# TREADING WATER IN THE DATA PRIVACY AGE: AN ANALYSIS OF SAFE HARBOR'S FIRST YEAR

## I. INTRODUCTION

In 1995 the European Union (EU) enacted the Data Privacy Directive[1] (Directive), a comprehensive law requiring each EU Member State[2] to adopt strict controls over the use of personal information gathered in Internet transactions and the creation of national privacy regulators.[3] The Directive, which became effective on October 25, 1998, requires EU member states to prohibit the transfer of personally identifiable data[4] to non-EU countries that do not provide "adequate" privacy protections, thereby forcing such countries to enact legislative provisions that would meet this "adequacy" standard.[5]

From its inception the Directive has proven problematic for United States companies as the U.S. has stood firm on its policy to not create broad privacy laws.[6] The U.S. has long sought to foster its capatalistic market economy by encouraging industry self-regulation, rather than enacting broad

---

1. *See* Council Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 (O.J. 95/L281). (hereinafter *Directive 95/46/EC*) *See also* THE EUROPEAN COMMISSION INTERNAL MARKET DIRECTIVE *available at* http://europa.eu.int/comm/internal_market/en/ (last visited on Oct. 26, 2001).

2. The fifteen Member States of the EU include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. *See* SAFE HARBOR WORKBOOK, *at* http://www.export.gov/safeharbor/sh_workbook.html (last visited Oct. 26, 2001).

3. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 1-4 (1997). The rise of data transfer technology over the last few decades has made the protection for individual's personal information all the more difficult. *See id.* In meeting the struggle to maintain an appropriate level of protection, countries throughout the world have developed legislative enactments. *See id.* As this area of law continues to expand, it can be expected to draw increasing attention from the U.S. Legislature. *See id.* In the 104th Congress, nearly 1,000 of 7,945 bills introduced addressed some privacy issue. *See id. See also* James M. Assay, Jr., Demetrious A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145 (2001).

For a discussion on information acquisition techniques including covert acquisition, overt acquisition and use of information obtained from consumers see Anna E. Shimanek, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455 (2001).

4. The Directive defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Directive 95/46/EC*, *supra* note 1, at art. 2(a). For more on the definition of "personal data" see *infra* note 65.

5. *Directive 95/46/EC*, *supra* note 1, at art. 25(1).

6. *See* CATE, *supra* note 3, at 48. "It is difficult to imagine a regulatory regime offering any greater protection to information privacy, or any greater contrast to U.S. law." *Id.*

legislation, in providing protection for its citizens' personal information.[7] With the inception of the EU's Data Privacy Directive, however, many feared that the United States' failure to meet the Directive's standards may cause U.S. companies to lose a great deal in revenue and efficiency as data transfers "are the life blood of many organizations and the underpinnings for all of electronic commerce."[8] To overcome this obstacle, the United States began negotiating "Safe Harbor" privacy principles with the EU.[9] Under these provisions, U.S. companies would voluntarily create a set of self-regulatory guidelines that would be deemed "adequate" by the Data Privacy Directive standards.[10] In order to acquire personal data from companies in EU Member States, U.S. companies who agree to the regulation must provide a higher level of privacy to these consumers by promising them basic control over how their information is used.[11]

Following a period of intense negotiations, and to the dismay of broad privacy law advocates and many in the European Union Parliament, in July 1999, the U.S. convinced the European Commission, by a vote of 279 to 259, to accept the Safe Harbor principles.[12] On November 1, 2000, the compromise took effect, leaving many uncertain as to whether U.S. companies would jump on board and be willing to operate under the self-regulated Safe Harbor

---

7. *See* SAFE HARBOR WORKBOOK, *supra* note 2.

8. *Id.* In 1999, the U.S. had approximately $350 billion in trade with EU Member States. *See id.* In terms of cost efficiency, where many multinational corporations share offices in both the U.S. and in one or more EU Member States, the prohibition of transferring information such as personal telephone directories, personal records, and other human resource information within a single organization could lead to a significant increase in costs and decreased efficiency. *See id.* In terms of revenue, one source estimated the loss to be as much as $120 billion. *See* Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 650 (2001). *See also* Neil King, Jr., *Clinton and EU Make Progress, but Not a Lot*, WALL ST. J., June 1, 2000, at A24.

The Directive's standard states that the EU could prohibit the transfer of data to the U.S. if the U.S. is unwilling to provide an "adequate" level of protection. *See Directive 95/46/EC*, *supra* note 1, art. 25(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." *Id.*

9. ISSUANCE OF SAFE HARBOR PRIVACY PRINCIPLES AND TRANSMISSION TO EUROPEAN COMMISSION, 65 Fed. Reg. 45,666 (2000) [hereinafter *Safe Harbor*]. For more on the EU and U.S. positions in the negotiations see *infra* note 80

10. *See Safe Harbor*, *supra* note 9, at 45,666. *See also Directive 95/46/EC*, *supra* note 1, at art. 25(1).

11. *See* Juliana Gruenwald, *Stormy Seas Ahead Over 'Safe Harbor'*, INTERACTIVE WEEK (Oct. 30, 2000), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2646060,00.html. From the onset, this has been one of the chief concerns with the U.S. compromising with the EU in enacting the Safe Harbor program. *See id.* Under the program, U.S. companies would be agreeing to provide a higher level of information protection to EU Member State citizens than to citizens of the U.S. *See id.*

12. *See Safe Harbor*, *supra* note 9, at 45,666.

provisions.[13] Further, many wondered whether U.S. consumers would stand for companies providing higher levels of protection for European consumers than for U.S. consumers.[14]

Following the close of the Safe Harbor program's first year, many are continuing to call the U.S. Legislature to abandon the Safe Harbor self-regulatory program and enact broad privacy laws.[15] This note, however, will show that in light of the first year of Safe Harbor, the United States policy of self-regulation in the private sector based upon its capitalistic market economy is actually strengthened and that the program is proving beneficial to both U.S. organizations and U.S. citizens. The analysis will begin in Section II with a comparison of privacy policies under European and United States perspectives. Section III will present the development and guidelines of the Directive and the provisions of the Safe Harbor compromise negotiated by the EU and the United States. Finally, Section IV will show how U.S. companies have responded to the Safe Harbor program in its first year, how U.S. companies have weighed the benefits and costs associated with Safe Harbor, and how Safe Harbor has impacted U.S. companies, U.S. citizens, and U.S. policy as a whole.

## II. A COMPARISON OF THE EU AND U.S. APPROACHES TO DATA PRIVACY LAW

### A. *European Approach*

To understand the conflict the United States has had in collaborating with the terms of the EU's Directive, the two governmental approaches on privacy issues must first be discussed. While the United States has long sought to avoid broad policy laws and allow industries to self-regulate protection of data privacy matters,[16] European nations have recognized individual data privacy as a fundamental right,[17] leading many European

---

13. *See id. See also* Gruenwald, *supra* note 11. Many experts feel that the plan will fall apart as U.S. companies fail to join the safe harbor program. *See id.*

14. *See* Gruenwald, *supra* note 11.

15. *See The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearings Before the Subcomm. On Commerce, Trade and Consumer Protection*, 107th Cong. at 40-41 (Mar. 8, 2001)(statement by Rep. Markey)[hereinafter *Hearings*]. In his address to the Subcommittee on Commerce, Trade, and Consumer Protection, Representative Markey expressed his concern that rather than Congress listening to the "85% of Americans" who would prefer broad privacy enforcement, Republicans and Democrats in the House of Representatives have turned this into a political battle. *See id.*

16. *See* Assay, *supra* note 3, at 149-50.

17. *See* SAFE HARBOR WORKBOOK, *supra* note 2. In addressing the history of the European fundamental right view, the Chairman of the Committee on Energy and Commerce, Hon. W.J. "Billy" Tauzin, stated:

> The U.S. and EU Member States approach the issue of privacy from different perspectives. Europeans are instilled with the belief that privacy is a

governments to enact "rights-based data protection."[18]

The history of European data privacy protection law goes back to 1970 when the German state of Hesse enacted the first data protection statute.[19] Sweden soon followed in enacting the first national data protection statute.[20] By 1997, most European nations[21] had broad policy or data protection statutes.[22]

The 1980's opened with the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD) issuing their *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Guidelines).[23] The Guidelines presented basic data privacy principles and allowed for data to freely pass between nations who adopted the principles.[24] The OECD intended that these "principles . . . be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."[25] One year following the issuance of the Guidelines, the Council of Europe promulgated a convention, *For the Protection of Individuals with Regard to Automatic Processing of Personal Data*, which took effect in 1985.[26] The convention focused more heavily on protection of personal

---

> fundamental human right. There are a number of reasons for this belief, including the vast and traumatic experiences of the Nazi regime during the 1940's. Another reason for this perspective is the simple fact that many EU countries are relatively new democracies.

*Hearings, supra* note 15, at 5. (statement by Hon. W.J. "Billy" Tauzin, Chairman, CEC). This recognition of privacy rights as fundamental was codified in Chapter I, Article 1, of the Directive where it states,

> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

*Directive 95/46/EC, supra* note 1, at art. 1.

