A SAFETY NET IN THE E-MARKETPLACE: THE SAFE HARBOR PRINCIPLES OFFER COMPREHENSIVE PRIVACY PROTECTION WITHOUT STOPPING DATA FLOW

William J. Kambas[*]

I. INTRODUCTION 150
II. A BRIEF CHRONOLOGICAL DEVELOPMENT OF COMPREHENSIVE CONSUMER PRIVACY PROTECTION 151
III. A GOOD START: THE FAIR INFORMATION PRACTICE PRINCIPLES AND THE OECD GUIDELINES 155
A. *FIPP* 155
1. OECD Guidelines 157
2. Limitations of the FIPP and OECD Guidelines 160
3. The E.U. Data Directive: in harmony with the FIPP and OECD Guidelines 161
4. A Bridge: The Safe Harbor Principles 163
IV. SAFE HARBOR PRINCIPLES: A SAFETY NET FOR THE PROTECTION OF CONSUMER PRIVACY 164
1. The Creation Of The SHP 165
2. The Substance of the SHP 165
3. Implementation of the SHP in the U.S. 170
V. PENDING QUESTIONS: CRITICISM OF THE SAFE HARBOR PRINCIPLES 171
1. Does the SHP offer sufficient protection? 171
2. Is There Protection From Discrimination? 172
3. Does the E.U. Gets Greater Protection Than U.S.? . 172
4. Does the SHP Lack Enforcement and Accountability? 173
VI. SHARING THE BURDEN: TECHNOLOGIES THAT ENHANCE THE EFFECTIVENESS OF THE SAFE HARBOR PRINCIPLES 176
1. Developments in the E-Marketplace: Giving The Consumer Tools To Survive 176
2. Code: Creating The Need For Protection 176

* J.D./M.B.A., University of Connecticut, expected 2003; B.A., Skidmore College, 1996. The author would like to thank Professor Paul Schiff Berman, University of Connecticut School of Law. Professor Berman not only provided guidance, but also encouraged a belief in and respect for academic dialogue.

3. For The Do-It-Yourself'ers: Privacy And Data Protection Technology 178
VII. THIRD PARTIES TO THE RESCUE: PROVIDING KNOWLEDGE AND KNOW-HOW TO CONSUMERS 181
VIII. CONCLUSION 182

I. INTRODUCTION

In May of 2000, the FTC, under Chairman Robert Pitofsky, concluded that industry self-regulation was not effective in protecting consumer privacy and in a report to Congress the FTC expressed the view "that legislation [was] necessary to ensure further implementation of consumer data protection devices."[1] At the same time, the U.S. Department of Commerce ("DOC") and the European Commission jointly developed the so-called Safe Harbor Principles ("SHP").[2] The Safe Harbor Principles signify mutual agreement regarding basic and internationally accepted principles for the protection of consumer privacy.

On October 4, 2001, the Federal Trade Commission ("FTC") announced that it has changed its course.[3] Chairman, Timothy Muris, shifted the FTC's position and stated that it is still "to soon" to "fashion workable legislation"[4] and the that FTC would instead concentrate on the enforcement of existing privacy laws. In so doing, Muris has abandoned three important steps to creating comprehensive consumer privacy protection. These steps were: First, the FTC's Fair Information Practice Principles ("FIPP"); Second, the Organization for Economic Cooperation and Development's Privacy Guidelines (the "OECD" and the "OECD Guidelines"); and lastly, the FTC's latest move backs away from the recent culmination of comprehensive privacy protection guidelines as established by the SHP (as referenced above). Although there has been some criticism about the effectiveness of comprehensive international privacy protection standards, the SHP are a logical and rational progression in consumer privacy protection.

In this article, I will argue that the SHP mark significant progress over the FIPP and OECD Guidelines (despite the fact that they are currently limited to the protection of European Union citizens). Further, I will discuss why criticism

---

1. FEDERAL TRADE COMM'N, *Privacy Online: Fair Information Practices In The Electronic Marketplace, A Report To Congress* (May 2000) *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

2. The SHP was developed by the U.S. Department of Commerce in consultation with the European Commission and became effective November 2000.

3. Timothy Muris, Remarks at the Privacy 2001 Conference (Oct. 4, 2001) *at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

4. *Id.*

surrounding the SHP, in particular concerns about its enforceability, is misplaced, or at least premature. Rather, when combined with emerging technologies and services, the SHP help level the playing field between consumers and data collectors and provide a safety net that will benefit both. Lastly, because of the strengths of the SHP, they should serve as a model for comprehensive US legislation. The 106th Congress considered numerous privacy bills and 107th has continued with those efforts. The SHP offer a valuable model.

The time is right for comprehensive consumer privacy protection. There is considerable evidence that the e-marketplace recognizes the benefits of collecting consumer data and is taking steps to maximize its unhindered use of consumer information. Consider the brief example of Amazon.com's August 2000 privacy policy amendment. Amazon.com now "classifies customer information as a business asset, and is transferable to third parties if Amazon or one of its business units is sold. Previously, the company promised its customers that it would not sell, trade or rent personally identifying consumer data."[5] Although European consumers are still protected from un-consented to transfers,[6] non-E.U. citizens are not protected. Amazon.com's rationale behind this move is that "such restrictions on data-sharing would impede its budding partnerships."[7] Although this type of corporate discretion may allow for added commercial conveniences, fundamental rights are at issue and the consumer must be a willing and informed participant.

II. A BRIEF CHRONOLOGICAL DEVELOPMENT OF COMPREHENSIVE CONSUMER PRIVACY PROTECTION

There is little question that consumers need privacy protection.[8] Privacy is an important part of an effective society. It is necessary for participatory governance[9] and is a basic right of citizens in a democratic state.[10] Further,

---

5. Keith Perine, *Privacy Centers Have Their Eyes on Amazon*, THE INDUST. STAND. Dec. 4, 2000, *at* http://www.thestandard.com/article/display/0,1151,20586,00.html; *see also* http://www.amazon.com/exec/obidos/tg/browse/-/468496/107-6133111-3237344.

6. The E.U. Data Directive restricts transfers that are made without the consent of the data subject. EUA. PARL. DIR. (95/46/EC) (Oct. 24, 1995) *at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en 395L0046.html.

7. *See* Amy Borrus, *Online Privacy: Congress Has No Time To Waste*, BUS. WK., Sept. 18, 2000, at 54.

8. The United States Federal Trade Commission (FTC) states on the webpage for Privacy Initiatives that "as personal information becomes more accessible, each of us - companies, associations, government agencies, and consumers - must take precautions to protect against the misuse of that information." http://www.ftc.gov/privacy/index.html; *see also* Federal Trade Commission *supra* note 2.

9. *See* Spiros Simitis, *Reviewing Privacy In An Information Society* 135 U. PA. L. REV. 707 at 732 (1997).

10. Jed Rubenfeld, *The Right Of Privacy* 102 HARV. L. REV. 737 (1989).

consumers themselves are concerned with privacy. An October 1999 survey indicated that 72% of internet users in the United States, Germany, and the United Kingdom were "very" concerned about personal privacy, another 20% were "somewhat" concerned.[11] Forrester Research estimated that, in 1999 alone, 2.8 billion dollars of internet related transactions were lost due to consumer concerns about privacy.[12]

Concerns for consumer privacy have not gone ignored. Privacy has sometimes been recognized as an individual's fundamental right or as a constitutive value that helps form individual identities or social consensus.[13] Although numerous legislative and private industry efforts have been undertaken, few have been successful in adapting to changes in society, in particular, the changes brought by the internet.

The FTC articulated its FIPP in 1998 report, *Privacy Online: A Report to Congress*. The FTC was responding to a concern about "privacy" and the effectiveness of "self-regulation."[14] The FTC revisited the FIPP in May of 2000,[15] and, perhaps attesting to the importance of fair information practices, the FTC re-endorsed the FIPP and offered renewed support.

As the FIPP were being developed, the OECD, an international working to "co-ordinate domestic and international policies,"[16] began work on privacy

---

11. *IBM Multi-National Consumer Privacy Survey* (Oct. 1999) at 72. This report was prepared by Louis Harris & Associates Inc., *available at* http://www.ibm.com/services/files/privacy_survey_oct991.pdf; *see also* Electronic Privacy Information Center (EPIC): Public Opinion on Privacy *at* http://www.epic.org/privacy/survey.

12. Forrester Research, Inc., *The Internet's Privacy Migraine*, (May 2000) *at* http://www.forrester.com/ER/Research/Report/Excerpt/0,1338,9363,FF.html.

13. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) establishes a fundamental right of privacy through the First, Third, Fourth, Fifth, and Fourteenth Amendments of the U.S. Constitution. This right to privacy is also recognized in the European Union's Data Directive, 95/46/EC which was established to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy." Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995, Article 1, ¶ 1 *available at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en 395L0046.html. *See also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996). Paul Schwartz, a leading scholar in privacy law, has characterized "information privacy as a constitutive value that helps both to form the society in which we live in and to shape our individual identities" and that the "State has a special role in two areas: (1) creating and maintaining conditions for a functioning privacy market, and (2) developing privacy norms that prevent access to personal information that would cause too great a rate of preference falsification in society." Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 816-17 (2000).

14. *See* Federal Trade Commission, *Privacy Online: A Report To Congress*, Executive Summary *available at* http://www.ftc.gov/reports/privacy3/exeintro.htm#Executive Summary.

