

200. *Id.*

201. *Id.*

202. *Id.*

203. *Panelists Say Privacy Solutions Ignore First Amendment,* COMM. DAILY, Oct. 26, 2000. Some argue that the security of personal information should be the larger issue, as opposed to the mere fact that information is collected. *Id.* Tools designed to make personal information more secure are susceptible to fraud and could lead to "social hacking." *Id.*

204. Jennifer Jones, *Financial Institutions Grapple With New Privacy Regulations,* INFOWORLD.COM (Oct. 27, 2000), *at* http://www.infoworld.com/articles/hn/xml/00/10/30/001030hnprivacy.xml. Although the article dealt with compliance with the Gramm-Leach-Bliley Act, the same problems will be faced with the Safe Harbor.

205. Rubin, *supra* note 21. "All of these costs are 'fixed' costs, and so are higher per unit of output for small than for large firms. Thus, any such regulations would serve at least in part as a barrier to entry against small firms, and as a source of protection for large established firms." *Id.*

206. Linda Rosencrance, *Complying With Privacy Law Too Pricey for Kid Site,* COMPUTERWORLD (Sept. 18, 2000), *at* http://www.computerworld.com/storyba/0,4125,NAV47_STO50556,00.html. Although Zeek.com was dealing with the costs of complying with the Children's Online Privacy Protection Act, the costs and requirements of the Safety Harbor are equivalent. *Id.*

207. Rubin, *supra* note 21.

is used only for approved purposes.[208] This also impacts the use of company-wide Intranet services. In designing such services, companies must either restrict access to U.S. domestic employees or take the expensive measures necessary to ensure compliance with the Safe Harbor.

Currently the Safe Harbor only controls transactions with individuals within the European Union, but proposed legislation indicates that the protections Europeans receive will soon be extended to U.S. citizens.[209] For those companies adhering to the Safe Harbor in their treatment of Europeans, applying this treatment to U.S. citizens will increase costs because there will be more information for which to account. Furthermore, there is a value in collecting, analyzing, and using the data of consumers. The Safe Harbor and the resulting legislation will severely limit the use of such data.

The Safe Harbor and resulting legislation take away another competitive tool of Internet companies: Internet companies could otherwise distinguish themselves from their competitors according to the level of the privacy protection they provide. U.S. privacy legislation will have the effect of "leveling the playing field." A recent Forrester Research survey found that forty-one percent of Internet shoppers read the privacy policies of websites they visited for the first time.[210] The more satisfied they are with a site's privacy policy, the more likely they are to stay and shop.[211] Furthermore, a user could choose to maintain complete anonymity on a site, but in return may be unable to access some portions of the site.[212] This method would allow users to determine the value of their personal information.[213] The Forrester Research survey found that trust develops when people can control their information and receive a benefit for sharing it.[214]

---

208. Stephen Lawson, *Former U.S. Trade Official: Privacy Headaches Will Linger*, IDG NEWS SERVICE (Mar. 27, 2001), *at* http://www.idg.net/crd_idgsearch_0.html?url=http%3A%2F%2Fwww%2Ecomputerworld%2Ecom%2Fcwi%2Fstory%2F0%2C1199%2CNAV47_STO59023%2C00%2Ehtml&sc=. "[M]ultinational companies that centralize their human-resources operations in the U.S. may have to grapple with what information can and can't be carried across borders and stored." *Id.*

209. Patrick Thibodeau, *'Safe Harbor' Deal Takes Effect, But Adoption May Be Slow*, COMPUTERWORLD (Nov. 1, 2000), *at* http://www.computerworld.com/storyba/0,4125,NAV47_STO53171,00.html. "Americans are going to ask why they are second-class citizens in their own country." *Id.*

210. Pamela Blackstone, *Making Privacy a Policy*, PUBLISH, *at* http://www.publish.com/features/0012/feature13.html.

211. *Id.*

212. *Id.*

213. Consumers willing to exchange their personal data online are often able to find better discounts. Karen Talaski, *E-tailers discover coupons; Online shoppers make more purchases*, DETROIT NEWS, Oct. 10, 2000, at B1. Other customers are willing to exchange data for the chance to wins thousands, even millions, of dollars. Fred O. Williams, *Area Man Wins Cybercash*, BUFFALO NEWS, Oct. 28, 2000, at C11.