18. Assay, *supra* note 3, at 148.

19. *See* CATE, *supra* note 3, at 32.

20. *See id.*

21. These nations include Austria, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom. *See id.*

22. *See id.*

23. *See* GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, O.E.C.D. Doc (C 58 final)(Oct. 1, 1980) [hereinafter GUIDELINES]. *See also* CATE, *supra* note 3, at 34.

24. *See* GUIDELINES, *supra* note 23.

25. Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 466 (2000), *citing* GUIDELINES, *supra note 23*. The principles set forth in the Guidelines were intended as a response to the "danger that disparities in national legislations could hamper the free flow of personal data across frontiers." *Id.* These principles are largely mirrored in the Directive. *See id.*

26. *See* CATE, *supra* note 3, at 34. Both the Guidelines and the convention are criticized due to the lack of enforcement power held by the OECD and the Council. *See id.* However, where the Guidelines failed to set a vision for how countries should work together to bridge their different protection standards, the Convention focused on "stregthen[ing] democracy, human rights, and the rule of law throughout its member states" and attempted to inform national legislation on the uniform protection of personal data. Fromholz, *supra* note 25, at 466,

privacy than the Guidelines and required member countries to enact conforming national laws.[27] Following the Council of Europe's urging EU Member States to ratify and implement the convention, by 1997 all but one of the EU Member States had national legislation consistent with the convention.[28]

The enactment of the Directive in 1998 acted as a harmonization of the domestic privacy laws of many of the member states.[29] The Directive's roots, however, can be traced to the *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*,[30] a 1990 draft publication of the commission of the European Community[31] that sought to move European data protection policies away from merely an economic perspective and into the political realm, thus, creating a broad-based political union.[32] The draft directive was soon thereafter amended and approved in 1992, as the European Parliament sought

---

467 *quoting* OECD WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, MINISTERIAL DECLARATION ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS, 5 (Oct. 1998).

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

28. *See id.* at 35. Although the principles of the convention were adopted by fourteen of the fifteen EU member states and Switzerland, there was disunity between the legislative enactments of the states. *See id.* One author concluded that this was due to three reasons: first, some national legislation existed before the convention; second, the convention was not self-executing, meaning that each country could enact their own national laws in different ways; and third, the convention failed to define what an "adequate" level of data protection was, leaving countries to enact their own standard. *See id.*

29. *See* Assay, *supra* note 3, at 149. For more on the Directive acting as a response to a number of domestic privacy laws that arose in Europe throughout the 1970's and 1980's see Kevin Bloss, *Raising or Razing the E-Curtain?: The EU Directive on the Protection of Personal Data*, 9 MINN. J. GLOBAL TRADE 645 (2000).

30. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF EUROPE ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, art. 4, *reprinted in* THE PRIVACY LAW SOURCEBOOK 1999: UNTITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 219 (Marc Rotenberg ed., 1999).

31. *See id. See also* CATE, *supra* note 3, at 35.

32. *See* CATE, *supra* note 3, at 35. Many feel that the European approach is an attempt to prevent an authoritarian regime as was seen in Nazi Germany. *See id.* One author noted: European data protection laws include the hidden agenda discouraging a recurrence of the Nazi and Gestapo efforts to control the population, and so seek to prevent the reappearance of an oppressive bureaucracy that might use existing data for nefarious purposes. This concern is such a vital foundation of current legislation that it is rarely expressed in formal discussions. This helps to explain the general European preference for strict licensing systems of data protection . . . . Thus European legislators have reflected a real fear of Big Brother based on common experience with the potential destructiveness of surveillance through record-keeping. None wish to repeat the experiences endured under the Nazis during the second World War. *Id.* at 43-44 *quoting* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES, 306 (University of North Carolina Press, 1989). In his analysis, Fred H. Cate stated, "It is ironic that the directive seeks to ensure the prevention of an authoritarian regime by creating government authorities with sweeping powers to oversee data-related activities." CATE, *supra* note 3, at 44.

to do away with any distinction between information gathered from private and public sectors.[33] In 1995, the Council of Ministers formally approved the Directive which would take effect three years later.[34]

### *B. United States Approach*

While Europe has moved from individual states enacting rights-based data protection in the 1970's and 1980's to a uniform broad-based political information protection in the 1990's, the United States has consistently held to its market-based, industry-regulated approach.[35] The U.S. Constitution does not address privacy and personal autonomy directly, and therefore, privacy rights in general were not recognized as fundamental for many years.[36] The Supreme Court expanded the term "liberty" over the last century to include certain privacy protections for U.S. citizens.[37] In this expansion, the Supreme Court has interpreted a number of the Bill of Rights amendments as providing a right to privacy against intrusive governmental activities.[38] These individual fundamental rights of privacy, however, are limited to protection from the public, governmental sector, unless otherwise provided by state action.[39]

U.S. privacy law in the private sector can be a bit troubling as Congressional privacy protections in general provide little help.[40] Adding to the confusion in the private sector, the definition of "privacy" itself seems to change from one area of the law to another.[41] One author described this inconsistency: "Privacy is a notoriously slippery term. Because, for good or ill, United States citizens enjoy limited privacy rights under a patchwork of sectoral privacy laws, different situations call for different definitions of privacy."[42]

---

33. *See* CATE, *supra* note 3, at 36.

34. *See Directive 95/46/EC, supra* note 1. *See also* CATE, *supra* note 3, at 36.

35. *See* SAFE HARBOR WORKBOOK, *supra* note 2.

36. *See* CATE, *supra* note 3, at 52.

37. *See* WILLIAM COHEN, AND JOHNATHON D. VARAT, CONSTITUTIONAL LAW: CASES AND MATERIALS, 570-71 (Tenth Edition, The Foundation Press, Inc., Westbury, New York, 1997).

38. *See* CATE, *supra* note 3, at 52. The Amendments in the Bill of Rights interpreted by the Supreme Court to provide such protection include the First Amendment's provisions for freedom of expression and association, the Third Amendment's protection against quartering solders in one's home, the Fourth Amendment's protection against unreasonable searches and seizures, the Fifth Amendment's due process clause and freedom from self-incrimination, the Ninth and Tenth Amendments' freedom for people to retain power over state, and the Fourteenth Amendment's due process clause and equal protection clause. *See id.*

39. *See id.*

40. *See id.*

41. *See* Jenab, *supra* note 8, at 647.

42. *Id.*

The purpose of the U.S. approach is based upon the premise that information privacy is not an unlimited or absolute right.[43] U.S. policy, therefore, seeks to draw a balance between the individual's desire to maintain a level of privacy over his personal information and society's benefit in its use of such information.[44] In its continued attempt to steer clear of broad-privacy policies while providing a means for appropriate personal information protection, the U.S. continues to approach data-privacy in the private sector through issuance of regulations and statutes protecting specific types of data.[45] Specifically, the U.S. has regulated privacy in five areas: federal statutes and regulations, state statutes and regulations, state common law, self-regulation, and through the EU Directive.[46]

With regard to the first area, federal statutes, Congress has passed a number of enactments intended to protect individual privacy data that is specific to the area of the enactment.[47] Examples include the Fair Credit Reporting Act,[48] which governs credit reporting agencies and employment-

---

43. *See* Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1197 (1999).

44. *See id.*

45. *See* Eric Jorstad, *The Privacy Paradox*, 27 WM. MITCHELL L. REV. 1503, 1513-14 (2001).

46. *See id.* For more on the provisions of the EU's Data Privacy Directive see *infra* Part III. State statutes and regulations and state common law are beyond the scope of this note and, therefore, will be excluded from the discussion. However, for more information concerning these areas of privacy law see *id.* at 1516-17.

47. *See id.* at 1514. Recently, in *Reno v. Condon*, 528 U.S. 141 (2000), the Supreme Court reinforced this power of Congress to enact narrowly drawn statutes governing protection of personal information in specific fields. *See id.* at 151. In this case, the State of South Carolina and its Attorney General brought an action against the United States challenging the constitutionality of the Driver's Privacy Protection Act, 18 U.S.C. §2721-2725 (DPPA). *See Reno v. Condon*, 528 U.S. 141 at 143. The DPPA restricts the ability of the states to disclose a driver's personal information without the driver's consent. *See* Driver's Privacy Protection Act, 18 U.S.C. §2721-2725. Upon granting certiorari, the Supreme Court reversed the district courts issuance of summary judgment for the plaintiff and held that the DPPA is a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause. *See Reno v. Condon*, 528 U.S. 141 at 151.
Although the decision in *Reno v. Condon* may have expanded the scope of Congressional authority over personal information "sold or released into the interstate stream of business," *Id.* at 148, Congress still falls short from being able to enact generalized privacy regulations over the private sector as much of the information transferred and used does not meet the standard of "sold or released." *Id. See also* Shimanek, *supra* note 3, at 470.