15. Federal Trade Comm'n, *supra* note 2.

16. "The OECD consists of Australia (1971), Austria (1961), Belgium (1961), Canada (1961), Czech Republic (1995), Denmark (1961), Finland (1969), France, (1961), Germany (1961), Greece (1961), Hungary (1996), Iceland (1961), Ireland (1961), Italy (1961), Japan (1964), Korea (1996), Luxembourg (1961), Mexico

guidelines to facilitate the creation of privacy policies by governments, businesses, individuals, and law enforcement officials.[17] The OECD Guidelines were promulgated on September 23, 1980 in the *OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data*[18] and purport to "represent an international consensus on how best to balance effective privacy protection with the free flow of personal data."[19]

Both the FIPP and the OECD Guidelines provide guidance to legislative efforts and the development of private sector privacy policies.[20] However, despite the fact that both the FIPP and OECD Guidelines have withstood the tests of time, the e-marketplace is still void of effective consumer privacy protection.

Following the development and acceptance of the FIPP and OECD Guidelines, the European Union adopted Directive 95/46/EC Of The European Parliament And Of The Council Of 24 October 1995 On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data.[21] The E.U. Data Directive were enacted in October 1995 and went into effect in October 1998. It affirmatively established standards for the protection consumer data and privacy in an effort to promote the free flow of information between member nations. Not only does the E.U. Data Directive create a standard to serve as the common law between member nations, but it also prohibits the transfer of information from one of those countries to any third party without adequate privacy protections in place. It requires that those who wish to use consumers' personal data must provide "an adequate level of protection" for that personal data.[22] Thus, any party interested

---

(1994), The Netherlands (1961), New Zealand (1973), Norway (1961), Poland (1996), Portugal (1961), Spain (1961), Sweden (1961), Switzerland (1961), Turkey (1961), United Kingdom (1961), and United States (1961). The goals of the OECD are to promote "an open market economy, democratic pluralism and respect for human rights." Interestingly, in addition to developing guidelines, the 29 member nations have also "agreed to participate in the exercise ... called "peer review", which is based on transparency, explanation, and, when needed, self-criticism by the countries examined." OECD Online, About: Membership *at* http://www.oecd.org.

17. *See* http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

18. *See O.E.C.D. Doc. C58 (final)(Oct. 1, 1980), reprinted in 20 I.L.M. 422 (1981) available at* http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

19. *O.E.C.D. Doc. C58 (final)(Oct. 1, 1980), reprinted in 20 I.L.M. 422 (1981) available at* http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

20. TRUSTe, a "leader in promoting privacy policy disclosure, informed user consent, and consumer education", has established its privacy protection practices "based on long-standing principles of fair information practices as interpreted by the U.S. government." http://www.truste.com/about/about_whitepaper.html.

21. EUR. PARL. DIR., *supra* note 6.

22. *Id.*

in collecting personal data from citizens of European Union member nations must comply with the comprehensive standards of the E.U. Data Directive.

In this era of increasing globalization, international harmony is necessary. Recognizing this, the U.S. Department of Commerce ("DOC") and the European Commission jointly developed standards meant to enable U.S. businesses to meet the requirements of the E.U. Data Directive. The so-called Safe Harbor Principles ("SHP")[23] were developed to facilitate international commerce by creating a bridge between the E.U. Data Directive and U.S. practices. Additionally, by creating means for compliance with the E.U. Data Directive, the SHP attempted to ensure the fundamental right of privacy and security of personal data. The SHP require that consumers be notified of actions to collect data, be provided the opportunity to withhold information, be offered the chance to review and correct collected information, and be assured of security measures and redress in case of abuse.

This is a valuable step toward comprehensive consumer privacy protection because consumers become active participants in the transfer of their personal data. The SHP are flexible enough to adjust to changing times and changing preferences, consistent with the current trend of "mass-customization." As Professor Anita L. Allen-Castellito points out, "imposing privacy norms to make sure everyone lives in accordance with a particular vision of privacy-would be problematic."[24] Consistent with a liberal conception of private choice,[25] the SHP provide for choices crucial to a successful privacy regime. Further, by providing a comprehensive approach to consumer privacy and data protection, the SHP avoid some of setbacks other efforts have suffered.[26]

---

23. The SHP was developed by "the U.S. Department of Commerce in consultation with the European Commission" and became effective November 2000.

24. Anita L. Allen, *Coercing Privacy*, 40 WM & MARY L. REV. 723, 729 (1999).

25. *See generally* Allen, *Coercing Privacy*, 40 WM & MARY L. REV. 723. Professor Allen describes the liberal conception of private choice as "the idea that government ought to promote interests in decisional privacy, chiefly by allowing individuals...to make many, though not all, of the most important decisions..." *Id.* Privacy and private choice are "indispensable, foundational goods." *Id.* Further, although Professor Allen encourages choice, she argues that some people must be coerced into privacy. This is problematic, as pointed out by Neal Devins in *Reflections on Coercing Privacy*, 40 WM & MARY L. REV. 795 (1999). The Safe Harbor Principles strike a balance by giving subjects choice while requiring responsible use and protection of personal information on collectors. Therefore, although one consumer may wish to give up as much data as practical, that data will not color the use of another subject's data.

26. A recent agreement between the Federal Trade Commission and leading online advertisers (including Doubleclick and Engage) pledged to give consumers choice "about when such companies can snoop on their Web-surfing habits." The agreement was easily side stepped by Pharmatrak, Inc., a specialized consulting firm, that is not an "advertiser" but helps drug companies compare and improve their websites. The data collection is "invisible to consumers unless their browsers are specifically set up to alert them when such "bugs" are being used." Marcia Stepanek, *Surf At Your Own Risk*, BUS. WK., Oct. 30, 2000, at 143.

III. A GOOD START: THE FAIR INFORMATION PRACTICE PRINCIPLES AND THE OECD GUIDELINES

A. FIPP

As privacy legislation matured in the 1970's, the FTC compiled principles that would serve as guidance in the protection of consumer privacy. These were not enacted into law; rather, they were a distillation of existing legislation.[27] The FIPP focuses on five issues: 1) Notice/Awareness; 2) Choice/Consent; 3) Access/Participation; 4) Integrity/Security; and 5) Enforcement/Redress.[28] These elements encourage consumer involvement in the data collection process. They keep consumers in the loop and keep them informed of potentially invisible practices while facilitating consumers' ability to choose whether or not they wish to share their personal data. As Professor Schwartz has stated, "fair information practices are the building blocks of modern information privacy law."[29]

The First principle of the FIPP is notice. Notice is the element that makes the other elements – choice/consent, access/participation, and enforcement/redress – possible. While the nature of the notice may vary depending on what is collected, the FIPP state that data subjects should be notified of the following: 1) identification of the entity collecting the data; 2) identification of the uses to which the data will be put; 3) identification of any potential recipients of the data; 4) the nature of the data collected and the means by which it is collected...; 5) whether the ... requested data is voluntary or required; 6) the consequences of a refusal to provide the requested information; and 7) the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[30] With such information, the consumer will have the building blocks for informed decision making.

---

27. The Fair Information Practice originated in the United States Department of Health, Education and Welfare's 1973 report entitled Records, Computers and the Rights of Citizens (1973). Other reports addressing the fair information practice principles are: The Privacy Protection Study Commission, Personal Privacy in an Information Society (1977); Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995); U.S. Dept. of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995); The European Union Directive on the Protection of Personal Data (1995); and the Canadian Standards Association, Model Code for the Protection of Personal Information: A National Standard of Canada (1996). *See* http://www.ftc.gov/reports/privacy3/endnotes.htm#N_27_.

28. Federal Trade Comm'n, *Fair Information Practice Principals, at http://www.ftc.gov/reports/privacy3/fairinfo.htm.*

29. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1614 (1999).

30. Federal Trade Comm'n, *supra* note 28.

Once notice is established, it is a logical step for the consumer to have the ability to make choices based preferences. Choice makes the consumer an active participant of the transaction. This includes marketing, sale to third parties or any other use. Without the informed consent of the data subject, data collectors are prohibited from using personal information for their own gain.

Notice and choice facilitates awareness, access permits participation. For meaningful participation, consumers should have "ability both to access data [collected] about him or herself" and to "contest [its] accuracy and completeness."[31] Further, access must be reasonable. A data collector should provide "simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients."[32] Such qualifications help ensure that consumers do not get caught behind a web of hurdles or red tape. Such consumer involvement also facilitates data accuracy.

Providing consumers with information about what is being collected, choices regarding collection, and the ability to check and correct inaccurate information promotes cooperative management of consumer data. Adequate management is also facilitated by sufficient security of collected data.

The FIPP addresses precautionary measures.[33] Data collectors are encouraged to structure their internal organizational processes to prevent inadvertent misuse or dissemination of sensitive data.[34] Data collectors are also encouraged to use encryption "in the transmission and storage of data."[35] And once data is collected, it should be stored on "secure servers or computers that are inaccessible by modem."[36]

These principles, when put into practice, provide a foundation for the safe and open collection and use of data. However, such principles may not be put into practice. The FIPP conclude by suggesting that data collectors develop methods of enforcement through either "industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions."[37] This, however, is too flexible. Although Congressional bills based on the FIPP have been introduced,[38] and industry groups are growing concerned over privacy

---

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. Federal Trade Comm'n, *supra* note 28.

36. *Id.*

37. *See id* ¶ 5

38. Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001). Social Security On-line

legislation,[39] the FIPP are at risk of becoming merely suggestive by remaining unenforceable.

Interestingly, the FTC, which has been a proponent for self-regulation in the past, now acknowledges that legislative measures may be necessary.[40] The conclusion of the FTC's 1998 Report to Congress indicates that the FTC is prepared to take action, where appropriate, through the authority of the Federal Trade Commission Act.[41] The FTC Act "authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act. It therefore provides a basis for "government enforcement" of the FIPP.[42] The FTC openly warns: "failure to comply with stated information practices may constitute a deceptive practice in certain circumstances."[43]

The FIPP were developed to ensure "that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests."[44] They are comprehensive and provide for the general wellbeing of consumers. Interestingly, the FIPP are not the only attempt at comprehensive consumer privacy protection. Another prominent development is the OECD Guidelines.

