

**TRANSBORDER PRIVACY PROTECTION:
DOES IT HELP U.S. CONSUMERS?**

by

Diane MacDonald and Judith Ramaglia***

CITE AS 5 ALSB INT'L B LAW REV 16

Copyright 2005 by Diane MacDonald and Judith Ramaglia
macdondb@plu.edu, ramaglia@plu.edu

INTRODUCTION

The U.S. has long had a love hate relationship with the concept of protecting personal information.¹ Celebrity information feeds an industry of peeking into the lives of the rich and famous. Reality TV not only identifies individuals, it often showcases them in their most private moments. In other circumstances individuals value privacy, particularly when it relates to keeping personal information out of the hands of government agencies. Many of the privacy statutes enacted over the last four decades reflect exactly this concern: that government should be restrained in its ability to access information about the private lives of its citizens.² Furthermore, information that is available to government, such as tax records, should not be used against citizens without safeguards to allow a contest of government action.³

Individuals also value privacy when the information is personal, embarrassing, and made public without their consent. It may be another individual or media organization that is in possession of the information. In this case individuals are left to their own devices to stop the offending use of information by bringing a private action based on the tort of invasion of privacy. The tort, however, provides minimal protection against the disclosure of personal information obtained through means other than illegal means.⁴

* Associate Dean, School of Business, Pacific Lutheran University

** Professor, School of Business, Pacific Lutheran University, Tacoma, WA

¹ For purposes of this paper, personal information and personal data are used interchangeably. The definition of personal data is information that identifies or is identifiable to a particular individual.

² See, e.g., Freedom of Information Act of 1966, 5 U.S.C.S. §552 (2004) (LEXIS through P.L. 108-301) (giving individuals access to information files collected by government and its agents including electronic files); Privacy Act, 5 U.S.C.S. § 552a (2004) (LEXIS through P.L. 108-301) (regulating the collection and use of personal information by federal executive branch agencies).

³ See, e.g., Taxpayer Bill of Rights 2, 26 U.S.C.S. § 7802 (2004) (LEXIS through Pub. L. 108-301) (creating the office of taxpayer advocate).

⁴ James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 29-35 (2003).

In their 1890 article in the Harvard Law Review exploring the nature of the right to privacy, Samuel Warren and Louis Brandeis noted that

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone.” Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”⁵

Warren and Brandeis were concerned with the evils of newspapers spreading gossip. “To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.”⁶ One can only imagine the reaction of Warren and Brandeis to today’s world of electronic monitoring and data collection.

Electronically gathering, distributing and using personal information for commercial purposes is one of those legal activities that likely preclude the kind of private action envisioned by Warren and Brandeis. The call for regulation of data collection has intensified in recent years due to the growing problem of identity theft.⁷ The attendant cost to the victim as well as the difficulty in correcting erroneous information that has been widely electronically disseminated has heightened awareness of the consequences when personal information is not secured.⁸

Although government data collection practices are regulated by statute and private invasions of privacy are remedied through private court action, the government regulators’ stance regarding the commercial collection of personal data has been one of accepting and even promoting industry self-regulation. Although there is evidence that self regulation has failed both to protect individuals’ private information and to protect against misuse of private information, U.S. legislators have been reluctant to impose statutory limitations on the information gathering activities of commercial enterprises or to regulate the use of such information once acquired.⁹

Legal writers in the U.S. have both applauded and lamented government inaction in regulating electronic commerce in general and the business of data gathering in particular.¹⁰

⁵ Samuel Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 202 (1890) (analyzing the existence of the right to privacy and the remedies available to redress an infringement of that right).

⁶ *Id.* at 196.

⁷ See generally Stephanie Byers, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141 (2001) (discussing the impact of transnational identity theft and concluding that stricter privacy laws limiting access to personal information would decrease instances of identity theft).

⁸ See generally Erin Suzanne Davis, *A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet*, 12 WASH. U.J.L. & POL’Y 201, 203-04 (identifying steps the international community can take to reduce international identity theft).