48. Fair Credit Reporting Act, 15 U.S.C. § 1681, (1994 & Supp. 1998). The statute requires consumer reporting agencies to "adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter." *Id.* at §1681(b). The statute creates civil liability for consumer reporting agencies and users of consumer reports that fail to comply with its requirements. *See Wiggins v. Philip Morris, Inc.*, 853 F.Supp 458, at 468 (D.D.C. 1994).

related data,[49] the Gramm-Leach-Bliley Act,[50] which governs data practices of financial institutions,[51] and the Health Insurance Portability and Accountability Act,[52] which governs data gathered by health care institutions.[53] Other federal statutes regulate data collection based upon the age of the data subject, type of data recipient, or means of data collection.[54] These examples illustrate that U.S. privacy statutes are narrowly drawn to govern either the collection and use of personal identifiable information within specific industrial or economic sectors or are limited to government collection and use of personally identifiable information.[55]

A second manner in which the U.S. protects data is through industry self-regulation.[56] The idea is to allow private-sector industries to develop themselves without the burden of government interference.[57] These self-regulatory programs are designed to allow industry representatives to work along side consumer groups, and often the Secretary of Commerce and the Director of the Office of Management and Budget, to develop mechanisms to protect privacy using traditional fair information privacy practices.[58] This

---

49. *See* Jorstad, *supra* note 45, at 1514.

50. Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999). The Gramm-Leach-Bliley Act was signed into law by President Clinton on November 12, 1999. *See id.* Under the act, financial institutions must provide clear and conspicuous notice to consumers upon their initiating the customer relationship, obtain consent from consumers prior to disclosing a consumer's nonpublic information to a nonaffiliated third party, and provide a reasonable method for consumer's to "opt out" of such disclosures. *See id.* The statute became mandatory on July 1, 2001. *See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33, 677 (May 24, 2000). *See also* Bradley A. Slutsky, Allison S. Brantley, *21st Annual Institute on Computer Law, I. Privacy on the Internet: A Summary of Government and Legal Responses and a Practical Guide to Protecting Your Client*, 637 PLI/PAT 85, 90 (Feb.-Mar. 2001).

51. *See* Slutsky, *supra* note 50, at 90.

52. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996). This statute was created by the 104th Congress to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes." *Id.*

53. *See* Jorstad, *supra* note 45, at 1514.

54. *See id.* Examples of such regulatory statutes include The Children's Online Privacy Act, which provides protection for web site collection and use of data of children age thirteen and under, 15 U.S.C. § 1601-1606 (Supp. 1998), The Electronic Communications Privacy Act, which governs the turning over of information to law enforcement agencies, 18 U.S.C. §2510-2513, 2515-2522 (1994 & Supp. 1998), and Federal anti-eavesdropping and wiretapping laws that prohibit third party interception of communications. *See* Anti-Wire Tapping Act, 18 U.S.C.A. § 2511 (West 2000). *See also* Communications Act of 1934, 47 U.S.C.A. § 605a (West 1991).

55. *See* Cody, *supra* note 43, at 1197.

56. *See* Jorstad, *supra* note 45, at 1514.

57. *See* Cody, *supra* note 43, at 1203.

58. *See id.* Many advocates for the U.S. self-regulatory approach feel that industries change too rapidly for government legislative solutions. *See* CATE, *supra* note 3, at 198. Also, most U.S. corporations are looking at a global market, which is impossible for a single country

level of industry autonomy, free from governmental intrusion, has long been a foundation for the U.S. market economy.[59]

## III. ELEMENTS OF THE DIRECTIVE AND THE U.S.-EU COMPROMISE

With the two approaches towards protecting private information so drastically opposing, it is no wonder that the U.S. struggled with the EU's development of the Directive in 1995. In particular, the U.S. conflict with the Directive arises under the Directive's "adequacy" requirement,[60] where EU Member States are prohibited from transferring personal data[61] to any non-EU country that fails to provide "adequate" privacy protection.[62] As a result of this requirement being aimed at receiving countries rather than receiving organizations, the Directive forces these countries to enact broad privacy laws if they desire to continue receiving this information from EU countries.[63] Without such broad legislation, the EU argues that the basic purpose of the Directive, to protect personal information from citizens within the EU community, would be undermined.[64] The EU determines this level of

---

to regulate. *See id.* It is interesting to note that certain industries have successfully regulated personal sensitive information without government encouragement or mandates. *See id.* This has been primarily through recognized privileged relationships such as attorney-client, doctor-patient, and news reporter-source. *See id.* at 199. For more discussion on industry self-regulatory development see *id.* at 198, 199. *See also* Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000).

59. *See* Cody, *supra* note 43, at 1203.

60. *Directive 95/46/EC*, *supra* note 1, at art. 25.

61. Under the Directive, "Personal Data" is defined broadly as "any information relating to an identified or identifiable natural person." *Id.* at art. 2(a). Thus, Personal Data includes more than mere textual information but also photographs, audiovisual images, and sound recordings of an identified or identifiable person. *See* CATE, *supra* note 3, at 36. Additionally, under this definition personal data is protected for any "natural person" rather than just a "living person," meaning that the requirements to protect an individual's private information continues on beyond life. *See id.*

62. *See* Assay, *supra* note 3, at 146. "Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection." *Directive 95/46/EC*, *supra* note 1, at art. 25(1). In his address to the House of Representatives' Subcommittee on Commerce, Trade, and Consumer Protection, David Smith, the Assistant Information Commissioner from the United Kingdom, stated, "What is actually meant by 'adequacy'? It doesn't necessarily require data protection law. It does depend on the nature of the data that are transferred, codes of practice, enforceable codes, and the like, that exist in the country involved." *Hearing*, *supra* note 15, at 15 (testimony of David Smith, Assistant Commissioner, Office of the UK Information Commissioner).

63. *See Directive 95/46/EC*, *supra* note 1, at art. 25(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." *Id.*

64. *See* CATE, *supra* note 3, at 41.

adequacy "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations."[65]

The Directive does, however, provide certain exceptions to the requirement for recipient countries to enact broad privacy laws.[66] Article 26(2) states:

> A Member State may authorize 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.[67]

In response to this provision, a few countries,[68] the U.S. being the first, have accepted "Safe Harbor" provisions as negotiated between the U.S. Department of Commerce and the EU.[69] The Safe Harbor provisions allow companies based within these countries to individually adopt regulatory principles that govern their use of data received from organizations based within the EU countries.[70] As an additional method, the EU has recently approved a standard contractual clause for data transfer to non-EU countries.[71] Approved on June 18, 2001, these contract clauses ensure adequate safeguards for personal data transferred from the EU to countries outside the EU.[72]

---

65. *Directive 95/46/EC, supra* note 1, at art. 25(2).

66. *See id.* at art. 26.

67. *Id.* at art. 26(2). "Controller" is defined in Article 2(d) as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." *Id.* at art. 2(d).

68. Hungary and Switzerland have adopted the Safe Harbor provisions negotiated by the U.S. Department of Commerce. *See Data Protection: Commission Approves Standard Contractual Clauses for Data Transfers to non-EU Countries,* at http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2.htm (last modified June 18, 2001).

69. *See Safe Harbor, supra* note 9, at 45,666.

70. *See id.*

71. The option for the contract clause method is provided in *Directive 95/46/EC, supra* note 1, at art. 26(4), which states, "Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision." *Id.* For more information concerning the contract clauses approved by the European Commission see *Standard Contractual Clauses for the Transfer of Personal Data to Third Countries - Frequently Asked Questions,* at http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm (last modified June 18, 2001).

72. Many feel that the contract clause approach has great merit. *See Data Protection: Commission Approves Standard Contractual Clauses for Data Transfers to non-EU Countries, supra* note 68. The clause approach could be especially useful in allowing companies within the U.S. who do not receive great amounts of information from EU countries to insert the clause in a one-time agreement with an organization based in an EU country. *See id.* The clause

In order to maintain the transfer of data from European nations to U.S. companies, the Department of Commerce initiated negotiations with the EU in 1998.[73] Throughout the negotiations, both the U.S. and the EU were in agreement that levels of U.S. privacy protection needed improvement.[74] Both parties, however, continued to disagree on the nature of the improvement, each holding to their privacy policy approaches.[75] While the EU continued to call on the U.S. to enact federal legislation governing commercial entities' use of personal information transferred from EU Member States, the Department of Commerce continued to hold to its industry self-regulation approach.[76]

---

simply calls for the "Data Exporter" and the "Data Importer" to undertake the transfer process in accordance with the basic protection rules provided for in the Directive. *See id.* Frits Bokestein, the EU Internal Market Commissioner, stated, "This new practical measure will make it easier for companies and organizations to comply with their obligation to ensure 'adequate protection' for personal data transferred from the Community to the rest of the world while safeguarding individuals' right to privacy." *Id.*

This view, however, is not shared by all. In his address to the Subcommittee on Commerce, Trade, and Consumer Protection, Chairman Tauzin expressed his fear that the contracts are merely providing additional protection on top of Safe Harbor for the EU community. *See Hearings, supra* note 15, at 6 (statement by Hon. W.J. "Billy" Tauzin, Chairman, CEC). In his address he stated, "Many experts have suggested that the model contracts will be imposed on U.S. firms as a way to 'top off' or strengthen the Safe Harbor. This seems to directly contradict the purpose of the Safe Harbor and the negotiations that took place. Was the Department of Commerce duped into supporting the Safe Harbor? Are the Europeans really trying to find ways to strengthen the Privacy Directive?" *Id.*

73. *See Safe Harbor, supra* note 9, at 45,666. After the EU found that U.S. information privacy laws failed to meet this adequacy requirement, the EU began negotiations with the U.S. Department of Commerce pursuant to Article 25(5) which states, "At the appropriate time, the Commission shall enter into negotiations with a view of remedying the situation resulting from the finding made pursuant to paragraph 4." *Directive* 95/46/EC, *supra* note 1, at art. 25(5). *See also* Sean D. Murphy, *U.S.-EU "Safe Harbor" Data Privacy Arrangement*, 95 AM. J. INT'L L. 156, 157 (2001).