1. OECD Guidelines

The OECD Guidelines followed the FIPP and address similar concerns. These concerns include: 1) limits on collection of information; 2) mechanisms to promote data quality; 3) notification of the specific purpose for collection; 4) limits on the use of data collected; 5) safeguards for the security of data collected; 6) openness with regard to practices and policies for the collection and use of personal data; 7) data subject's participation in maintaining the integrity of data collected; and 8) accountability of data collectors for compliance with the Guidelines.[45]

These eight elements are based on the principle of "openness."[46] Openness allows the consumer to become a meaningful participant in the e-marketplace.

Privacy Protection Act, H.R. 91, 107th Cong. (2001). Electronic Privacy Protection Act, H.R. 112, 107th Cong. (2001). Consumer Internet Privacy Enhancement Act, H.R. 237, 107th Cong. (2001). Spyware Control and Privacy Protection Act, S. 197, 107th Cong. (2001).

39. Ted Bridis, *Industry Studies Attack Web-Privacy Laws*, WALL ST. J. (March 13, 2001) at B6.

40. *See generally* Federal Trade Comm'n, *supra* note 30.

41. 15 U.S.C. § 41.

42. Federal Trade Comm'n, *supra* note 28.

43. *Id.*

44. *Id.*

45. *See* O.E.C.D., *supra* note 18.

46. *See id.* The concept of openness suggests that "there should be a general policy of openness about developments, practices, and policies with respect to personal data."

This is important for the creation of a democratic e-marketplace. As Paul Schwartz states in *Privacy and Democracy in Cyberspace*, if consumers are not given procedural and substantive rights they will be deterred "from participating in activities that promote cyber-democracy and self-definition on the Internet."[47]

Openness begins by making consumers aware of data collectors' practices. This is achieved by providing notice of collectors' practice. The Collection Limitation Principle, the Purpose Specification Principle, and the Openness Principle each direct data collectors to notify data subjects of the practices they will be subject to.

The Collection Limitation Principle of the OECD Guidelines only permits collection of data "where appropriate [and] with the knowledge or consent of the data subject."[48] This implies notice and provides the first parallel to the FIPP. Further, the purpose for the collection of consumer data must be stated either before or at the time of collection as stated by the Purpose Specification Principle.[49] Notice also extends to changes of use, collectors must notify consumers of "each occasion of change of purpose."[50]

The Openness Principle further expands the notice requirements. Data collectors must disclose practices and policies and provide data subjects with information regarding the "existence and nature of personal data, and the main purposes of their use (as established by the Purpose Specification Principle), as well as the identity and usual residence of the data controller."[51] This is the foundation to transparent practices and a level playing field.

Like the FIPP, the OECD Guidelines address consumer choice. The Collection Limitation Principle allows data subjects to choose whether or not they want data collected and collection is restricted to consumer preferences.[52]

The Use Limitation Principle also implicates consumer choice. Consumers must consent to the data collector's use of personal information.[53] The data

---

47. Schwartz, *supra* note 29 at 1677-78. For effective community on the internet Professor Schwartz states that data subjects must "(1) be able to allow or refuse collection of more than a minimum amount of these data or further use for a non-compatible use; (2) be informed of the data consequences of relevant behavior, such as signing up for service with an ISP or entering a specific Web site; and (3) be granted a mechanism by which she can inspect and correct personal data and find out which parties have gained access to her records." Notice how closely these elements that Professor Schwartz advocates mirror the standards imposed by the Safe Harbor Principles. Each of these objectives are met through the Safe Harbor Principles.

48. O.E.C.D, *supra* note 18 at ¶ 7.

49. *See Id.* at ¶ 9.

50. *Id.*

51. *Id.* at ¶ 12.

52. *Id.* at ¶ 7.

53. *See* O.E.C.D., *supra* note 18 at ¶ 10. This is also assuming that there is no overriding legal authority requiring collection regardless of a data subject's consent as provided by this paragraph of the

collector is then limited to the extent that the data subject has permitted use. The Purpose Specification Principle further limits permitted uses to those purposes explicitly stated by the data collector. In other words, the data collector is restricted from using consumer data in ways not previously disclosed.

These elements of the OECD Guidelines illustrate clear concern for consumer notice and choice. In accordance with the FIPP, the OECD Guidelines suggest that consumers become active participants of the data collection process.

The Purpose Specification Principle of the OECD Guidelines address the possibility of trade of consumer personal data. This principle limits transfer of personal information after the initial purpose of collection is met or if any use is incompatible with the initially specified purpose.[54] The Use Limitation Principle further develops the concept that use must be consistent with the initial purpose for collection and "should not be disclosed" or "made available" without the consent of the data subject or as authorized by law.[55]

The OECD Guidelines also promote data integrity by preventing inappropriate or potentially harmful altercation of a consumer data. This is done through the Data Quality Principle. This principle requires that the data collected be "relevant," "accurate," "complete," and "kept up-to-date."[56] To achieve these ends, the OECD Guidelines, like the FIPP, encourage consumer access to collected data.

The Individual Participation Principle of the OECD Guidelines corresponds directly to the access element of the FIPP. Data subjects are unambiguously afforded the opportunity to obtain confirmation whether or not data is collected. Data subjects are also given the opportunity to challenge and possibly erase, rectify, complete or amend any inconsistencies in the information held by a data collector.[57] The OECD Guidelines provide for data subjects to directly request information from data collectors and if a reasonable request is denied, the data subject should "be able to challenge such denial."[58] Consumers therefore play a valuable role in maintaining the integrity of collected data. The groundwork for data collector and data subject cooperation is created.

In addition to allowing the data subject access to information, the concept of making the data subject a meaningful participant in the e-marketplace reflects

---

Guidelines.

54. *See id.* at ¶ *9.*

55. *See id.* at ¶ 10.

56. *See id.* at ¶ *8.*

57. *See id.* at ¶ 13.

58. O.E.C.D. *supra* note 18.

the OECD's concern for openness. Without the ability to access information it would be impossible for data subjects to evaluate "the existence and nature of personal data."[59]

The Openness Principle, true to its title, prescribes transparency on behalf of data collectors. Data subjects must have knowledge of the collection of their personal data. In theory, this is good; however, without imposing accountability on a data collector, there is no incentive for data collectors to comply. Thus, the OECD included an Accountability Principle.

Though broad, the Accountability Principle states that a data collector should "be accountable for complying with measures which give effect to the principles stated above."[60] This illustrates concern for enforceability. It also recognizes that the privacy-protecting measures of the OECD Guidelines are at risk of inadequate implementation or of not being followed at all.

2. Limitations of the FIPP and OECD Guidelines

The OECD Guidelines and the FIPP are straightforward. They both address comprehensive protection of consumer data through the establishment of a privacy friendly environment. One in which the consumer plays an active and informed role in the data collection process.

Both the FIPP and the OECD Guidelines, however, are weakened by the fact that they only "suggest" proper practices. The FIPP are the result of a "series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices."[61] They were drafted as a distillation of common beliefs on appropriate methods to protect consumer privacy. Similarly, the OECD Guidelines were drafted to serve as a "recommendation" to "harmoni[z]e national privacy legislation" with an eye towards "human rights" and at the same time promote "international flows of data."[62] Neither has been adopted into U.S. law. Further, neither the FIPP nor the OECD Guidelines has been adopted in full by U.S. business.[63] As we stand today, U.S. consumers lack comprehensive privacy protection. The FIPP and the OECD Guidelines offer models, but these models have not been formally adopted.

---

59. *Id.* at ¶ 12.

60. *Id.*

61. Fair Information Practice Principles, *supra* note 28.

62. O.E.C.D. *supra* note 18.

63. The Georgetown Internet Privacy Policy Survey conducted by Professor Mary Culnan "[drew a random sample] of the most-heavily trafficked sites on the World Wide Web and [surveyed] the busiest 100 sites. The survey found that "only 10% of the sites posted disclosures that even touched on all four fair information practice principles." Federal Trade Comm'n, *supra* note 28.

On the other, the European Union has adopted and enacted comprehensive privacy protection legislation. Although the E.U. Data Directive was not simply based on the OECD Guidelines or the FIPP, the intentions are noticeably similar.[64] Professor Marc Rotenberg has pointed out that the E.U. Data Directive was indirectly influenced by the development of United State's privacy law.[65] The most notable difference, for the purposes of this article, is that the E.U. Data Directive mandates privacy-friendly practices and procedures for data collectors and data subjects.

3. The E.U. Data Directive: in harmony with the FIPP and OECD Guidelines

The E.U. Data Directive recognizes and affirmatively establishes transparent practices for data collectors. By enacting a pan-European "directive" these transparent practices are binding enforceable by law.[66] Although not organized like the FIPP or the OECD Guidelines (which set out specific principles as discussed above), the E.U. Data Directive does address the elements of notice, choice, access, security, and enforcement.

Notice is addressed in Articles 10 and 11 of the E.U. Data Directive. Together, these articles require disclosure of a data collector's identity, purpose for processing data, whether the data collection is obligatory or voluntary, the

---

64. Graham Greenleaf, Associate Professor of Law at the University of New South Wales has compared the E.U. Data Directive to the OECD Guidelines and has found that the E.U. Data Directive is in "general terms similar to the information privacy principles found in the OECD Guidelines and the Council of Europe Convention. A rough comparison of the articles in Chapter II with the titles of the OECD's eight principles is as follows: collection limitation principles (art 10, art 11, parts of art 7); data quality principles (art 6); purpose specification principle (art 6); use limitation principle (art 16); security safeguards principle (art 17); openness principle (art 21); individual participation principle (art 12, art 14); and accountability principle (definition of 'controller'). Other articles cover matters not always found in previous sets of principles, such as purpose justification (art 7), 'sensitive' data (art 8), automated decision-making (art 15), and notification (arts 18, 19, 20)." Graham Greenleaf, *The European Privacy Directive – Completed*, Privacy Law & Policy Reporter, Art. 2, No. 5 (1995) 2 PRIV. L. & POLICY REP. 81, *available at* http://www.austlii.edu.au/au/other/plpr/vol2/Vol2No05/v02n05a.html#fn1.

65. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. L. Rev. 1 (2001). Professor Rotenberg states that offering privacy protection is not just a "European approach... in contrast to a US approach." Developments in privacy law were "derived from the Brandeis and Warren article of 1890, which was even characterized by European scholars as the 'American tort.'" Other examples of influential efforts by the U.S. include the Federal Wiretap Act of 1968 and the Privacy Act of 1974.

66. The E.U. Data Directive requires that each E.U. member nation appoint a "supervisory authority" to ensure the Directive is followed. Among other powers, the supervisory authority has "the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities. EUR. PARL. DIR., *supra* note 6.

consequences of failure to reply to collection questions, and whether a right of access exists.[67] Article 7 of the E.U. Data Directive then provides that personal data may only be processed where an individual's consent has been obtained (or in certain cases of necessity, such as the compliance with a legal obligation or to protect the vital interests of the data subject among others[68]). After giving notice, the data subject's consent must be "unambiguously given."

The E.U. Data Directive also addresses consumer consent. Article 7 explicitly states that "personal data may be processed only if: the data subject has unambiguously given his consent; or [...] processing is necessary for "the performance of a contract" at the request of the data subject, "for compliance with a legal obligation," "to protect the vital interests of the data subject", processing is necessary for the public interest or official authority."[69] Article 8 offers further protection to specific types of data. Data that is especially sensitive or unique to the consumer such as: "racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership" as well as details of a person's health or sex life"[70] requires explicit consumer consent must before it can be processed.[71] Article 13 provides another exemption to the protection of personal data. This article provides that national security; defense; public security; the prevention, investigation, detection or prosecution of criminal offenses; important economic or financial interests; certain inspection and regulatory functions; or the protection of the data subject or the rights and freedoms of others will trump the individual's rights to privacy protection.[72]

Although the E.U. Data Directive allows freedom to collect data in circumstances of "journalistic purposes or for the purpose of artistic or literary expression...," Article 9 states that the collection of data is only permissible "if necessary to reconcile the right to privacy with the rules governing freedom of expression."[73] Given the tough stance on protecting consumer data, it is unlikely that this exemption will be abused.

Consumers are also given the right to access information that has been collected. The consumer's right to access includes "confirmation [that personal data is] being processed" notice of the "categories of recipients to whom the data are disclosed", as well as information concerning the "automatic processing of data."[74] Article 12 of the E.U. Data Directive also grants data subjects the

67. *See id.* at Arts. 10-11.

68. *Id.* at Art. 7.

69. *Id.*

70. *Id.* at Art. 8.

71. EUR. PARL. DIR., *supra* note 6, at Art. 8.

72. *Id.* at Art. 13.

73. *Id.* at Art. 9.

74. *Id.* at Art. 12.

right to "rectify, erase or block data" that is collected but not used in accordance with the Data Directive.

To promote stepped up security for consumer's personal data, the E.U. Data Directive limits any processing of consumer data to necessity.[75] In other words, fewer attempts at processing will help safeguard from accidental disclosure. Article 17 of the Directive also requires that data collectors take precautionary steps to prevent "accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access."[76] Data collectors must take "technical security measures" (such as employing sufficient cryptography) as well as take "organizational measures" to prevent internal or employee mishaps.[77]

The development and implementation of the E.U. Data Directive had international consequences. It thrust a new hurdle in international consumer data collection. Any data collector wishing to collect data from citizens of European Union member nations had to comply with the E.U. Data Directive or be subject to the legal ramifications of breaking E.U. law. As mentioned above, Safe Harbor Principles are a consequence of the E.U. Data Directive.

4. A Bridge: The Safe Harbor Principles

The final version of the SHP was released on July 21, 2000.[78] It consists of seven elements: 1) Notice; 2) Choice; 3) Onward Transfer; 4) Data Security; 5) Data Integrity; 6) Access; and 7) Enforcement.[79] To ease implementing the SHP, the DOC set up a compliance checklist for data collectors.[80]

It is apparent from titles alone that the SHP mirror the FIPP and the OECD Guidelines. The reemergence of these principles can be seen as an affirmation accepted thought on consumer privacy and data protection. The SHP are merely an elaboration of existing U.S. principles. Because the SHP are international in nature, they potentially create a world-wide safety net for consumers; something necessary in our borderless e-marketplace.

---

75. *Id.* Art. 17.

76. EUR. PARL. DIR., *supra* note 6.

77. *Id.*

78. US DEPT. OF COMM., Safe Harbor Docs., Issuance of Principles and Transm'n to Eur. Comm'n., 65 Fed. Reg. 45666 (July 24, 2000).

79. *Id.*

80. *See* Safe Harbor Privacy Principles Checklist *available at* http://www.export.gov/safeharbor/checklist.htm.

IV. SAFE HARBOR PRINCIPLES: A SAFETY NET FOR THE PROTECTION OF CONSUMER PRIVACY

There have been numerous attempts to secure effective protection for consumer privacy. The 106th Congress considered numerous privacy related bills[81] and the 107th Congress is following continues to address the protection of consumer privacy.[82] However, Congress is still only beginning to recognize the importance of comprehensive consumer privacy legislation. For example, Congress is not considering the Consumer Internet Privacy Enhancement Act.[83] This bill, consistent with the FIPP, would require data collectors to provide notice to data subjects about the identity of the data collector, whether information would be collected, the types of information collected, how the information would be used, and how the data subject can prevent collection.[84] If enacted into law, this bill would be enforced under the FTC Act because a violation would be considered "an unfair or deceptive act or practice in or affecting commerce."[85] Although this bill addresses Notice, Choice, and Enforcement, it falls short of the comprehensive protections created by the FIPP and the OECD Guidelines. It also falls short of the standards imposed by E.U. Data Directive. The proposed Consumer Internet Privacy Enhancement Act represents an initial, yet still incomprehensive, approach to protecting consumer privacy.

As Professor Joel R. Reidenberg argues in *Restoring Americans' Privacy in Electronic Commerce*,[86] The OECD Guidelines, as a reflection of the FIPP "should be adopted in law as the American framework for information privacy."[87] All five elements of the FIPP, as reaffirmed in the OECD Guidelines, when taken together, are necessary for an effective privacy

---

81. The 106th Congress considered 50 bills relating to privacy, 48 of which were specifically concerned with "consumer privacy." *See* thomas.loc.gov.

82. The 107th Congress is evaluating 50 bills also, seven of which are specifically concerned with "consumer privacy." These seven are: 1. Internet Tax Nondiscrimination Act S. 288, 107th Cong. (2001); 2 . Internet Tax Moratorium and Equity Act S. 512, 107th Cong. (2001); 3. Consumer Internet Privacy Enhancement Act, H.R. 237,107th Cong. (2001). 4 . Consumer Online Privacy and Disclosure Act H.R. 347, 107th Cong. (2001); 5. Bankruptcy Reform Act of 2001 S. 420., 107th Cong. (2001); 6 . Bankruptcy Reform Act of 2001 S. 420, 107th Cong. (2001); and 7 . Comprehensive and Balanced Energy Policy Act of 2001S. 597 107th Cong. (2001).

83. H. R. 237, 107th Cong. (2001). Introduced to protect the privacy of consumers who use the Internet.

84. H. R. 237 at § 2(b)(1).

85. H.R. 237 at § 3(a). Unfair and deceptive acts are defined in section 18(a)(1)(B) of the Federal Trade Commission Act 15 U.S.C. § 57(a)(1)(B). *See id.*

86. Joel R.Reidenberg, *Restoring Americans' Privacy in Electronic Commerce,* 14 BERKELEY TECH. L.J. 771 (1999).

87. *Id.* at 788.

protection program. The SHP offer just such a combination. They reflect the values and ideas of the FIPP and the OECD Guidelines and do so in compliance with the E.U. Data Directive.

1. The Creation Of The SHP

As discussed above, the SHP were developed to help U.S. businesses meet the requirements of the E.U. Data Directive. The theory behind the E.U. Data Directive is that privacy is a fundamental human right and that collected data should be protected.[88] The SHP serve as a bridge between privacy protection and international trade.

The SHP are necessary because Article 25 of the E.U. Data Directive restricts the transfer of personal data outside of the European Union. The United States and by implication, those businesses operating in the U.S., does not meet the standards of Article 25 because, as discussed above, no comprehensive consumer data protection legislation exists. Although data collectors that operate exclusively in the United States are not subject to the E.U. Data Directive, those businesses with European operations or intending to do business with E.U. member countries must comply.

Although the U.S. has historically taken a "sectional" approach to consumer privacy protection[89] and the European Union has now adopted a "comprehensive" privacy protection program,[90] globalization has led to increased interaction between countries. This convergence of cultures requires that differences be ironed out. The SHP do just that.

2. The Substance of the SHP

As discussed above, the SHP address the same topics as the FIPP and the OECD Guidelines: Notice, Choice, Access, Security, and Enforcement. However, the SHP also explicitly address onward transfer of consumer data and the maintenance of data integrity.

---

88. EUR. PARL. DIR., *supra* note 6.

89. Rotenberg, *supra* note 65; *see also,* U.S. Department of Commerce website for the implementation of the Safe Harbor Principles which states that "while the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation" http://www.export.gov/safeharbor/.