⁹ See Marsha Cope Huie et al., *The Right to Privacy in Personal Data: the EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT’L L. 391 (2002) (advocating a Constitutional amendment to guarantee privacy because of the failure of the judiciary and Congress to support an omnibus privacy statute).

¹⁰ Will Thomas DeVries, *Annual Review of Law and Technology: III. Cyber Law: Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283 (2003) (recognizing that the changing nature of privacy in an electronic environment calls for new approaches to systematically address privacy violations and remedies); Jay P. Kesan, *Private Internet Governance*, 35 LOY. U. CHI. L.J. 87 (2003) (maintaining the view that self-regulation alone without some level of government regulation is ineffective); Joel R. Reidenberg, *Restoring Americans’ Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999) (proposing a privacy commission to preserve the balance between individual privacy and industry needs); Shaum A. Sparks, *The Direct Marketing Model and Virtual Identity: Why*

This lack of consensus in the legal profession and among legislators reflects the same lack of consensus among those in industry.¹¹ The industry position is dictated by its economic interests with regard to the data collection practice at issue. Many have noted with irony the activities of those companies which are the ultimate examples of data collection enterprises, the credit reporting companies. On the one hand their business is to collect as much personal data as possible and sell that data for profit; on the other hand they offer to sell to the data subjects, protection from the unauthorized use of that data through annual subscription services.¹² Advances in technology make it increasingly easier and less costly to collect and store personal data and to correlate and use the data in ways previously unimagined. The collection techniques are both overt and surreptitious.¹³

European companies, in particular those operating in member states of the European Union (EU), face greater challenges in collecting personal data due to the consensus position of governments and individuals alike: personal privacy is a fundamental human right. The Convention for the Protection of Human Rights and Fundamental Freedoms declares that “everyone has the right to respect for his private and family life, his home and his correspondence.”¹⁴ This basic philosophical assumption was an outgrowth of the World War II experience¹⁵ and one can assume is further fueled by those governments still attempting to

the United States Should Not Create Legislative Controls on the Use of Online Consumer Personal Data, 18 DICK. J. INT’L L. 517 (2000) (asserting that regulation will stifle the information age and summarizing the costs of regulation); Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL’Y 87 (2001) (maintaining that privacy regulation will “chill the creation of beneficial collective goods” and be too burdensome for society as a whole); David Raj Nijhawan, *The Emperor Has No Clothes: A Critique of Applying the European Union approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939 (2003) (discussing how a European style of regulatory scheme would conflict with the First Amendment of the US Constitution and contradict the traditional U.S. approach to privacy values); Angela Vitale, *The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT’L L. 321 (2002) (cautioning against adopting the European Union approach to privacy regulation because it is contrary to free speech and may be economically detrimental); William J. Clinton and Albert Gore, Jr., *Framework for Global Electronic Commerce*, July 1, 1997, at <http://www.nyls.edu/cm/c/papers/whgiiifra.htm> (last visited Aug. 15, 2004) (encouraging the creation of uniform commercial principles along the line of the Uniform Commercial Code to regulate electronic commerce and adopting the position with respect to privacy protection that “private efforts of industry working in cooperation with consumer groups are preferable to government regulation”).

¹¹ A recent example of industry discord over a consumer privacy issue occurred over the Federal Trade Commission’s Do Not Call Registry. When first proposed in 2003, the registry was overwhelmingly favored by consumers and immediately attacked by the telemarketing industry on first amendment grounds. The rule was ultimately upheld as a valid commercial speech regulation. For an overview of the regulation, consumer support and industry reaction, see *Mainstream Marketing Services et al. v. Federal Trade Commission* (No. 03-1429) (10th Cir. Feb. 17, 2004), available at <http://www.kscourts.org/ca10/cases/2004/02/03-1429.htm>. For a strong statement of consumer need for privacy protection in this area, see Brief of Amicus Curiae AARP at 4-15, *Mainstream* (No. 03-1429) available at <http://law.richmond.edu/jolt/v10i4/article35.pdf> (last visited Aug. 16, 2004).