Interestingly, the U.S. Department of Commerce stays away from the term "negotiation" in its SAFE HARBOR WORKBOOK, *supra* note 2. Instead, the Department states that ". . . [T]he United States initiated *a high-level formal dialogue*, led by the U.S. Department of Commerce' International Trade Administration and the European Commission Directorate for Internal Markets, with the goals of ensuring the free flow of data and effective protection of personal data." *Id.* (emphasis added).

74. *See Safe Harbor, supra* note 9, at 45,667. *See also* Assay, *supra* note 3, at 472. In a statement concerning privacy practices, Representative Mike Doyle noted, "[I]f we in America do not act to establish some general requirements to ensure the integrity of personal privacy for our citizens and global consumers, both Americans and Europeans may very well risk losing out on vast economic opportunities." *Hearings, supra* note 15, at 7 (statement by Hon. Mike Doyle).

75. For a discussion on the EU and U.S. policies on privacy law see *supra* Section II. *See also* SAFE HARBOR WORKBOOK, *supra* note 2.

76. *See* Assay, *supra* note 3, at 147, 48. Throughout the negotiations, the U.S. held to three bottom line issues. *See Hearings, supra* note 15, at 44 (statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP). First, The U.S. was not going to negotiate a treaty or an executive agreement that would apply the Directive in the United States. *See id.* The U.S. was willing, however, to issue guidance to companies within the U.S. on the elements of the Directive. *See id.* In the past the Department of Commerce has issued guidance to help U.S. companies doing business with countries such as China and the Soviet Union. *See*

After submitting five proposals, each rejected by the EU, the EU and the U.S. Department of Commerce finally reached an agreement on March 14, 2000, "The Safe Harbor Agreement."[77] The agreement presented a set of protection provisions to the EU that would allow U.S. companies who comply with Safe Harbor to receive and use personal data from EU Member States by granting a presumption of "adequacy" for purposes of the Directive.[78] The Safe Harbor framework is comprised of seven privacy principles that, when followed, qualify organizations for this protection.[79]

The first principle, "Notice," requires an organization to inform individuals about the purpose for which it collects and uses their personal information.[80] Further, the notice requirement mandates that the organization provide contact information to the individual so that the individual may inquire into the organization's use of the information.[81] This includes allowing the individual to lodge a complaint, inquire as to the types of third parties to which the information may be disclosed, and have opportunities available to limit such disclosure.[82] The notice must be in "clear and conspicuous" language.[83]

Under the second requirement, "Choice," the organization must provide the individual an opportunity to "opt out" of disclosing their information to third parties or to use the information for a purpose other than what was originally authorized by the individual.[84] Again, the option for this choice

---

*id.* Second, the U.S. would not accept European jurisdiction. *See id.* The EU and the U.S. did finally agree to be silent on this issue, but the voluntary self-regulatory scheme of Safe Harbor is under the framework of existing U.S. law. *See id.* Third, in order to adapt the provisions of the Directive to the advanced information economy of the U.S., the U.S. felt that the Safe Harbor principles must be more flexible and address real-world information practices. *See id.*

The EU also had a bottom line position. *See id.* at 44-45. The EU insisted on a high level of privacy protection for European personal data as defined in the Directive. *See id. See also Directive 95/46/EC, supra* note 1, at art. 2(a).

77. *Safe Harbor, supra* note 9, at 45,667. *See also* Assay, *supra* note 3, at 147.

78. *See Safe Harbor, supra* note 9, at 45,666.

79. *See id. See also* SAFE HARBOR WORKBOOK, *supra* note 2. *See also* Murphy, *supra* note 71, at 159.

80. *See Safe Harbor, supra* note 9, at 45,667.

81. *See id.*

82. *See id.*

83. *See id.* Footnote 1 provides an exception where the recipient of the personal information is acting in an agency capacity to the discloser. *See id.* at 45,667, n.1. "It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures." *Id.*

84. *See id.* at 45,667, 45,668. *See also* Assay, *supra* note 3, at 151, 152. *See also* Murphy, *supra* note 71, at 158. This principle ensures that consumers have choices regarding the collection of their personal data. *See* SAFE HARBOR WORKBOOK, *supra* note 2. Under the "Choice" principle, consumers can choose to not have their information shared, have complimentary goods and services market to them, or have their information sold to third parties. *See id.*

must be made to the individual with "clear and conspicuous" language by the organization.[85]

Third, where the organization is transferring personal information to an agency of the organization, it may do so only where the agent has either adopted the privacy principles set out in the Directive or contracted with the organization to adopt adequate privacy policies concerning the information.[86] This "Onward Transfer" requirement provides protection for the organization if, after complying with this provision, the third party agent misuses the information.[87]

The fourth and fifth principles are designed to protect the treatment of the transferred information.[88] The fourth provision, "Security," directs the organization to take reasonable precautions to protect the personal information it uses or disseminates from "loss, misuse and unauthorized access, disclosure, alteration and destruction."[89] Under the fifth principle, "Data Integrity," the organization is required to limit the use of such information only to where it is relevant for its purpose.[90] This provision attempts to minimize the risk that personal information will be misused or abused.[91]

The sixth provision, "Access," requires the organization to allow individuals the opportunity to access their personal information and to grant these individuals the ability to "correct, amend, or delete information where it is inaccurate."[92] The exception to this provision is where the expense of providing access greatly outweighs the risks associated with the individual's privacy or where the rights of a third person would be violated.[93]

Finally, the seventh provision, "Enforcement," states that the privacy protection must have effective enforcement mechanisms in place to ensure compliance with the safe harbor principles.[94] The Safe Harbor Privacy Principles lay out the basic framework for this enforcement requirement:

---

85. *See Safe Harbor, supra* note 9, at 45,668. For certain "sensitive" information, the "opt out" requirement becomes an "opt in" requirement. *See id.* That is, for transfer and use of information such as medical or health conditions, racial or ethnic origin, political opinions, religious beliefs, or information regarding the sexual preferences of the individual, the organization must receive the explicit approval from the individual that the information can be transferred or used. *See id.* As with the requirement of Notice, the agency exception of footnote 1 applies to choice as well. *See id.* at 45,667, n.1.

86. *See id.* at 45,668.

87. *See id.*

88. *See id.*

89. *Id.*

90. *See id.*

91. *See* SAFE HARBOR WORKBOOK, *supra* note 2.

92. *Safe Harbor, supra* note 9, at 45,668. However, according to the SAFE HARBOR WORKBOOK, *supra* note 2, "Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable." *Id.* Additionally, "[t]he sensitivity of the data is also important in considering whether access should be provided." *Id.*

93. *See Safe Harbor, supra* note 9, at 45,668.

94. *See id.*

> At minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference 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.[95]

Under the provisions of the Safe Harbor program, participation in Safe Harbor is completely voluntary, but it is not self-executing.[96] That is, an organization must take the affirmative step and self-certify annually to the Department of Commerce that it adheres to the Safe Harbor requirements.[97] Additionally, an organization must publicly announce their intention to do so.[98] Also, the Department of Commerce recommends that the organization state in its published privacy policy that it adheres to the Safe Harbor requirements.[99] These requirements to qualify for Safe Harbor can be met in one of two ways: an organization may join a self-regulatory privacy program that adheres to the Safe Harbor requirements or it may develop its own self regulatory privacy policy that conforms to Safe Harbor.[100]

## IV. ANALYSIS

On November 1, 2000, the Safe Harbor principles went into effect as the U.S. Department of Commerce began accepting Safe Harbor applications and launched a website dedicated to helping U.S. organizations join the program.[101]

---

95. *Id.* This final provision is divided into three components for safe harbor private sector enforcement: verification, dispute resolution, and remedy. *See* SAFE HARBOR WORKBOOK, *supra* note 2. Organizations are required to have procedures for verifying compliance, to have a dispute resolution system that will investigate and resolve individual disputes, and to remedy problems arising out of a failure to comply with the principles. *See id.*

96. *See* M. Flynn Justice, *Emerging Internet Laws*, 1230 PLI/CORP 123 (2001).