90. *See id.*

a. Notice

The SHP require that consumers be provided with the identity and contact information of the data collector. Data collectors must also provide "clear and conspicuous" notice when personal information is collected.[91] Fine print will probably not suffice. Additionally, the information collected must be "relevant for the purposes for which it is to be used."[92]

For example, a shoe salesman would most likely not be allowed to collect information about a consumer's race, religion, or medical conditions. Further, "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."[93] Notice must also be provided before the organization uses such information or discloses it to a third party.[94]

b. Choice

Consumers must also be able to choose – choose whether or not to give information and what information to give. Data collectors are required to provide the option of opting-out of disclosure of personal information to third parties. Consumers may also opt-out of disclosure if the information is to be used for purposes other than as authorized by the data subject.[95] As discussed when addressing the FIPP and OECD Guidelines, choice and notice make consumers informed participants in the e-marketplace.

c. Data Integrity

The SHP require the data collector to take "reasonable steps to ensure that the data collected is reliable for its intended use, accurate, complete, and current."[96] Although this places the data collector in the potentially precarious position of having the responsibility to validate personal information, it also prevents the circulation of false or misleading information. Interestingly, this element, does target those consumers who would otherwise wish to be identified as a "dog."[97]

---

91. DEPT. OF COMM., Safe Harbor Privacy Principles Issued By The U.S. Department Of Commerce July 21, 2000 *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

92. Safe Harbor Privacy Principle *available at* http://www.export.gov/safeharbor/SafeHarborDocuments.htm.

93. *Id.*

94. *See id.*

95. Department of Comm., *supra* note 78.

96. *Id.*

97. As in the famous cartoon by Peter Steiner from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20).

Information has value and "data has power."[98] If data is not correct, its value is reduced and its power is illegitimate. The data integrity element helps prevents spoliation of collected information. Allowing the consumer access to review the data that has been collected also enhances data integrity.

d. Access

Consumers are often in the best position to verify the accuracy of their personal information. They are also in the best position to keep it up to date. The access principle provides that consumers be permitted to view the data collected about them and "to correct, amend, or delete that information where it is inaccurate."[99] This right of access, however, is limited to situations where "the burden or expense of providing access" would not 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."[100]

Advising consumers of the data collection process, giving consumers the opportunity to consent to collection, and providing access to review and correct data promote transparent practices and make the consumer a meaningful participant in the collection process. However, effective consumer privacy protection also includes secure and responsible use of consumer data.

e. Onward Transfer

Onward transfer requires that third party transferees provide the same protections that the data collector was required to provide. This protects information used at point B even when it was collected at point A.

Transfer of consumer data is restricted to instances where the consumer has consented to such transfer. However, once consent has been obtained, and there are assurances that the third party (the new data user) complies the SHP use and security restrictions[101], consumer data can be used by that third party.

Although transfer is limited to those parties that comply with the objectives of the SHP, effort is made to facilitate the transfer of data. As discussed above, the SHP were developed with the understanding that consumer privacy concerns are linked to international commerce.[102] The SHP bridge these two interests.

---

98. Lawrence Lessig, *Behind the Curtain*, THE INDUS. STAND., Sept. 4, 2000.

99. Department of Comm., *supra* note 6.

100. *Id.*

101. *Id.* The notice provision restricts use to those uses specified at the time of collection. The security provision requires that third party data users provide "adequate" security for consumer data.

102. Although further discussion of the criticisms of the SHP are discussed in following sections, the concept of privacy as fundamental "human right" versus "commercial concern" was fundamental to the Trans Atlantic Consumer Dialogue's (TACD) criticism of the SHP. In paragraph four of the TACD Resolution On

Even if a third party has not completely adopted the SHP but still wants consumer data, that party may execute a written agreement "requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles."[103]

f. Security

Collection of consumer data will inevitably yield files of consumer data. Once these files are created, they must be protected from misuse (both internal and external) and from inadvertent dissemination. Measures must be taken to ensure the security of information collected. That which is not secure cannot be considered private.

It is clear that data controllers are responsible for the confidentiality and security of consumer data. "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."[104] Although not mentioned, cryptography and encryption are likely requirements.[105]

Recognizing that some information may require special treatment, the SHP differentiate between types of personal information and encourage special treatment of sensitive information. Consistent with the E.U. Data Directive, sensitive information includes "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."[106] Data subjects must give "affirmative or explicit (opt-in)" consent if sensitive information is going be disclosed to a third party or used outside of the immediate transaction. This provides heightened protection

---

Safe Harbor Principles, TACD criticizes the SHP for not recognizing that privacy is a "human right" and placing it on the same ground as "commercial concerns." TACD Doc No. Ecom-18-00 (February, 2000) at ¶ 4. The purpose behind the SHP is to "provide a more predictable framework for such data transfers." Safe Harbor Privacy Principles Issued By The U.S. Department Of Commerce (July 21, 2000). This implies that commercial concerns are to be considered the rights and concerns are intimately linked and by addressing them together will facilitate a comprehensive solution.

103. Department of Comm., *supra* note 6.

104. *Id.*

105. "Encryption technologies" are "the locks and keys of the information age. "They" are special programs designed to protect sensitive information on digital communications networks. Encryption technologies work by scrambling and encoding information so that it can only be read by the proper recipient." Center For Democracy and Technology, Introduction to "what is crypto" *at* http://www.cdt.org/crypto/new2crypto/1.shtml "Strong encryption is freely available today inside the United States."

106. Department of Comm., *supra* note 6.

to a sphere of information that could be particularly harmful to a data subject if mishandled.[107]

g. Enforcement

The old adage that knowledge is power is just as true in the e-marketplace as it is outside.[108] Information therefore becomes an easy target for abuse and proper enforcement is needed. Further, enforcement measures add confidence.

Enforcement must be available through mechanisms that: 1) ensure compliance, 2) acknowledge that recourse is available and affordable, and 3) illustrate that consequences exist.[109] This includes independent recourse (in accordance with applicable law or private sector initiatives).[110] Data collectors must follow-up on complaints of violation and work to remedy problems. These efforts must also be backed up by self-imposed consequences that are serious enough to ensure compliance when violations occur.[111] If these measures are not taken and recourse is not available, the data collector will be considered to be in breach of its duties to the consumer and therefore subject to the ramifications of unfair and deceptive practices under the FTC Act.

Although the technicalities of this element are vague, the objective is clear. Data subjects must be made aware that recourse is available when personal data is misused. This is achieved when data collectors publicly acknowledge that they are in compliance, acknowledge that there are consequences of misuse of personal data, and that they have an obligation to remedy problems. Because the broadness of this principle may lead to varied application, SHP Frequently Asked Question (FAQ) number 11 specifically addresses methods of compliance[112] and encourages data collectors to work with a third party to test

---

107. This element opens the door to a theoretical question regarding the right to privacy and that different rights may extend to different kinds of information. This, although very interesting, is beyond the scope of this paper.

108. Consider the success of online marketing firms such as Engage.com. Engage is a "leader in audience profiling technology and maintains the world's largest database of anonymous Internet profiles." See Engage Company information *available at* http://www.engage.com/company. (Fortunately, Engage maintains the practice of keeping anonymous profile technology and thus recognizes the importance of protecting consumer privacy.)

109. Department of Comm., *supra* note 6.

110. *See id.*

111. *Id.*

112. *See* Frequently Asked Question (FAQ) number 11 *available at* http://www.ita.doc.gov/td/ecom/FAQ11FINAL.htm (regarding dispute resolution and enforcement). To satisfy the first and third elements of the enforcement principle, an organization can either (1) comply with a privacy program developed in the private sector that incorporates the Safe Harbor Principles into its rules and that includes effective enforcement mechanisms; (2) comply with legal or regulatory supervisory authorities that provide for handling of complaints; or (3) commit to cooperate with European data protection authorities. To

its practices. By bringing in a third party, such as a certifying organization (like TRUSTe) or legal counsel, there is a greater likelihood that unbiased judgment will be made that the data collector could serve the needs of concerned consumers.

3. Implementation of the SHP in the U.S.

The principles of Safe Harbor allow for "controlled self-regulation." Data collectors could implement the principles themselves and get a stamp of approval from a government agency (currently the United States Department of Commerce).[113] This would appeal to U.S. interests that believe business should decide how to manage the collection of consumer data. Further, pursuant to Article 4 of the E.U. Data Directive, American law will still govern U.S. businesses.[114] Despite criticism from the European Parliament,[115] the European Council and the United States have agreed to follow the SHP.

The DOC (or its designee) will serve as a liaison for U.S. companies. It will register organizations that are certified under the SHP[116] and maintain a

---

satisfy the second point, an organization must verify that the assertions it makes about its privacy program are true either through self-assessment or outside compliance reviews.

113. *See generally* Official Journal of the European Communities of 23 November 1995 No. L. 281 p. 31. Art. 29. Supervisory Authority, Working Party on the Protection of Individuals. Unofficial copy available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html. *See also* US Department of Commerce website for the implementation of the Safe Harbor Principles which states that "to be assured of safe harbor benefits, an organization needs to self certify annually to the Department of Commerce in writing that it agrees to adhere to the safe harbor's requirements" *available at* http://www.export.gov/safeharbor/SafeHarborInfo.htm.

114. This, however, is being challenged. It was recently reported that "The European Parliament approved ... a measure that lets customers sue operators of foreign e-commerce sites in the courts of the consumers' home countries." *See* Rick Perera, *E.U. strengthens consumers' e-commerce rights,* The Industry Standard, September 22, 2000 *available at* http://www.thestandard.com/article/display/0,1151,18785,00.html.

115. E.U. Parliament stated that that the Safe Harbor Principles do not offer adequate protections because they neither provide for monetary damages for breach nor right of appeal in the United States.