¹² For one example, see the Credit ManagerSM subscription service offered by Experian, <http://www.experian.com>. This is not unlike the call blocking services offered by telephone companies to eliminate telemarketing calls.

¹³ See Nehf, *supra* note 4, at 20-23 (summarizing the impact of new technologies on the ability of direct marketers to acquire information surreptitiously).

¹⁴ Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8, *opened for signature* Nov. 4, 1950, Europ.T.S. No. 005 (September 3, 1953) (herein Convention for Human Rights), <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> (last visited Aug. 16, 2004).

¹⁵ Jason A. Kotzker, *The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad*, 15 ST. THOMAS L. REV. 727, 747-50 (2003) (describing how the EU view of regulation was a reaction against the Nazi misuse of personal information). See also Huie, *supra* note 9, at 441-42 (describing the affect of World War II on the European view of privacy).

cleanse the population of undesirables. Because of the underlying assumption of privacy as a human right, European governments have more actively addressed concerns over the business of gathering personal data about individual citizens and the use made of that data. Rather than adopt the industry self-regulation approach, European governments have adopted specific legislation regulating the collection and use of personal data.

This article will briefly summarize the history of privacy regulation in the EU and the U.S. It will then describe one way in which U.S. companies are meeting the EU regulatory requirements relating to the transborder transmission of personal data by self-certifying compliance with EU privacy regulations. The article then addresses the question: Does a regulatory system result in greater personal data privacy protection than a system that relies on industry self-regulation? An answer is attempted by analyzing the results of a survey conducted to determine if there is any difference in the privacy protection policies of U.S. companies that certify compliance with EU privacy regulations and the privacy protection policies of U.S. companies that choose to self-regulate.¹⁶

A BRIEF HISTORY OF PRIVACY REGULATION: THE UNITED STATES

The U.S. does not have a national law protecting personal information. Only ten state constitutions explicitly recite a right to privacy; the U.S. Constitution does not.¹⁷ The courts have implied a right to privacy with respect to certain aspects of an individual's life, such as reproductive rights, but not with respect to privacy of an individual's identity.¹⁸ In such Constitutional cases, the individual's privacy is secured against unreasonable government intrusion. Furthermore, the U.S. Congress (Congress) chooses to take a patchwork approach to protecting individual privacy, often in reaction to a particular problem coming to the attention of the electorate. So, for example, when Robert Bork's video rental records were released by the media during his 1987 Supreme Court confirmation hearings, Congress passed legislation to protect video rental privacy.¹⁹ States collected personal data from licensed drivers as part of motor vehicle records. This included information such as a person's name, address and even social security number, the key to obtaining credit, employment, and social welfare benefits. Many states sold or otherwise made the data available to commercial information vendors and

¹⁶ Portions of this article and the preliminary survey results were presented as conference papers. See Diane MacDonald & Judith Ramaglia, *US Companies Dance to EU Tune: A Lesson in Privacy Protection*, International Conference on Industrial Organization, Law and Economics, Chalkidiki, Greece, 17-20 June 2004 (Forthcoming in *Proceedings 2004*) (discussing the differences between the EU and U.S. concepts of privacy protection and how U.S. companies are complying with EU requirements, and presenting the raw data from the survey); Judith Ramaglia & Diane MacDonald, *Doing Business the EU Way*, Proceedings 6th Conference of Emerging Issues in Accounting, CD-ROM (June 2004) (discussing preliminary results of the survey and implications for auditors and accountants).

¹⁷ See National Conference of State Legislatures, *Privacy Protections in State Constitutions*, at <http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm> (Aug. 15, 2004) (listing the state constitutions that explicitly protect privacy rights; see also Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 428-29 (2002) (discussing privacy protection in the U.S. Constitution).