97. *See* SAFE HARBOR WORKBOOK, *supra* note 2.

98. *See id.* The organization's annual self-certification must be in writing and include elements such as notice, choice, access, and enforcement. *See id.*

99. *See id.*

100. *See id.*

101. *See* SAFE HARBOR WORKBOOK, *supra* note 2. The U.S. Department of Commerce developed a website to provide basic information concerning the provisions of the Directive and Safe Harbor, information on how to apply for certification under Safe Harbor, and a list of companies that to date have filed for certification. *See Safe Harbor Overview, at*

Since the date of the compromise, politicians, commerce experts, and corporate directors have been split on their predictions of whether the program would be successful.[102] While many have criticized the Safe Harbor program as providing little incentive for companies to join, others have been quick to stand behind the program and argue that it is a long-overdue unifying bridge between the U.S. and European approaches to data privacy.[103] Some have expressed that the Safe Harbor provisions would collapse as U.S. companies would avoid complying with the unenforceable provisions,[104] while others have expressed great satisfaction in the potential for increased efficiency and higher measure of certainty that the program would grant companies.[105] On October 30, 2000, two days before the opening of the program, one critic of the program, Simon Davies, Director of Privacy International in London, expressed, "It'll fall to pieces within a year because of lack of take-up."[106]

In reaction to these views, the following analysis will show how Safe Harbor has impacted U.S. parties in its first year. Part A of this analysis will address how U.S. companies have reacted to certification. Part B will analyze the benefits and costs recognized by U.S. parties, and Part C will weigh the costs and benefits to determine the impact of Safe Harbor on U.S. companies, U.S. citizens, and U.S. policy in general.

### *A. Review of the First Year: U.S. Companies React to Safe Harbor*

On the opening date of the program, many felt that U.S. companies would be slow to join.[107] To a large degree, this has been true. On February 1, 2001, three months into the program, only twenty companies were on board receiving certification.[108] By May 1, 2001, six months into the program, the number of companies had increased to a mere thirty-nine.[109] The consistent slow growth continued throughout the first year as by August 1, 2001, the number of companies certified under safe harbor had increased only to

---

http://www.export.gov/safeharbor/sh_overview.html (last visited Oct. 26, 2001). *See also* Assay, *supra* note 3, at 147.

102. *See* Sara Fitzgerald, E-Commerce Privacy War, CORPORATE LEGAL TIMES 9(94), pBWB19 (Sept. 1999).

103. *See id.*

104. *See* Assay, *supra* note 3, at 158.

105. *See id.* at 156.

106. Gruenwald, *supra* note 11.

107. *See id.* However, some U.S official expressed hope that 100 companies would sign up in the first month and 1,000 within the first year. *See Microsoft Plans to Sign EU Document*, ASSOCIATED PRESS ONLINE, May 15, 2001.

108. The U.S. Department of Commerce provides a list of companies certified under safe harbor and their dates of certification, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Nov. 1, 2001) [hereinafter *Safe Harbor List*].

109. *See id.*

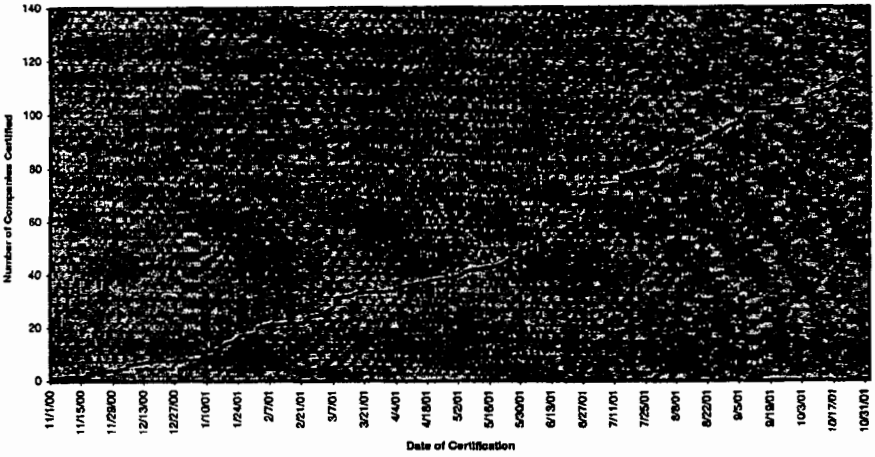
eighty,[110] and by October 31, 2001, at the completion of one full year of the program, the certified total was 124.[111]

---

110. *See id.*

111. *See id.* The following chart, Figure 1, shows the consistent growth trend in companies joining the safe harbor program:

Figure 1: Companies Certified by Safe Harbor




The information used to develop Figure 1 was drawn from the Department of Commerce's Safe Harbor List. *See id.* Figure 1 presents the 124 U.S. companies that have applied for certification under Safe Harbor as of October 31, 2001 with the y-axis representing the total number of companies certified and the x-axis representing their dates of certification. The chart shows a linear trend (consistent growth) over the first year represented by the equation $y = 0.3527x - 15.796$, where time (x) is measured in days, solving for the total number of companies certified (y). Under linear interpretation, it could be estimated that the end of year two (720 days), 239 companies will be certified under the program. A further computation of this equation shows that the Department of Commerce's goal of 1,000 companies certified by the end of year one would not actually occur for seven years and eleven months. *See Microsoft Plans to Sign EU Document, supra* note 107.

This equation, however, does not consider other factors that may drive the trend out of linear growth. First, the idea that more companies will be willing to join as they see more companies become certified, *see* Assay, *supra* note 3, at 158, implies exponential growth, under which, the curve begins a low horizontal line near the x axis (y increases minimally while x increases greatly) until it hits a range where the curve begins to climb. It climbs to where the curve is nearly, but never actually becomes, a vertical line (x increases minimally for a very large increase in y).

If U.S. organizations begin to become more comfortable with Safe Harbor and the growth become exponential, the curve will at some future point return to a consistent linear growth as EU enforcement and industry regulation becomes routine practice. However, for this analysis, there is no way to assess at what point companies will begin applying for certification at a higher rate.

Second, the linear interpretation fails to take into effect other cause-and-effect factors such as EU enforcement (or lack of enforcement), industry international trade situations, and other economic trends. *See* Featherely, *supra* note 160. Any of these factors could effect, likely negatively, U.S. companies' applying for certification. *See id.*

By February 16, three and a half months into the program, only twenty-one companies had applied for certification.[112] One information technology journalist noticed that with the exception of Hewlett Packard Company and The Dun & Bradstreet Corporation, all of the certified companies were small to medium size businesses.[113] It appeared that the larger Fortune 500-type companies were either "investigating their options or taking a wait-and-see approach."[114] As the large U.S. companies were showing their reluctancy to join, many were calling the program an early failure.[115] One member of Congress argued that Republicans and the corporate sector were trying to block privacy measures that have been introduced at both the federal and state levels.[116]

The reluctancy of large companies to join, however, did not last long. By October 31, 2001, the end of the first year of the Safe Harbor program, a number of large corporate entities had been approved for certification.[117] Many of these larger corporations did not join until seven months or more after the start of the program.[118] Just recently, in October 2001, Eastman Kodak, Gateway and Pennzoil-Quaker State sought certification.[119] Thus, it appears that although many larger corporations did not join the program within the first couple of months after its inception, many started joining by the end of the first year.[120]

June 30, 2001 represented the EU's deadline on continued transfer of personal information from EU Member States to U.S. companies that have not been certified for Safe Harbor.[121] Since that date, U.S. companies that are not committed to the Safe Harbor Privacy Principles for "adequate" data protection and are doing business in or receiving personal data from EU Member States risk disruptions in the transfer of such information or prosecution under European privacy laws.[122] In light of these potential harms, Microsoft registered for Safe Harbor in May 2001,[123] followed shortly by other

---

112. *See Safe Harbor List, supra* note 108.

113. *See* Patrick Thibodeau, *HP Embraces U.S.-Europe 'Safe Harbor' Privacy Deal*, COMPUTERWORLD, (Feb. 16, 2001), *at* http://www.computerworld.com/cwi/story/0,1199,NA47_STO57787,00.html.

114. *Id. quoting* Jeff Rohlmeier, a trade official at the Commerce Department.

115. *See Hearings, supra* note 15, at 41 (statement by Rep. Markey). *See also* Shimanek, *supra* note 3, at 476-77.

116. *See id.*

117. *See Safe Harbor List, supra* note 108. The list of larger companies includes Baxter Healthcare, Genetic Technologies, Hewlett Packard, Intel, Microsoft, Pharmaceutical Product Development, Proctor & Gamble, The BMW Group, and The Dun & Bradstreet. *See id.*

118. *See id.* In May 2001, seven months into the program, Intel, Microsoft, Proctor & Gamble, and Baxter Healthcare all applied and were approved for certification. *See id.*

119. *See id.*

120. *See id.*

121. *See Safe Harbor, supra* note 9, at 45,667.