116. An organization can obtain acknowledgement that it is in compliance with the SHP by self certifying. To qualify, organizations must "provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:

1. name of organization, mailing address, email address, telephone and fax numbers;
2. description of the activities of the organization with respect to personal information received from the EU; and
3. description of the organization's privacy policy for such personal information, including:
    a. where the privacy policy is available for viewing by the public,
    b. its effective date of implementation,
    c. a contact office for the handling of complaints, access requests, and any

publicly available list of all organizations that are in compliance with the SHP.[117] This will facilitate business to business transfers of information by reducing the pre-transfer due diligence. The DOC's list currently registers sixty-seven registered U.S. based data collectors.[118]

V. PENDING QUESTIONS: CRITICISM OF THE SAFE HARBOR PRINCIPLES

1. Does the SHP offer sufficient protection?

Privacy advocates have long been skeptical of self-regulation. In February of 2000, Marc Rotenberg, director of the Electronic Privacy Information Center, stated that U.S. "self-regulation is inviting a 'race to the bottom.'"[119] This concern illustrates a need for a mandatory and enforceable standard-of-care for data collectors. It also speaks to the weaknesses behind the FIPP and OECD Guidelines. Because neither *required* comprehensive adoption, they were subject to being applied incompletely and therefore only offering incomplete protection. In essence, both were subject to abuse because data collectors could partially adopt the recommendations and still say that they were attentive to FIPP.

The Transatlantic Consumer Dialogue ("TACD"), a consumer advocate, has expressed concern that international consumer privacy protection is necessary.[120] The increasingly international e-marketplace demands an international set of standards. Further, the TACD does "acknowledge that the

---

other issues arising under the safe harbor,

d. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles),

e. name of any privacy programs in which the organization is a member,

f. method of verification (e.g. in-house, third party), and

g. the independent recourse mechanism that is available to investigate unresolved complaints." http://www.ita.doc.gov/td/ecom/FAQ6Self CertFINAL.htm.

117. *See* Safe Harbor Privacy Principles FAQ No. 6 para. 4 *available at* http://www.ita.doc.gov/td/ecom/FAQ6SelfCertFINAL.htm.

118. Department of Commerce Safe Harbor List at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list. (last visited June 30, 2001).

119. Keith Perine, The Indust. Stand., *How Private Is Private Enough?* (Feb 28, 2000) *available at* http://www.thestandard.com/article/display/0,1151,12348,00.html.

120. *See* Press Release, TACD, Consumer Groups Warn That Safe Harbor Privacy Proposal Will Undermine Consumers' Legal Rights (Mar. 30, 2000) *at* http://www.tacd.org/press_releases/warn300300.html.

current text of the safe harbor agreement represents some progress" despite the fact that they "maintain their reservations."[121]

The progress that the SHP represent is significant. It is distillation of the widely supported U.S. FIPP and OECD Guidelines. Rather that risking a race to the bottom, the SHP represent affirmative action in favor of comprehensive adoption of the FIPP and the OECD Guidelines.

2. Is There Protection From Discrimination?

Another concern about the SHP, as with any standard, is that data collectors will discriminate against consumers that choose not to disclose their personal information. Goods or services may be withheld if information is not provided. Or worse, goods or services may not be offered based on the information collected.

Although this is a concern, there is no provision in the SHP to address discriminatory practices by data collectors. In the event of such discrimination, national discrimination laws would most likely apply. Although this is beyond the scope to this article, the desire for transparent data collection practices would most likely reveal such discrimination and facilitate proper prosecution.

3. Does the E.U. Gets Greater Protection Than U.S.?

The TACD also criticizes the SHP because they are a watered down version of the E.U. Data Directive and therefore "compromise the privacy interests of European citizens."[122] The compromise, however, is not substantial. As discussed above, the SHP has adopted the elements of the E.U. Data Directive and was developed in accordance with the E.U. Data Directive. Although, the SHP streamline the E.U. Data Directive, they still serve to maintain the rights provided through the E.U. Data Directive. European citizens are not sacrificing their legal rights with the implementation of the SHP. Further, because legislative intent is a well established technique for interpreting legislation, courts will most likely look directly to the E.U. Data Directive to interpret violations of the SHP. Admittedly, this will be on a case by case basis and will not be determined until the SHP is the subject of court proceedings.

As discussed above, the SHP only apply to citizens of E.U. member nations. This affords E.U. citizens greater protections than U.S. citizens. Comprehensive U.S. consumer privacy legislation has been slow in the making. Although there have been some efforts[123] nothing has been passed. Likewise,

---

121. *Id.*

122. TACD *Safe Harbor Proposal and International Convention on Privacy Protection*, Doc. No Ecom 8-99 *at* http://www.tacd.org/ecommercef.html#consumer.

123. *See supra* notes 86 and 87.

I advocate that the SHP be used as a template for comprehensive U.S. consumer privacy legislation. This would raise the bar in the U.S. to one closer to that of Europe.

4. Does the SHP Lack Enforcement and Accountability?

Enforcement of the SHP has been questioned.[124] One of the primary and most often sited criticisms of the SHP is that the SHP will be unenforceable.[125] This concern is based in part on the belief that consumers will not have a forum to bring complaints, making redress difficult. Although in the past this concern may have been well grounded, recent developments offer a promising likelihood that redress will be available.

Recent FTC actions and statements illustrates that consumer privacy is an area of concern.[126] The FTC's traditionally pro-business reputation is ebbing.[127] The FTC has abandoned its support of industry self-regulation in favor of legislative efforts to protect consumer privacy.[128] In addition to this revised, consumer-privacy-friendly stance, the FTC has created precedent for the enforcement of privacy policies. Consider the FTC's actions in the case against GeoCities.[129] The FTC brought action for deceptive practices in the collection and use of consumers' personal information because GoeCities misrepresented their privacy policy in violation of the FTC Act.[130]

---

124. *See generally* Julie Fromholz, *The European Union Data Privacy Directive*, 15 Berkeley Tech. L.J. 461 (2000). *See also,* Press Release, *supra* note 120. TACD maintains "reservations [...] above all, on the issue of effective enforcement; and TACD, *Safe Harbor*, Doc. Ecom-07/03/01 The most significant shortfall of the Safe Harbor Principles is the lack of enforcement and accountability.

125. *See* Fromholz, *supra* note 124 at 475. In this article, Ms. Fromholz argues that safe harbor will not be enough of a permanent protection because protection laws are still outstanding and cannot be effective without further US policy and law enforcement. "In addition, the Directive requires so much oversight of even individual data transfers that the transaction costs of implementing a system that fulfilled the requirements for every transfer could be prohibitive. It would seem to make little sense for the U.S. and other third countries to spend significant resources attempting to comply with a regulation that cannot realistically be enforced."

126. *See* Federal Trade Comm'n, *supra* note 8. The FTC states "that self-regulatory initiatives to date *fall far short* of broad-based implementation of effective self-regulatory programs" (*emphasis added*).

127. *See* Reidenberg, *supra* note 86.

128. Federal Trade Comm'n, *supra* note 8, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. "Ongoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumers' privacy on the Internet. Accordingly, the Commission recommends that Congress enact legislation to ensure adequate protection of consumer privacy online."

129. *In the Matter of* GeoCities, 1999 WL 69858 (Feb. 5, 1999) (F.T.C.). The Decision and Order is *available at* http://www.ftc.gov/os/1999/9902/9823015.do.htm.

130. *See id.*

GeoCities operated a website that created a community of individual homepages. This community consisted of about 2 million users, including adults and children.[131] Consumers were required to complete an online application form disclosing personal information. GeoCities then created a database that included e-mail and postal addresses, member interest areas, and demographics including income, education, gender, marital status and occupation.[132] This information was then disclosed to third parties. The FTC brought the complaint and followed up with the charge. Although GeoCities settled the case with no admission of wrongdoing, this shows that the FTC is concerned with consumer privacy and is willing to investigate potential violations of consumer rights. The FTC has also probed sites such as iVillage.com and HeathCentral.com "for possible unfair and deceptive trade practices" resulting from "improperly shar[ing] information with third parties" or "violat[ing] their stated privacy policies."[133]

Foreseeing the concern for the protection of consumer privacy, there has also been Congressional action and the U.S. Department of Commerce released a memorandum addressing the issue.[134] Enforcement will be initiated in the private sector and will move to the federal arena if the private sector does not respond effectively.[135] Data collectors are required to have a dispute resolution system to investigate and resolve complaints.[136] This provides for the initial contact. If matters are not handled adequately, a data subject can seek relief under "federal or state law prohibiting unfair and deceptive acts" or the False Statements Act.[137] The FTC would be a likely candidate to challenge violations

131. Press Release, FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (FTC File No. 982 3015) (Aug. 13, 1998) *available at* http://www.ftc.gov/opa/1998/9808/geocitie.htm. Copies of the complaint, the proposed consent order, the analysis of the proposed consent order to aid public comment, the brochure, "Site-Seeing on the Internet," as well as information, including Commission reports and testimony about its privacy initiative are available from the FTC's web site at http://www.ftc.gov and also from the FTC's Consumer Response Center, Room 130, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 25080; 202-FTC-HELP (202-382-4357).

132. *See id.*

133. *See* Keith Perine, *FTC Probes Health Site Privacy*, The Indust. Stand., (Feb. 18, 2000) *available at* http://www.thestandard.com/article/display/0,1151,11120,00.html.

134. *See Safe Harbor Enforcement Overview Federal and State "Unfair and Deceptive Practices" Authority and Privacy*, (July 14, 2000) *available at* http://www.export.gov/safeharbor/ENFORCEMENTOVERVIEWFINAL.htm.

135. *See* http://www.export.gov/safeharbor/SafeHarborInfo.htm.

136. *Id.*

137. *Id.* The Federal Trade Commission and the Department of Transportation with respect to air carriers and ticket agents have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the safe harbor framework but then fail to live up to their statements." *Id.* Further, If an organization "frequently fails to comply with

where websites claim to adhere to the SHP but do not offer the required protections.