¹⁸ For examples of Supreme Court cases dealing with identity privacy, see Kotzker, *supra* note 15, at 730-31.

¹⁹ See Video Privacy Protection Act of 1988, 18 U.S.C. §§2710 (2002), Cornell Legal Info. Inst., available at <http://www4.law.cornell.edu/uscode/18/p1ch121.html> (as of Aug. 16, 2004).

even private individuals. The practice was finally prohibited by the Congress in 1994 after much publicity surrounding the stalker-murder of actress Rebecca Schaeffer.²⁰ It was not until 1998 that Congress passed legislation to make identity theft a crime on a national level.²¹

Commercial Collection of Data

Individuals have had to rely on private actions to preserve their information privacy when collected in a commercial environment. With respect to regulating the commercial aspects of data collection, Congress has chosen to regulate specific industries and/or transactions. Three of the high profile instances of such action include The Health Insurance Portability and Accountability Act (HIPAA) which limits the use of medical information without consent;²² the Financial Services Modernization Act (also known as Gramm-Leach-Bliley Act) which requires financial institutions to disclose their privacy policies and allows a customer to opt-out of having the information made available for other uses;²³ and the Children's Online Privacy Protection Act of 1998 (COPPA) which requires parental consent to collect information online for children under the age of thirteen.²⁴

The Role of the Federal Trade Commission

The Federal Trade Commission (FTC) has been studying the ways companies use their online websites to collect information from those visiting the sites. While the FTC has no explicit authority to enforce privacy rules per se, under Section 5 of the FTC Act it does have an overall authority to monitor businesses and prohibit practices that it determines to be unfair and deceptive.²⁵ In this capacity, the FTC monitored the manner in which businesses collect personal information through their websites and how such practices were disclosed to those individuals visiting the site. The FTC wrote a series of reports to Congress summarizing the findings.

The FTC wrote its first report in 1998.²⁶ The FTC noted that by early 1997 there were fifty-one million adults online, and 73% of them had used the internet to find product information. It also noted that consumers are wary of participating in electronic commerce due to privacy concerns.²⁷ After reviewing government studies and industry association guidelines, the FTC identified what it considered generally accepted core principles of privacy protection within the context of collecting personal consumer information: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress.

²⁰ See The Driver's Protection Act of 1994, 18 U.S.C.S. §§2721-2725 (2004) (LEXIS through P.L. 108-301).

²¹ See Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C.S. §1028 (2004) (LEXIS through P.L. 108-301).

²² Health Insurance Portability and Accountability Act of 1996, Pub. L. No.104-191, 110 Stat. 1936 (1996) available at <http://aspe.hhs.gov/admsimp/pl104191.htm> (last visited Aug. 15, 2004).

²³ Financial Services Modernization Act (Gramm-Leach-Bliley Act) of 1999, 15 U.S.C.S. §§6801-6809 (2004) (LEXIS through P.L. 108-301).

²⁴ Children's Online Privacy Protection Act of 1998, 15 U.S.C.S. §§ 6501-6506 (2004) (LEXIS through P.L. 108-301).

²⁵ John T. Soma, et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L. L.J. 171, 183 & n.134 (2004) (discussing statutory and Congressional authority for the FTC to regulate internet practices).

²⁶ *Privacy Online: A Report to Congress* (June 1998), <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (hereinafter the *1998 Report*) (last visited Aug. 16, 2004).

²⁷ *Id.* at 3 & 46 n.9.

The FTC Fair Information Principles

The FTC fair information principles are briefly described as follows.