122. *See Microsoft Plans to Sign EU Document, supra* note 107.

123. *See id. See also Safe Harbor List, supra* note 108.

Fortune 500 companies such as Intel and Proctor & Gamble.[124] The addition of these giant, industry-leading firms has not only proven that such companies will adhere to the Safe Harbor principles,[125] but many feel that it was the stepping stone needed for other companies to join.[126]

### *B. Cost/Benefit Analysis of Safe Harbor*

#### *(1) Benefits*

The Safe Harbor program provides benefits for both the U.S. as a whole and for individual U.S. organizations.[127] First, participating with Safe Harbor offers organizations a higher level of certainty and predictability.[128] This is noticed primarily in the presumption of "adequacy" provided to companies certified under Safe Harbor.[129] That is, once certified, an organization will be deemed "adequate" under the EU Directive, thereby binding all fifteen EU Member States, and will continue to receive transfer of data from EU Member States.[130] Under Safe Harbor, these transfers are automatically approved, thereby allowing transfers to process quickly.[131] This also alleviates the administrative burden upon the organization of providing protection on a case-by-case basis.[132] Further, the organization's administration will not need to seek approval from each EU Member State individually.[133] Under Safe Harbor, all fifteen Member States are bound to give a presumption of "adequacy."[134]

Second, organizations certified under the program are provided a "flexible privacy regime more congenial to the U.S. approach to privacy."[135] Companies are provided with the independence of self-regulation coupled with the benefit of a single set of provisions for which to comply.[136] Hewlett Packard Company (HP) recognized this benefit as it was one of the first large

---

124. *See Safe Harbor List*, *supra* note 108.

125. *See* Thibodeau, *supra* note 113.

126. *See id.*

127. *See* Assay, *supra* note 3, at 156.

128. *See* SAFE HARBOR WORKBOOK, *supra* note 2.

129. *See* Assay, *supra* note 3, at 156.

130. *See id. See also* SAFE HARBOR WORKBOOK, *supra* note 2.

131. *See Safe Harbor*, *supra* note 9, at 45,666.

132. *See id.* at 46,667. This decreased burden also works itself into decreased costs. *See* Thibodeau, *supra* note 113. The Dun & Bradstreet Corporation, for example, recognized that it saved a significant amount in legal expenses by gaining a waiver for transfers. *See id. See also* Assay, *supra* note 3, at 156.

133. *See* Rolf Rykken, *Europe's Privacy Directives*, EXPORT TODAY'S GLOBAL BUSINESS, 17(2) at 22 (Feb. 2001).

134. *See id.*

135. *See* SAFE HARBOR WORKBOOK, *supra* note 2.

136. *See* Patrick Thibodeau, *Key U.S. Lawmaker Calls for Review of Europe's Privacy Laws*, COMPUTERWORLD (March 8, 2001) *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58406,00.html.

companies to join the Safe Harbor program, applying for certification on January 23, 2001.[137] Barbara Lawler, the HP Manager of Customer Privacy, stated, "HP believes that self-regulation and credible third-party enforcement . . . is the single most important step that businesses can take to ensure that consumers' privacy will be respected and protected."[138] With regard to Safe Harbor, Ms. Lawler stated, "[I]t's the ultimate 'self-regulatory' approach."[139] In a later interview, speaking on joining Safe Harbor, Ms. Lawler asserted, "If corporations are serious about following the self-regulation approach, rather than having to deal with privacy regulations, then this is what they should be looking at."[140]

This benefit extends beyond individual organizations and reaches the U.S. policy as a whole.[141] Not only has the U.S. Department of Commerce negotiated a regime that will allow U.S. companies to continue receiving private personal data from EU Member States, thus dodging the potentially enormous economic hit valued by many economists as being in the billions of

---

137. *See Hearings, supra* note 15, at 78 (statement of Barbara Lawler, Manager, Customer Privacy, Hewlett-Packard Company). *See also* Thibodeau, *supra* note 113. *See also Safe Harbor List, supra* note 108.

138. *Hearings, supra* note 15, at 78 (statement of Barbara Lawler, Manager, Customer Privacy, Hewlett-Packard Company).

139. *Id.* at 80.

140. Thibodeau, *supra* note 113, *quoting* Barbara Lawler, Hewlett Packard consumer privacy manager.

Some have stated that this freedom to self-regulate balanced with the standard set of policy principles is very similar to the U.S. Better Business Bureau privacy program which is already followed by a number of U.S. businesses, including HP. *See* Rykken, *supra* note 133, at 22. Gerrit de Graaf, the Trade Counselor in the Washington office of the EC, expressed that the Better Business Bureau standards "are in line with the Safe Harbor standards. If your company follows the BBB, you can sign up on Safe Harbor." *Id.* Initiated in 1997, the U.S. Better Business Bureau privacy standards allow companies to join and adopt privacy standards for their consumers' Internet transactions. *See id.* The programs also allow consumers to identify online businesses that are following the standards. *See id.* "BBB*OnLine*'s mission is to promote trust and confidence on the Internet through the BBB*OnLine* Reliability and BBB*OnLine* Privacy programs." BBBOnline, *at* http://www.bbbonline.org (last visited Oct 20, 2001).

The Bureau has two privacy "trustmark" programs with over 11,000 combined participating websites. *See id.* One of these programs, the "Privacy Seal," fully incorporates the requirements of Safe Harbor, providing "Privacy Seal" members with the option of joining Safe Harbor. *See* BBBOnline's Privacy Seal website, *at* http://www.bbbonline.com/privacy/index.asp (last visited Oct. 20, 2001). Posted on the website, "[T]he BBB*OnLine* Privacy Seal fully incorporates the requirements of the US/EU Safe Harbor Agreement, providing BBB*OnLine* Privacy Seal Participants with the ability to enter the EU Safe Harbor. Any company collecting and transferring personally identifiable information from European consumers, or its own European employees, to the US via their website, is required to meet E.U. Data Directive requirements." *Id.* The "privacy seal" program includes "verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component" for members. *Id.* For more information on the Better Business Bureau's "Privacy Seal" program see *id.*

141. *See Hearings, supra* note 15, at 44 (statement by David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP). *See also id.* at 70 (statement by Joel R. Reidenberg, Professor of Law, Fordham University School of Law).

dollars,[142] but in the program's providing the benefits listed above to individual companies, the U.S. policy on self-regulation is actually strengthened.[143] In the conflict between the European and U.S. approaches towards information privacy policies, many felt that the EU's Directive threatened national sovereignty as the EU insisted that its Directive be treated as the de facto global standard.[144] As it is understandable that the EU desires to protect the objectives of the Directive, which are feared to be lost if third countries were not bound by the "adequacy" standards,[145] many feel that the Directive's extraterritorial force upon non-EU countries to either adopt the EU legislation

---

142. *See* Jenab, *supra* note 8, at 650.

143. *See Hearings, supra* note 15, at 44 (statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP). In his address to the Subcommittee on Commerce, Trade, and Consumer Protection, Mr. Aaron stated his belief that Safe Harbor strengthens the U.S. self-regulatory approach by providing a uniform system for all fifty states. *See id.* One of the original goals for the Directive was to develop one market amongst the fifteen EU Member States. *See id.* In the same manner, the Safe Harbor program could provide one market amongst the fifty United States. *See id.*

U.S. policy will continue to be strengthened by Safe Harbor if Safe Harbor proves effective. *See* Assay, *supra* note 3, at 158. Many feel that this will show itself true as more large companies come aboard. *See* Thibodeau, *supra* note 113. *See also* Karen Dearne, *Privacy Threatens EU Trade*, THE AUSTRAILIAN, May 22, 2001, at 25.

144. *See Hearings, supra* note 15, at 5 (statement of Hon. W.J. "Billy" Tauzin, Chairman, CEC). In his address to the Subcommittee, Chairman Tauzin stated:

> I believe that the EU Privacy Directive may act as a de-facto privacy standard on the world . . . [I]t certainly is an effort to impose the EU's will on the U.S. While I recognize that similar charges have been laid against certain U.S. policies, the EU Privacy Directive could be the imposition of the one of the largest free trade barriers ever seen and is a direct reversal of the efforts we have made in various free trade agreements. It certainly provides for extraterritorial enforcement of EU principles on Americans and American companies.

*Id.* at 5-6. The Chairman further stated, "I have serious reservations about the real impact of the EU Privacy Directive on commerce and trade. I am very concerned that U.S. companies, which have been the creators and the leaders of E-commerce, will be forced to deal with such a restrictive concept." *Id.* at 6.