The remaining criticism over the enforcement of the SHP is that they only apply to Europeans and others living outside of the United States. They should serve as a framework for comprehensive U.S. legislation. In fact, a bill was introduced in the 106th Congress to adopt legislation to "protect the privacy of American consumers."[138] This bill, short title "Consumer Privacy Protection Act", embraces the FIPP in full and applies not only to data collectors but also to third parties, thus accounting for onward transfer of data.

Although the FTC is still developing its privacy protection expertise, it has made commendable strides toward the protection of consumer privacy and is currently the only agency overseeing compliance with privacy protection policies. Other options include setting up a separate agency to monitor privacy violations. Professor Paul Schwartz advocates the appointment of a privacy commissioner.[139] Professor Schwartz believes that this commissioner should do more than just enforce privacy standards and should "assist the public, social groups, and the legislature in understanding strengths and weaknesses in the boundaries of existing information territories."[140] Similar suggestions have also arisen through the TACD.[141] Although this is an interesting option and one that deserves consideration, I will not discuss it further in this article. For the purposes of this article, it is sufficient to note that some federal entity (currently the FTC) is monitoring privacy violations.

Lastly, the element of enforcement gives the SHP teeth. These teeth, however, must adapt to inevitable changes in technology. By not specifying which specific mechanisms must be in place, the SHP remain flexible and enable a system of communication between data collector and data subject rather than rigid specifications. This communication will facilitate an environment that will "create new markets and opportunities for the development of privacy protecting products."[142] Our new economy requires

---

the requirements to the point where its claim to comply is no longer credible" action may be taken under the False Statements Act (18 U.S.C. § 1001). This also addresses the Trans Atlantic Consumer Dialogue (TACD) concern that there are not satisfactory procedures for consumers when they have a grievance. *See* http://www.epic.org/privacy/intl/TACD_SH_comments_0300.html (Submission of the TACD concerning the U.S. Department of Commerce Draft International Safe Harbor Privacy Principles and FAQs, published on March 15, 2000).

138. S. 2606, 106th Cong., (2000).

139. Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 VAND. L. REV. 1607, 1680 (1999).

140. *Id.*

141. *See* TACD, *supra* note 122.

142. Reidenberg, *supra* note 127 at 790. Reidenberg argues that adoption of the OECD Guidelines, combined with the creation of a "data privacy commissioner", would enhance consumer privacy protections.

adaptability. What might seem required today may become antiquated by tomorrow. Effective regulations are adaptive regulations and enforcement is thus strengthened by such flexibility.

VI. SHARING THE BURDEN: TECHNOLOGIES THAT ENHANCE THE EFFECTIVENESS OF THE SAFE HARBOR PRINCIPLES

It is not hard for an individual to recognize when their home or vehicle has been broken into; the evidence of broken windows or missing items is apparent to the naked eye. The collection of data, on the other hand, is not so apparent. With the aid of developments in technology, consumers will be able to help defend themselves against abuses. The victim of theft can report that theft to the appropriate authorities as soon as it is noticed. With the SHP in place, the involved and educated consumer who becomes victim to privacy or data collection abuses will be able to seek redress with haste. Consumer privacy technology can help prevent "the tremendous risk that incomplete national assumptions will be powerful, that multinational media giants will assert themselves, and that imperfect enforcement schemes will allow loopholes and cheating."[143]

1. Developments in the E-Marketplace: Giving The Consumer Tools To Survive

There are three aspects of the e-marketplace that have considerable impact on the consumers' ability to navigate safely. These areas are: 1) the existing technology and architecture of the internet, 2) software upgrades, and 3) third party service providers. They each represent avenues impacting consumers' ability to enforce privacy rights and personal data protection. The SHP may provide a safety net but that net must be secure. Technology will enable consumers to become experienced and proficient in the protection of personal data and thus serves to offer security on the frontlines of privacy abuses – with the consumers.

2. Code: Creating The Need For Protection

Before evaluating the services and technologies available, it is important to consider why they are helpful. The history of privacy protection in the U.S. has been one of competing interests. Products are developed that facilitate communication. However, in facilitating communication, these products also

---

Although I agree with the substance and insightful comments of the article, the Safe Harbor Principles would be an effective replacement for the OECD Guidelines.

143. Lance Liebman, *An Institutional Emphasis,* 32 CONN. L. REV. 923 at 927.

expose the user to easy intrusions to privacy. Consider the telephone, which led to wiretapping and caller identification. These developments made it necessary for regulations to be imposed and legal boundaries considered.[144]

Privacy protection has developed part and parcel with efforts to regulate technology (also known as "code," a term made famous by Lawrence Lessig in his book, *Code and Other Laws of Cyberspace*[145]). Regulation can be achieved either through imposing laws (such as forbidding wiretapping without a warrant) or by erecting walls (such as allowing the use of a caller-identification unit that can take advantage of telecommunications code to identify callers).[146] However, despite its heavy influence, "architecture is not pre-determined" and "can be made subject to reason, public debate, and the rule of law."[147] On the internet, code permits not only considerable collection, but also undetected collection. There are no walls to protect the flow of personal data. Although cookies may pop up to inform the user they are being set, many cookies never get noticed. They sit in the consumers hard-drive until they expire. This is the code we have. Effective enforcement of privacy standards will depend on adapting to it.

Professor Lawrence Lessig convincingly argues that the internet can be governed by architectural techniques ("code") to protect fundamental and constitutional values. He also illustrates that the same architecture or code can be used to destroy those values.[148] The truth of this is undisputed; however the impact of this concept is widely discussed.[149] For purposes of this article, however, the fact that code plays a predominant role in the governing of fundamental rights is taken as a given. Further, as communication technologies become more sophisticated, numerous devices are capable of using the internet, all with different operating systems (and therefore different codes). Consider Microsoft's closed source software, Linux's open source software, Palm, Inc.'s

144. Consider two widely cited U.S. Supreme Court cases, Olmstead v. United States, 277 U.S. 438 (1928). Although the majority held that telephone conversations were not protected within the 4th Amendment, Justice Brandeis dissented on the ground that time works changes and brings into existence new conditions and purposes. Katz v. United States, 389 U.S. 347 (1967). One has a reasonable expectation of privacy in a telephone booth.

145. *See infra* note 154.

146. *See* Paul Schiff Berman, *Cyberspace And The State Action Debate: The Cultural Value Of Applying Constitutional Norms To Private Regulation*, 71 U. COLO. L. REV. 1263-64 (2000). Although Professor Berman is primarily concerned with the State Action Doctrine of the 14th Amendment, he states that "it is important to realize that both the law and the wall function as regulatory tools."

147. Rotenberg, *supra* note 65 .

148. *See* Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE (1999).

149. *See generally Rotenberg, supra* note 65; Lawrence Lessig, *Cyberspace and Privacy: A New Legal Paradigm?* 52 STAN. L. REV. 987 (2000); and David Post, *What Larry Doesn't Get: Code, Law, And Liberty In Cyberspace*, 52 STAN. L. REV. 1439 (2000).

hand held devices, and the variety of internet capable cellular telephones. Each of these use the internet to communicate and each of these is capable of collecting and transmitting data.

The code itself is secondary to the fundamental rights of consumers. The safety net provided by the SHP does not distinguish between codes any more that it distinguishes retail transactions from wholesale (i.e. not at all).

Increased use of the e-marketplace will create an educated consumer base and familiar landscape. Consumers could then watch out for each other. Consider the Neighborhood Crime Watch programs.[150] If a violation is spotted, it is reported to the proper authorities. In the case of internet privacy, a data collector who abuses consumer privacy and personal data can be reported by those in the "neighborhood." Therefore, with the proper tools the consumer can work with the code of the e-marketplace and play a valuable role in the enforcement of standards.

3. For The Do-It-Yourself'ers: Privacy And Data Protection Technology

The e-marketplace is what we make of it. It provides mass-customization by default. The sites I visit, the products I buy, and the services I use are all a product of my preferences. My preferences are also valued for the information that it reveals about me.[151] I accept this; however, I also want some control.

Development of an open source system that codes my preferences may be above my abilities and is generally reserved to those sophisticated enough to develop software programs. As Paul Schwartz discussed in the third section of *Privacy and Democracy in Cyberspace,* it may be best to have a variety of privacy protection devices and techniques.[152] Fortunately, software developers are creating programs to expose industry practices. Examples include: Platform for Privacy Preferences (P3P)[153]; Firewalls; and/or Microsoft's Beta security

150. For an example of a Neighborhood Crime Watch program *see* http://www.state.ma.us/dhcd/components/crimewatch/programs.htm.

151. Professor Schwartz states that "information technology in cyberspace also affects privacy in ways that are dramatically different from anything previously possible. By generating comprehensive records of online behavior, information technology can broadcast an individual's secrets in ways that she can neither anticipate nor control. Once linked to the Internet, the computer on our desk becomes a potential recorder and betrayer of our confidences. In the absence of strong privacy rules, cyberspace's civic potential will never be attained." Schwartz, *supra* note 29 at 1610-11.

152. *Id.* at 1681-1701 (1999). Although Professor Schwartz does not specifically advocate software developments as a means of protecting the consumer, he recognizes that one technique alone may not be enough.

153. P3P is a filtering technology developed by the World Wide Web Consortium. Once a consumer downloads P3P and responds to questions, P3P reviews website's privacy policies and notifies the consumer if the policy does not conform to the preferences indicated. Consumers can also set preferences in their browsers to control data released and are notified if more information is requested. *See* http://www.w3.org/P3P.

patch for Internet Explorer 5.5.[154] There are numerous other products also, information for which is easily accessible on the internet.[155]

These software developments facilitate consumer education and independence. If you do not want your home broken into, put locks or an alarm on the door. Consumer technology works in a similar manner. P3P lets consumers program their browsers to alert them of incompatible requests for data. It then allows the consumer decide when to "open the door" and let data go.[156] However, this alone is not enough without the SHP. It places the burden of protection on consumers.