214. Blackstone, *supra* note 210.

Those websites that take extra steps to protect privacy earned this trust. Consumer desires prompt websites to take action without government coercion. Websites are motivated to avoid developing a reputation for not respecting consumer privacy rights.[215] The impact of these negative effects should be enough to motivate websites, and until it can be shown to be inadequate, government should not interfere.[216]

4. Increased Costs to Consumers

Privacy legislation may also increase costs for consumers who use the Internet. Currently, revenue generated from advertisement space on websites helps to fund the websites.[217] These advertisements, or banner ads, permit the placement of cookies to record online behavior.[218] Advertisers use this information under the credo "past behavior determines the future."[219] While consumers may not approve, it makes advertising more effective and consumer "web surfing" more efficient and cheaper. A self-regulatory scheme permits interaction between websites and consumer so that a balance can be struck between the amount of information a consumer reveals and the power of companies to effectively use the information. Proposed legislation may lead to fewer online services and reduced website content, because it will hinder the effectiveness of advertising, thus decreasing the incentive to advertise on the Internet.[220] This will hurt the same consumers that the legislation is intended to benefit.[221]

The Safe Harbor and proposed legislation fail to take into account variations among consumer preferences for privacy protection.[222] Consumers have shown a willingness to enroll in Internet surfing programs that monitor all browsing.[223] The Internet and privacy technology currently offer all levels of privacy

---

215. Rubin, *supra* note 21.

216. *Id.*

217. *Id.* (noting that "advertising revenue supports many valuable services that are provided to consumers at no charge. . . . The amount of free information available on the Internet is truly remarkable, and this information is paid for through advertising.").

218. Lynch, *supra* note 28.

219. *Id.*

220. Brailor, *supra* note 165.

221. *Id.* (arguing that the Internet should remain open and "allow consumers to enjoy the full benefits of the new economy's innovations").

222. Rubin, *supra* note 21. An AT&T Internet privacy survey found that roughly one quarter of Americans are "intensely" concerned about privacy and another quarter have little or no concern. *Id.*

223. *Id.* (noting that "AllAdvantage.com pays consumers to monitor their browsing").

protection.[224] This is different from the privacy environment of the EU Privacy Directive, where privacy is considered a fundamental right.[225] The level of preference for privacy protection is much more easily identifiable in such an environment. Europeans may be less willing than their U.S. counterparts to have their entire web browsing activities monitored. The Safe Harbor did not take this into account because it was concerned only with the interactions of U.S. companies with Europeans. U.S. legislation, however, should take this difference into account. Otherwise, those consumers who are willing to share their information in exchange for benefits will lose this option.[226]

Use of consumer data leads to efficiencies for consumers. Consumers receive information that is tailored to their interests.[227] This targeting prevents consumers from being bombarded by advertisements of no interest to them.[228] Both consumers and advertisers thus "have an interest in better targeting of advertising messages."[229]

Privacy legislation may adversely affect consumers in another way. It is possible that disclosing the volume of information required by the Safe Harbor will overwhelm Internet users.[230] Consumers may find it inconvenient to be forced to read notices of privacy policies before using a website.[231] "Opting-in," which is advocated by some, is one such example of inconvenient notices. Opting-in requires each site to obtain user permission before collecting personal data.[232] Those consumers that do read the notices may find them incomprehensible, even if efforts are made to ensure they are "clear and conspicuous."[233]

The more efficient method is "opting out," which requires users to proactively refuse to have their personal information collected.[234] Opting-out allows consumers who are concerned about their privacy to take easy steps to protect themselves, while those consumers who are not worried and want to benefit from the collection of their

---

224. *Id.*

225. *See supra*, European Union Treatment, Part III.B.

226. *See* Rubin, *supra* note 21. "Privacy regulations could have the effect of making some business plans infeasible and thereby depriving consumers of goods and services that are now available." *Id.*

227. *Id.*

228. *Id.*

229. *Id.*

230. Rotenberg Testimony, *supra* note 117.

231. *See id.*

232. Mark Rockwell, *ISPs Opt In and Out–Selling personal consumer information is a lucrative trade coming to a possible end*, TELE.COM, Dec. 11, 2000, at 37.

233. Rotenberg Testimony, *supra* note 117.

234. Privacy Glossary, *supra* note 25.

information can choose to do so without cumbersome procedures.[235] "Opting-in" places the burden on the concerned consumer, rather than the company and other consumers who are not concerned with the collection of their data.

5. Costs to the Market of Developing Businesses

Internet privacy legislation may sound a death knell for a developing industry. Regulation may destroy the need for privacy seals such as those provided by TRUSTe and BBBOnline, because the criteria and services these companies provide will be legislatively required. While TRUSTe has—at least temporarily—preserved a need for its services by partnering with the Department of Commerce,[236] this solution may be short-lived. If Congress passes legislation similar to the Safe Harbor, there will be little or no reason for companies to obtain a TRUSTe or BBBOnline privacy seal. If companies must, by law, comply with privacy regulations to operate on the Internet, there is no need for a privacy seal to assure customers that a website is respecting their privacy rights. The fear of legal action for failure to comply should be sufficient to warrant adherence to posted privacy policies.