In 1996, Congress enacted the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996, 22 U.S.C. § 6021, commonly referred to as The Helms-Burton Act, in an attempt to protect the property rights of American citizens whose property was confiscated without compensation by the Castro regime. *See id.* The Act imposed sanctions on those who profited off the stolen property. *See id.* In its response to the act the EU issued the following statement: The European Union is opposed to the use of extraterritorial legislation, both on legal and policy grounds. In the last few years there has been a surge of U.S. extraterritorial sanctions legislation [both at federal and sub-federal level]. Such laws represent an unwarranted interference by the U.S. with the sovereign rights of the EU to legislate over its own citizens and companies, and are, in the opinion of the EU, contrary to international law.

*Hearings, supra* note 15, at 47 (statement by Jonathan M. Winer, Counsel, Alston and Byrd LLP). For more on the topic of the EU overreaching its power see Thibodeau, *supra* note 136.

145. *See Hearings, supra* note 15, at 66 (testimony of Joel R. Reidenberg, Professor of Law, Fordham University School of Law). "I would disagree with the assessments that this is an extraterritorial application of European law, because I think that it is the European Union saying, 'If it is European origin data, we want to be sure that our local privacy rules are not circumvented oversees.'" *Id.*

or face the consequences is over reaching their rights.[146] Therefore, the fact that the U.S. came out of the negotiations maintaining its self-regulatory approach, refraining from enacting broad legislation, and implementing a program that has proven beneficial in giving more guidance and uniformity to individual industry self-regulatory standards has led the U.S. to a stronger overall policy.[147]

Third, claims that are brought by citizens of EU Member States against organizations certified under Safe Harbor against the organization's use or transfer of personal information will be heard in the U.S., subject to limited exceptions.[148] Enforcement of these claims will be carried out in accordance with U.S. law, primarily by the private sector.[149] This private sector self-regulation and enforcement is backed by federal and state unfair and deceptive statutes.[150]

Finally, organizations certified under Safe Harbor may recognize increased consumer confidence and approval as the concern of personal privacy issues continues to grow.[151] In her statement to the Subcommittee on Commerce, Trade and Consumer Protection, Ms. Lawler asserted, "We believe that consumer confidence will be enhanced by ensuring customer privacy rights on- and off-line in a global commerce environment. E-commerce will grow faster if consumer confidence is reinforced by company efforts to ensure consumers have an effective recourse for privacy complaints through agreements like the Safe Harbor."[152]

---

146. *See id.* at 6 (testimony of Hon. W.J. "Billy" Tauzin, Chairman, CEC). Chairman Tauzin stated, "I must admit that I take a dim view about the way the EU went about enacting this new privacy regime. The EU designed the rules and told the U.S. companies to abide by them or risk losing the transfer of any data from European nations. In essence, do it or suffer the consequences." *Id.*

147. *See Hearings, supra* note 15, at 44 (statement by David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP). *See also id.* at 70 (statement by Joel R. Reidenberg, Professor of Law, Fordham University School of Law).

148. *See* Thibodeau, *supra* note 136.

149. *See Safe Harbor Overview, supra* note 101.

150. *See id.*

151. *See* Assay, *supra* note 3, at 156. A recent company to apply for certification under Safe Harbor, Agilent Technologies, Inc., capitalized on this benefit. *See Agilent Technologies Signs U.S./Europe Safe Harbor Agreement to Promote Data Privacy: Framework Enhances Protection of Personal Data Transmitting from European Union Countries* (Oct. 4, 2001), *at* http://www.agilent.com/about/newsroom/presrel/2001/04oct2001a.html. In an October 4, 2001 interview, Agilent's director of customer privacy, Jim Allen, was quick to point out "Agilent places the highest priority on customer privacy." *Id.* Mr. Allen further stated, "Our company's global privacy policies are consistent with the European Union's principles for data protection, so our signing the safe harbor agreement is a logical next step in our commitment to customer privacy. In signing this critical agreement, we want to reassure our European customers that we treat their data in the most ethical manner." *Id.*

152. *Hearings, supra* note 15, at 79 (statement of Barbara Lawler, Manager, Customer Privacy, Hewlett-Packard Company).

*(2) Costs*

That is not to say, however, that there are no costs associated with an organization's certification under the Safe Harbor principles. First, certification may require that the organization make significant changes to its information practices.[153] Second, upon certification, the organization runs into an immediate decision of whether to provide the privacy protection to only EU citizens, as required, or whether it should extend the protection to U.S. consumers as well.[154] Either way, the organization is likely to meet additional costs and work itself into a couple of additional problems.[155] First, as a matter of good business practice, it may not be in the best interest of the organization to deny equal protection to U.S. consumers.[156] To do otherwise would be to treat the citizens of one's own country as second-class to EU citizens.[157] However, in granting the protection, the company risks lost transactions.[158] Additionally, in embracing more than one standard, the organization enters the difficult task of managing more than one level of protection and enforcement associated with different standards.[159]

Third, there are costs associated with implementing enforcement mechanisms to investigate and verify consumer complaints.[160] Finally, the organization has potential liabilities that it may incur if it fails to fulfill its obligations under the Safe Harbor provisions.[161] These liabilities could take the form of negative publicity campaigns, requirements to delete information or provide compensation for losses incurred, potential "delisting" where the organization continues to fail to comply, and potential liability for

---

153. *See* Assay, *supra* note 3, at 156. These changes may require employee education and/or technical improvements. *See id.*

154. *See id.*

155. *See id.*

156. *See id.*

157. *See id. See also Safe Harbor, supra* note 9, at 45,666. This has been a trouble point of the Directive since its inception. *See* Assay, *supra* note 3, at 156. If a U.S. organization complies with the elements of the Directive through the Safe Harbor Principles, it is in effect required to provide a higher level of privacy protection to citizens of foreign countries than it is required to provide to citizens of the U.S. *See id.*

One expert noted, "American law and practice allows those same companies to provide far less protection, if any, to data about American citizens. This is a particularly troubling aspect of US [sic] opposition to the European Directive's standards." *Hearings, supra* note 15, at 71 (statement by Joel R. Reidenberg, Professor of Law, Fordham University School of Law). He further asserted, "In effect, the proliferation of European style data protection measures around the world means increasingly that American citizens will be left with second class privacy in the United States and afforded greater privacy protection against American companies outside the US [sic] borders." *Id.*

158. *See* Assay, *supra* note 3, at 156.

159. *See id.*

160. *See id.*

161. *See id.*

misrepresentations made to the public and/or the government in its certification letters.[162]

### C. *Safe Harbor's Impact on U.S. Companies, U.S. Citizens, and U.S. Policy*

In the nature of a compromise, both the EU and the U.S. gained some benefit at some cost in their agreement to accept the Safe Harbor program.[163] U.S. companies, for example, would have preferred Safe Harbor principles that would be words without effect, leaving them free to maximize their autonomy to profit from the use of personal data.[164] The EU, on the other hand, would have preferred that the U.S. abandon its self-regulatory system and enact broad-privacy laws in accordance with the Directive's standards.[165] As a result of the compromise, however, the Safe Harbor provisions bind U.S. companies certified under the program to the standards set out in the Directive, securing the EU's chief objective,[166] but they also protect U.S. companies' autonomy to self-regulate and the U.S. government from being required to enact broad-privacy legislation, thus, securing the U.S.'s key objective.[167] With respect to the benefits and costs listed in the proceeding section, the following analysis will measure the impact of the Safe Harbor program on U.S. companies, U.S. citizens, and U.S. policy in general.

As its primary loss, U.S. companies lost ground on their ability to maximize profits from the use of personal information gathered from EU Member States.[168] However, to date, it is not clear that U.S. companies are reaping this effect.[169] In a recent study conducted by Anderson Consulting, American companies doing business oversees electronically failed to implement many of the minimum data privacy protections laid out in the Safe Harbor Principles.[170] Of seventy-five Fortune 500 and medium-sized companies polled,[171] none of the companies had privacy policies that met even six of the seven Safe Harbor Principles and only two of the companies had

---

162. *See id.*

163. For more discussion on the benefits and costs associated with Safe Harbor see Assay, *supra* note 3, at 156.

164. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 75 (Winter 2000).

165. *See id.*

166. *See id.*

167. *See id.*

168. *See id.*

169. *See* Kevin Featherly, *U.S. Companies Don't Make 'Safe Harbor' Privacy Grade – Study*, NEWS BYTES NEWS NETWORK, Aug. 16, 2001.

170. *See id.*

171. The seventy-five companies have a combined total of 1.7 trillion in annual revenues. *See id.*

policies that met five of the principles.[172] Enforcement was found to be the least complied with principle with only five percent of companies maintaining procedures to assure compliance while describing recourse for individuals whose privacy is breached.[173] However, the study also showed that the EU has been very slow to enforce the provisions of its Directive, let alone the principles of the Safe Harbor program.[174]

Therefore, from a U.S. company's prospective, not much has changed, as for the most part companies are not substantially changing their privacy policies.[175] This could change quickly if the EU decides to increase its enforcement against U.S. companies.[176] However, even if the EU does increase enforcement, it is still unclear as to the degree they will enforce the principles and whether the degree of force shown will lead U.S. companies to apply for certification.[177]

With respect to U.S. citizens, it has been argued that in initiating the Safe Harbor program, U.S. consumers may be treated as "second class citizens within their own country"[178] as U.S. companies will be required to provide a higher level of privacy protection to citizens of EU Member States than to U.S.