1. Notice/Awareness: Most fundamental in the FTC view, is notice of the methods used by the website to collect data. Notice includes identifying who is collecting the data and for what purpose, the identity of all those who will receive the data, the kind of data collected and the manner in which it is collected (overt and surreptitious), the consequence of refusing to supply data and the procedures in place to ensure confidentiality, quality and integrity.²⁸ The FTC noted one of the easiest ways to give notice is to post a privacy policy on the website itself in a conspicuous place which is easy to navigate.
2. Choice/Consent: The second principle allows consumers the option to choose how their own information will be used once it has been collected for the primary stated purpose.²⁹ For example, a consumer purchasing a product will give an email address for purposes of confirming shipment of the product, but may not want it used for solicitations for other products from the same vendor or for solicitations from other vendors. The FTC encourages using the technology available to provide more choice than the opt-in or opt-out options and to allow the consumer to tailor the way the personal information is used.³⁰
3. Access/Participation: The third principle recognizes an individual's right to access the personal information collected and to challenge and correct any inaccuracy.³¹ It requires a mechanism that is inexpensive and easy to use and one in which corrections are passed on to all subsequent users of the data.
4. Integrity/Security: The fourth principle requires that data be accurate in substance (collected from reliable sources and verified), and timely. It should be secured both internally and externally from unauthorized access, use or disclosure.³²
5. Enforcement/Redress: The fifth principle is essential to the effectiveness of the first four. It is in the enforcement/redress section of its report that the FTC discusses the alternatives for enforcement, such as industry self-regulation with appropriate consumer recourse, consumer self-help through creating a statutory private rights of action, and government enforcement with civil or criminal remedies.³³ While endorsing self-regulation in general, the FTC noted that the industry guidelines regarding information practices submitted as part of its study suggested the notice principle most often, and encouraged choice, but mostly ignored access or security and none suggested enforcement mechanisms.³⁴

Principles in Practice

For the 1998 report, when the FTC surveyed the actual data collection practices of 1400 websites, it found that 92% of the websites were collecting personal information, but only 14% made any disclosure about the practices associated with such collection.³⁵ A subset of websites,

²⁸ *Id.* at 7-8.

²⁹ *Id.* at 8-9.

³⁰ *Id.* at 9 & 50 nn.43-44.

³¹ *Id.* at 9.

³² *Id.* at 10.

³³ *Id.* at 10-11.

³⁴ *Id.* at ii.

³⁵ *Id.* at 21-30.

the 111 most popular sites had much better numbers: 97% collected information and 71% had a disclosure of some sort about information practices. The FTC noted, however, that these businesses had advance notice that they would be surveyed.³⁶ In another subset consisting of 620 comprehensive websites i.e., those likely to draw consumers, 92% collected information, but only 14% had any kind of disclosure. The survey reflected the broad industry adoption of the notice principle, but also reflected the lack of adoption of the other fair information principles. For example, 68% of the most popular websites allowed consumers some choice concerning the use of their information, but only 16% addressed issues of security.

Even though the FTC noted that, “the trade association guidelines submitted to the Commission do not reflect industry acceptance of the basic fair information practice principles,” the FTC chose to continue looking for ways to “encourage effective self-regulatory efforts by industry.”³⁷ The FTC’s final recommendations called for government regulatory action in only one area: the collection of information from children age 12 and under.³⁸ Congress subsequently passed COPPA.³⁹

Subsequent Reports

In 1999, the following year, the FTC again examined the privacy practices of online websites, specifically addressing self-regulation.⁴⁰ Sales continued to grow for online business –tripling from \$3 billion in 1997 to \$9 billion in 1998. Online revenues had equally impressive growth.⁴¹ The FTC again reported to Congress on privacy practices, this time based on the results of the Georgetown Internet Privacy Policy Survey (GIPPS).⁴² GIPPS included 361 of the busiest websites and the 100 most popular websites. It indicated that privacy disclosure overall increased, but only 10% of the busiest and 22% of the most popular websites used a disclosure that included all of the fair information principles identified by the FTC in the *1998 Report*.⁴³ The FTC took notice of the development of online seal programs as examples of progress in industry self-regulation.⁴⁴ Programs noted in particular were TRUSTe,⁴⁵ and BBBOnLine.⁴⁶ Notwithstanding, the FTC still concluded that, “although the results of the GIPPS . . . show that many online companies now understand the business case for protecting consumer privacy, they

³⁶ *Id.* at 28-29 & 59 n.122.