Another business that may be lost is currently developing technology to enable users to control the amount of data they reveal.[237] The technology is still relatively new and therefore has not had enough time to demonstrate its effectiveness.[238] This technology would allegedly improve a company's ability to compile data about consumers while attaching consumer preferences for gathering and sharing information.[239] Such technology enables websites to respect consumer privacy preferences without continuously bombarding

---

235. Brailor, *supra* note 165 (arguing that "[c]onsumers should be allowed to receive benefits and services from vendors in exchange for the use of information. It is important that the consumer understands this use and be able to make an informed choice to provide information in return for the benefit received.").

236. Privacy Seal Program, *supra* note 122. BBBOnline is also trying to secure a position for itself within a regulatory framework. BBBOnline has formed a partnership with the Japan Information Processing Development Center to develop recognizable privacy seals for Japan and the United States. *White House Annual Electronic Commerce Report Praises BBBOnline for Promoting Online Consumer Protection,* BUS. WIRE, Jan. 19, 2001.

237. For example, iPrivacy allows shoppers to use a password to check into a trusted site. Leslie Brooks Suzukamo, *To Some, It's a Cookie; To Others, A Monster,* NEWS AND OBSERVER, Jan. 22, 2001, at D6. From there shoppers go shopping on the web, but when the websites look at the shopper it sees the iPrivacy computer server, not the consumer's. *Id.* Another example is PersonaValet 3.0, which enables users to block and monitor unwanted cookies. *Id.* It lists the website that sent the cookie and allows the user to determine whether to destroy or keep the cookie. *Id.*

238. *Id.*

239. Robert O'Harrow, Jr., *Internet Firms Act to Ease Sharing of Personal Data,* WASH. POST, Dec. 5, 2000, at E1.

consumers with notice and consent requests.[240]

Another technology designed to help solve this issue was developed by the World Wide Web Consortium, and is called a "Platform for Privacy Preferences" (P3). P3 is based on the principles of notice, control, and choice.[241] This enables consumers to set their computer so it operates at a preferred level of privacy protection.[242] When a consumer attempts to visit a site which requests more information than the consumer is willing to disclose, the site can refuse to let the consumer enter, ask the consumer to make an exception, or waive its information request and allow the consumer to use the website without collecting information.[243]

If the collection of data were regulated, then there would be no need for such technologies. The market was in the process of crafting its own answer to the privacy dilemma. These technology-based solutions would have benefited both consumers and companies. Companies could still gather useful information and concerned consumers could choose to incur the costs to protect their privacy.[244] Also, concerned consumers utilizing privacy-protecting technology could choose to disclose information when they believed it was secure and beneficial for them to do so.[245]

6. Liability

As of yet, there has been no evidence that European authorities will enforce their data privacy laws against companies based in Europe.[246] U.S. companies are concerned that there may be a double standard.[247] U.S. companies should resist the Safe Harbor if they perceive that U.S. companies are being treated unfairly.[248] Upon implementation of the Directive, Privacy International, a leading

---

240. *Id.*

241. Budnitz, *supra* note 31, at 884. Other technology has also developed. Andrea M. Singh, *Internet Privacy, In Any Language, Is Beneficial*, NEWSDAY, Apr. 30, 2001, at C7. The Ponoi Corporation enables users to surf the Internet through the company website at http://www.ponio.com. *Id.* The technology prevents third parties from accessing personal data such as the identity of the user and Ponio does not have access to the personal data of its users. *Id.* The technology is portable, as it is within a browser as opposed to a desktop application. *Id.*

242. Bunditz, *supra* note 31, at 884.

243. *Id.*

244. Rubin, *supra* note 21; *see also NCC's Privacy Group Cautions*, *supra* note 199.

245. Steven Hetcher, *Climbing the Walls of Your Electronic Cage*, 98 MICH. L. REV. 1916, 1934 (2000).

246. Thibodeau, *supra* note 209. There is an argument that the current U.S. policy of self-regulation in fact provides U.S. Internet users more privacy protection than the EU privacy protection laws, which are seldom enforced. *Panelists Say Privacy Solutions Ignore First Amendment*, COMM. DAILY, Oct. 26, 2000.