Although consumers need to be informed decision makers, they should not be solely responsible. As Graham Pearce and Nicholas Platten observe in their article *Orchestrating Transatlantic Approaches To Personal Data Protection: A European Perspective*, products such as P3P "must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals."[157] Therefore, products like P3P, that shift data protection responsibility from data collectors to data subjects, fall short of the privacy protections prescribed by the E.U.

Microsoft's beta patch is also a good step toward educating consumers. Many consumers are just learning about cookies and this technology not only helps explain where they come from and what they do, but also gives consumers an easy way to check cookies installed on their computers and be notified of who planted them. Consumers are also given the option to refuse third party cookies.[158] However, as Microsoft's director of corporate privacy, Richard Purcell, has stated, cookie management "alone is not the answer to consumer privacy" ... but it will help "facilitat[e] online privacy."[159]

This distinction between first and third parties raises concern all its own. When does an entity become a third party? Is a parent a third party if data is collected by a subsidiary? What about longstanding affiliations and symbiotic relationships, where both parties exist for mutual cooperation? Consider the

---

154. The beta patch is a means of "cookie-management" for Internet Explorer 5.5. "The new features will automatically provide consumers with a clearer understanding of different types of cookies and where they originate—as well as an easy way to manage and delete them." *See* http://www.microsoft.com/presspass/features/2000/jul00/07-20cookies.asp.

155. A good start for many privacy enhancing technologies is available at http://www.ntia.doc.gov/ntiahome/privacy/900workshop/demoslist3.htm.

156. *See* World Wide Web Consortium, PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT *at* http://www.w3.org/P3P.

157. Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches To Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L. L. J. 2024 at 2044-47 (1999).

158. *See* http://www.microsoft.com/presspass/features/2000/jul00/07-20cookies.asp.

159. *Id.*

case of Toys 'R' Us.com and Coremetrics, data analysis services. A class action suit was brought against Toys 'R' Us because Coremetrics was obtaining personal information including "customer names, addresses, and other sensitive data" from Toys 'R' Us shoppers.[160] This "sharing" of information was discovered by "Internet security expert Matt Curtin."[161] Although Toys 'R' Us has ended this relationship, the issue illustrates why a safety net like the one created through the SHP is an important step, yet is strengthened by technologies and services made available to consumers.

Alone, consumer privacy technology creates a "bottom-up" method of protection, and regulations alone create a "top-down" method. The SHP, when viewed in light of emerging technologies and services, offer a middle of the road approach. The establishment of adequate privacy and data protection to consumers alone will not ensure high standards[162], but enabling consumers to take an active role in privacy protection facilitates the development of a consumer-friendly e-marketplace.

Although the individual should be part of the privacy and data protection process, "it can no longer reasonably be considered the only part."[163] The SHP promote consumer involvement in the data collection process. However, they also impose responsibilities on the data collectors and government, thus balancing the competing interests in the e-marketplace.[164]

In addition to developments in technology, developments in consumer services also protect the consumer. These services have some advantages over the technology. As we will see, they create a system where those with knowledge and experience assist those without.

---

160. Chris Oakes, *Toys R Us Ends Data Practice?*, Aug. 16, 2000.

161. Chris Oakes, *Lack of Notice Snags E-Service*, Aug. 2, 2000.

162. Professor Schwartz uses the term "autonomy trap" to illustrate that "a critical mass of sophisticated privacy consumers is not yet emerging" and "the rest of us cannot free-ride on the efforts of those who are more savvy about data privacy on the Internet." Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 822 (2000). However, Professor Schwartz uses this "autonomy trap" situation as a spring board for advocating regulatory standards. These standards would establish a safety net much like the Safe Harbor Principles which require care and responsibility of data collectors.

163. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000).

164. *Id.* at 880. Professor Cate points out that "United States has historically balanced competing interests" and "identifying the constitutional standard by which those balances are achieved has been one of the major tasks of the Supreme Court in the latter half of the twentieth century."

VII. THIRD PARTIES TO THE RESCUE: PROVIDING KNOWLEDGE AND KNOW-HOW TO CONSUMERS

As discussed above, the majority of consumers may not be knowledgeable enough to program their own operating system or develop monitoring technology. Fortunately, we are living in a time of entrepreneurial productivity and the internet has spurred considerable entrepreneurial activity. Where software developments have left off, third parties have taken the initiative to create non-governmental consumers' assistance and protection companies. These companies are often referred to as "trusted third parties" or "info-mediaries." The concept is not complicated. Essentially, they act as middle-men and monitor the e-marketplace for the consumer. Because it may be impractical for consumers to investigate privacy policies themselves, these third parties can be hired to do the legwork and report the results.

Examples of these third parties include: TRUSTe[165], BBBOnline[166], and The Personalization Consortium.[167] There are others which are easily accessible through the internet.[168] Each of these organizations approach privacy and data protection from a different perspective which are reflected in their services and goals. However, they all educate and assist in the development of privacy policies. Professor Schwartz has noted that these third parties can also provide value to the e-marketplace by providing "a venue for seeking redress after violations of privacy agreements."[169] Although it is clear that these services alone provide inadequate protections to consumers, they can become effective

---

165. *See* http://www.truste.com. "TRUSTe is an independent, non-profit privacy initiative dedicated to building users' trust and confidence on the Internet." They have developed a privacy seal program that alerts consumers to the protections provided while also assisting data collectors in the management of consumer personal data.

166. *See* http://www.bbbonline.org. BBBOnline is a subsidiary of the Council of Better Business Bureaus that also offers services to both business and consumers. It has created a seal that identifies "companies that stand behind their privacy policies and have met the program requirements of notice, choice, access and security in the use of personally identifiable information." BBBOnline also provides means for consumers to file complaints.

167. *See* http://www.personalization.org. Developed by and for marketing companies, including Doubleclick, PricewaterhouseCoopers, KPMG, and American Airlines "to promote the development and use of responsible one-to-one marketing technology and practices on the World Wide Web ... by expanding the scope and use of personalization technology that respects consumer privacy." Although clearly the effort of marketing firms, this consortium provides services and a forum that seeks to develop the e-marketplace in light of consumer concerns over privacy and data protection.

168. Examples include but are not limited to: PNI, *available at* http://www.privacyrights.org; the Online Privacy Alliance, *available at* http://www.privacyalliance.org; the Network Advertising Initiative, *available at* http://www.networkadvertising.org, and the ISA Service Provider Principles / Individual References Industry Principles *available at* http://www.bna.com/e-law/docs/dbguides.html.

169. Schwartz, *supra* note 29, at 1681 (1999).

catalysts for upholding the standards imposed by privacy directives such as the SHP.

There are limits to the effectiveness of these third parties, though. A chain is created that distances the consumer from the e-marketplace. This distance is potentially a weakness. Without direct participation, consumer values and conveniences to consumers might be sacrificed. The consumer's fate is also being trusted to a third party. Although that third party would hopefully be looking out for the best interests of the consumer, the consumer would not be playing any role in the monitoring of privacy policies and accuracy of information collected. This is contradicts the SHP and the spirit of openness that they embrace. An open marketplace will benefit from diversity of input. Third party services can play the valuable role of informing, educating and otherwise serving consumers, thereby enhancing the sophistication of the marketplace.

Alone, neither technology nor services will solve privacy and data protection concerns, but taken together with the standards created through the SHP consumer privacy concerns are greatly reduced.[170] The SHP create a safety net that facilitates exchanges in a global e-marketplace.

VIII. CONCLUSION

Just as the E.U. Data Directive was not "a radical departure from existing privacy laws" in European countries and was therefore easily adopted in "effort to harmonize commerce and privacy rights,"[171] the SHP are not a radical departure from current U.S. approaches to the protection of consumer privacy and use of personal data. The SHP were designed to "fill in [...] gaps in United States privacy statutes"[172] and therefore do not conflict with previous U.S. developments.

Commerce has been a tremendous avenue for growth and both consumers and service providers have legitimate concerns in the e-marketplace.[173] The SHP are sensitive to such concerns and benefit everyone in the e-marketplace:

---

170. Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L. J. 759, 768 (1999). "The only enemy is in the extremes." Although Professor Lessig was commenting on the difference between open and closed source software, the principle applies well to the case at hand. Consumer privacy and data protection is best served through the use of complementing systems.

171. Peter P. Swire & Robert E. Litan, *None Of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, 12 HARV. L. J. & TECH. 683 at 683.

172. Fromholz, *supra* note 125, at 476.

173. The trade of personal information itself has considerable value in the marketplace. The U.S. FTC, in a case concerning the "sale of target marketing lists, with consumer information" found that "The total gross annual revenue of companies supplying consumer direct marketing lists and file enhancement data may be $1.5 billion." In re Trans Union, FTC Docket No. 9255, at 53 (July 31, 1998) *available at* http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf.

consumers, because the SHP lay the groundwork required for active consumer involvement in the data collection process; commercial business, because the SHP allow continued collection of consumer data with minimal practical restraints; and governments, because the SHP provide groundwork for effective and meaningful legislation adaptable to a globalized era.

Legislative action is a prudent step to ensure the future of the SHP. Comprehensive consumer privacy protection legislation would "improve the functioning of a privacy market and play a positive role in the development of privacy norms."[174] Professor Schwartz outlined two steps that Government could take. The first step is to "discourage a default of maximum information disclosure" and two "encourage a market for privacy enhancing technology."[175] As discussed above of these is addressed by the SHP.

The purpose of this article has been to illustrate that adopting the SHP will level the playing field on which consumers and commercial interests coexist. A safety net is necessary, one that will require minimum standards and create an environment of openness. The Safe Harbor Principles do just that.

174. Schwartz, *supra* note 162, at 816-17.

175. *Id.* at 854.