---

172. *See id. See also* Safe Harbor, *supra* note 9, at 45,666.

173. *See* Featherly, *supra* note 169. Of the other principles, the Anderson study showed that twenty-five percent of the companies passed the Notice standard, eighty percent passed the Choice standard, forty-six passed Security, seventy-four passed Data Integrity, and thirty-four passed Access. *See id.* Of the industries polled, the financial services firms were highest in the choice standard (opt-in and opt-out), but lagged on data integrity and security; the retail industry was the worst at providing notice and access, but faired well in data integrity, choice security; the telecom/media/entertainment industry proved worst among all sectors, but scored highest in data integrity. *See id.*

174. *See id.* Although they have not acted upon their authority, the EU can begin enforcement and potentially block data transfer to U.S. companies that do not meet the Directive's requirements at any moment it desires. *See Directive 46/95/EC*, *supra* note 1, at art. 25(3). Many broad privacy law advocates are calling the EU and the United States to begin enforcing the Safe Harbor provisions in an attempt to force U.S. companies to comply with Safe Harbor. *See Hearings, supra* note 15 at 3 (statement of Rep. Towns, CEC). In a call for the United States to begin such enforcement, Representative Towns stated, "[A]ny privacy policy is meaningless unless it is enforceable. Therefore, government has an important part to play in making privacy enforceable." *Id.*

In addressing this enforcement concern, the Chairman of the Committee on Energy and Commerce stated, "Compliance and enforcement of the Privacy Directive has, at best, been spotty in European Nations . . . Given this, we need to know whether enforcement of the Privacy Directive on U.S. companies represent a double standard when compared to enforcement of European firms. We also need to know the consequences for competition if this occurs." *Id.* at 6 (statement by Hon. Tauzin, Chairman, CEC).

175. *See* Featherely, *supra* note 169.

176. *See id.*

177. *See id.*

178. Assay, *supra* note 3, at 156. *See also Hearings, supra* note 15, at 71 (testimony by Joel R. Reidenberg, Professor of Law, Fordham University School of Law). Professor Reidenberg expresses his concern that the Directive makes American citizens "second-class citizens in the privacy world." *Id.* For additional information on U.S. citizens being granted a lower level of privacy protection than EU citizens see *supra* note 157.

citizens.[179] Thus far, however, this has not shown to be the case. First, as U.S. companies are becoming certified under Safe Harbor and applying its seven principles, they are finding it more difficult to keep multiple databases to distinguish EU citizens from U.S. citizens than to merely apply equal privacy policies across the board to all consumers.[180] Second, most U.S. companies complying with the Safe Harbor principles are finding the "good business" factor of providing higher levels of privacy beneficial to their public image.[181] Therefore, due to individual companies analyzing the costs and benefits associated with applying the Safe Harbor principles to U.S. citizens and finding that it is more beneficial for them to grant U.S. citizens an equal level of protection, U.S. citizens are gaining protection and assurance under Safe Harbor.[182]

With respect to U.S. policy, many feel that the U.S. lost a piece of its ultimate sovereignty by compromising with the Safe Harbor principles in that, under Safe Harbor, the Department of Commerce and the Federal Trade Commission have the responsibility of providing overall enforcement on the principles as originally laid out in the Directive.[183] While the U.S. may have conformed to certain provisions of the Directive, the U.S. refrains from enacting broad legislation under the compromised framework.[184] If the U.S. would have adopted broad legislation, it would have fallen at the feet of what many consider an economic threat from the EU.[185] However, the compromise allowed the U.S. to maintain its self-regulatory approach, leaving for the most

---

179. *See* Assay, *supra* note 3, at 156.

180. *See id.*

181. *See Microsoft Plans to Sign EU Document*, *supra* note 107. In reaction to this concern, Microsoft has called Safe Harbor its "floor" for data protection company-wide and that the principles will be provided equally to citizens of all countries. *See id.*

182. *See id.*

Not discussed in the analysis, EU citizens will also be impacted by the issuance of Safe Harbor. *See Hearings*, *supra* note 15, at 44 (statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP). It is interesting that it is these individuals who were originally intended protection under the Directive, and yet, from their perspective it is unclear whether the Directive, let alone Safe Harbor, is succeeding at all. *See id.* A primary reason for this is the EU's lack of enforcement of the Directive in EU Member States. *See id.* If the EU were to step up enforcement, EU citizens may consider the protection as a benefit but may find the scale-back of U.S. companies offering services and products within their own country as too great a cost. *See id.* As the EU begins enforcing the Safe Harbor principles and finding certain U.S. companies as failing to provide "adequate" levels of privacy protection, European communities risk both long term economic loss as some companies will pull out of the European market altogether instead of revising their privacy policies and short term loss as companies will have to temporarily pull out of the market to update and revise their standards. *See id.* One expert noted, "[T]his could hurt Europe as much as it would the United States." *Id.*

183. *See* Shaffer, *supra* note 164, at 75.

184. *See Hearings*, *supra* note 15, at 6 (testimony of Hon. W.J. "Billy" Tauzin, Chairman, CEC).

185. *See id.*

part, the government out of industry privacy control.[186] Instead of initiating broad-privacy laws to which organizations must comply, the U.S. maintained its stance that individual organizations can choose whether to comply in light of the costs and benefits it will incur.[187] Although the Safe Harbor Principles are an alteration from the U.S. position before the compromise, the program upholds the foundational bedrock of U.S. commerce in promoting industry self-regulation.[188]

## V. CONCLUSION

In light of the two opposing approaches on data privacy protection, it is not surprising that the enactment of the Directive instigated great concern in the U.S. Where the European "fundamental rights" approach is geared towards broad legislative privacy law,[189] the U.S. has historically maintained a government "hands off" approach toward the private sector.[190] Instead, The U.S. encourages industry self-regulation on data privacy matters.[191] The Directive's calling for countries outside of the EU to enact broad information privacy laws that comply with its "adequate" privacy standard was quite over-reaching, threatening the U.S. to abandon its long standing position on privacy policy.[192]

The negotiated compromise of the Safe Harbor Privacy Principles[193] has not only allowed the U.S. to maintain its historical approach towards data privacy, but it has actually strengthened the approach.[194] Safe Harbor provides industries with guides and standards on privacy protection, allowing them to maintain efficiency in data transfer from EU Member States,[195] grants U.S. citizens a higher level of protection, assurance, and knowledge,[196] and maintains the foundational principles of U.S. policy.[197] Companies who come

---

186. *See id.* at 44 (statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP).

187. *See* Assay, *supra* note 3, at 156.

188. *See id.*

189. *See Directive 95/46/EC*, *supra* note 1, at art. 1. For more on the European "fundamental right" privacy approach see *supra* note 17.

190. *See* CATE, *supra* note 3, at 36.

191. *See id.*

192. *See Hearings*, *supra* note 15, at 6 (testimony of Hon. W.J. "Billy" Tauzin, Chairman, CEC).

193. *Safe Harbor*, *supra* note 9, at 45,666.

194. *See Hearings*, *supra* note 15, at 44 (statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP).

195. *See* SAFE HARBOR WORKBOOK, *supra* note 2. *See also* Assay, *supra* note 3, at 156.

196. *See Hearings*, *supra* note 15, at 78 (statement of Barbara Lawler, Manager, Customer Privacy, Hewlett-Packard Company). *See also* SAFE HARBOR WORKBOOK, *supra* note 2.

197. *See Hearings*, *supra* note 15, at 78 (statement of Barbara Lawler, Manager, Customer Privacy, Hewlett-Packard Company).

under Safe Harbor become more efficient in their application and development of individual regulatory systems.[198]

An ultimate deciding factor on whether Safe Harbor succeeds will be how the EU chooses to enforce the program.[199] To date, the EU has been slow to enforce Safe Harbor, let alone the Directive in general.[200] It appears, however, that the EU is ready to begin enforcement of the provisions and may do so soon.[201] U.S. companies, on the other hand, have shown interest in the program and will likely continue to come aboard. [202] In light of its first year, Safe Harbor is proving successful in providing a higher level of protection over the use and transfer of individual's personal information while maintaining the capitalistic nature of the U.S. economy.

*David A. Castor**

198. *See id.*

199. *See Hearings, supra* note 15, at 44 (statement of David L. Aaron, Senior International Advisor, Dorsey & Whitney LLP).

200. *See id. See also* Featherely, *supra* note 160.

201. *See Hearings, supra* note 15, at 6 (testimony of Hon. W.J. "Billy" Tauzin, Chairman, CEC).

202. *See* Safe Harbor List, *supra* note 108.

* J.D. Candidate, 2002, Indiana University School of Law-Indianapolis; 1997 graduate of Purdue University. The author would like to thank his beautiful wife, Sarah, who is a constant reminder of the joy we can have in Christ.