247. Thibodeau, *supra* note 209.

248. *Id.*

advocacy organization, began to investigate the practices of twenty-five multinational companies to determine whether their information practices violated the Directive.[249] Some of the companies investigated were Ford, Hilton International, Marriott International, and Microsoft.[250] There was no evidence that purely European companies were also being investigated on such a completely random basis.[251]

Regardless of whether U.S. privacy legislation is passed, if a U.S. company violates the Directive, its liability may be greater than its European counterparts for a suit brought by a European. The ability of a European to win a judgment against a U.S. company depends on two possible factors: the willingness of U.S. courts to apply European law to decide liability in a case brought against a U.S. company, and the willingness of U.S. courts to enforce a European judgment against assets located in the United States.[252] There may be more of an incentive to bring suit in a U.S. court because, unlike many European countries, the loser of litigation does not have to pay the legal expenses of the winner.[253] Also, damages are generally larger in the United States.

An even greater problem arises if the United States passes legislation that enables U.S. citizens to sue U.S. companies. Due to differences in the legal system between the European Union and United States, U.S. companies are subject to much larger judgments.[254] If U.S. legislation is passed, U.S. companies that fail to adhere to the Safe Harbor or U.S. legislation are at risk of much greater liability then their European counterparts. "Certain procedural factors, like jury trials and contingent fees, are absent in Europe, as are some of the economic incentives to sue, due to a more pervasive welfare system in Europe which offers adequate redress."[255] Also, the Consumer Internet Privacy Enhancement Act permits civil actions by states on behalf of individuals. The risk of civil liability is not an issue in Europe.[256]

Evidence suggests that European companies are actively

---

249. Woodward & Roethenbaugh, *supra* note 82.

250. *Id.*

251. *Id.*

252. Perritt & Stewart, *supra* note 9, at 817.

253. *Id.*

254. There is also the question of whether the inverse could be asked. Would Europeans with websites reaching U.S. customers be subject to greater damages in litigation then European websites that do not reach U.S. customers? Would this discourage European companies from trying to penetrate the U.S. market?

255. Joachim Zekoll, *Kant and Comparative Law—Some Reflections on a Reform Effort*, 70 TUL. L. REV. 2719, 2731-32 (1996).

256. In Europe, the loser of a civil liability claim must pay the court costs and attorney fees of the winner. This affects the selection of suits for litigation. Eric Talley, Symposium on Fee Shifting, *Liability Based Fee Shifting Rules and Mechanisms Under Incomplete Information*, 71 CHI.-KENT L. REV. 461 (1995).

collecting consumer data, even with the extensive regulations provided by the Directive.[257] Consumer World, a worldwide federation of 263 consumer organizations, conducted a study in which the privacy policies of popular U.S. and European sites were analyzed.[258] Among European sites, only nine percent asked permission to sell the information provided by the customer and only twenty percent asked permission before adding the customer to an e-mail distribution list.[259] Among U.S. sites, half asked for consent to sell customer information.[260] What is most striking about these figures is that the European websites analyzed were operating under a comprehensive set of privacy rules, while U.S. websites analyzed were operating in a relatively unregulated environment. This suggests that European regulations are not being enforced against European companies.

VII. CONCLUSION

The issue of privacy on the Internet is relatively new to the United States and should not be addressed hastily. Despite the strides that were being made under a self-regulatory approach, comprehensive legislation now appears inevitable. In creating such legislation, however, there must be careful consideration of both the current and future state of the Internet. The EU Directive and resulting Safe Harbor should not be followed blindly without considering the enormous differences in the historical treatment of privacy in the European Union, the legal structure of the European Union, and the geographically borderless features of the Internet and the global economy. These characteristics require U.S. legislators to thoroughly analyze privacy legislation options.

To carefully craft legislation, legislators should not begin with the Safe Harbor as a minimum standard for privacy legislation. The Safe Harbor should be recognized for what it is—a hasty attempt to assure compliance with the EU Directive. Legislation must consider the unique characteristics of the Internet in the United States, including the Internet's history of self-regulation and the speed at which the Internet grows and changes. Issues such as notice and consent should not take precedence over free speech and economic concerns. Legislators must keep in mind what the true issues are and not merely hurdle over them by beginning with the Safe Harbor as a basis for any newly proposed legislation. Time must be taken to

257. Evers, *supra* note 180.
258. *Id.*
259. *Id.*
260. *Id.*

ensure that legislation is well coordinated to protect consumers while fostering the growth of the Internet and ensuring that the costs of legislation do not exceed the benefits.

Angela Vitale[*]

---

* J.D. candidate 2002, Vanderbilt University. B.B.A. Finance 1999, The George Washington University. I would like to thank Jonathan Winer and Professor Steven Hetcher for taking the time to provide me with guidance on this topic.