³⁷ *Id.* at 41

³⁸ *Id.* at 42.

³⁹ Children’s Online Privacy Protection Act of 1998, *supra* note 24.

⁴⁰ *Self-Regulation and Privacy Online: A Report to Congress* (July 1999), <http://www.ftc.gov/os/1999/07/privacy99.pdf> (hereinafter the *1999 Report*) (last visited Aug. 16, 2004).

⁴¹ *Id.* at 1 & 15 nn.5-6.

⁴² *Id.* at 7 & 18 n. 33.

⁴³ In surveying the fair information practices, GIPPS included the first four of the practices identified in the *1998 Report*, i.e. notice/awareness, choice/consent, access/participation, and security/integrity, but did not include the fifth principle identified in the *1998 Report*, enforcement/redress. *See id.* at 6.

⁴⁴ A seal program is one in which an organization, such as the Better Business Bureau, allows a licensee to display a seal of the issuing organization (the licensor) to indicate adherence to a set of business principles promulgated by the licensor, such as incorporating fair information practices into website privacy policies.

⁴⁵ TRUSTe is a non-profit organization founded by the Commerce.Net and the Electronic Frontier Foundation. See the TRUSTe website for extensive information about the seal program, including requirements for privacy policies, costs, and dispute resolution processes, <http://www.truste.org>.

⁴⁶ BBBOnLine is the arm of the Council of Better Business Bureaus that deals with websites. See the BBBOnLine website for extensive information about the seal program, including requirements for privacy policies, costs, and dispute resolution processes, <http://www.bbbonline.org>.

also show that the implementation of fair information practices is not widespread among commercial Web sites.”⁴⁷

In 2000 the FTC conducted yet another survey of online privacy practices.⁴⁸ Once again the report took notice of the increased use of the Internet for consumer purchases and the continuing concern of consumers over issues of information privacy.⁴⁹ This time the survey included 335 of the busiest websites and 91 of the most popular sites. While the *2000 Report* refers to the fair information practices described in the *1998 Report*, the *2000 Report* identifies the core principles of privacy protection as notice, choice, access, and security.⁵⁰ In this survey, 97% of the busiest sites and 99% of the most popular sites collected personal data. While the vast majority of sites (88% and 100% respectively) had privacy disclosures, only 41% of the busiest sites and 60% of the most popular sites included both notice and choice, and only 20% of the busiest sites and 42% of the most popular sites incorporated all of the fair information principles.⁵¹

Although the *2000 Report* no longer identifies it as a core fair information practice, enforcement is still essential to ensure the protection nominally provided in the four core principles of notice, choice, access and security.⁵² In the *1999 Report* the FTC was optimistic about the development of seal programs. In the *2000 Report* the FTC noted that seal programs were displayed on only 8% of the busiest and 45% of the most popular websites.⁵³ As a consequence, the FTC recommended that Congress enact legislation in addition to industry self-regulation to ensure privacy safeguards for personal information collected online. “The Commission believes that industry’s limited success in implementing fair information practices online, as well as ongoing consumer concerns about Internet privacy, make this the appropriate time for legislative action.”⁵⁴ Congress has not yet passed such legislation and the current US regulatory scheme is still one of primarily industry self-regulation.

The Progress and Freedom Foundation Survey

A subsequent survey was commissioned by the Progress & Freedom Foundation, a self-described “market-oriented think tank.”⁵⁵ The survey was conducted by Ernst & Young and was intended to update information on privacy practices of online businesses since the *2000 Report*.⁵⁶ It modeled the methodology of the *2000 Report* so that the data could be compared to the data in the *2000 Report*.⁵⁷ The samples surveyed included the eighty-five busiest sites (Most Popular Group), a random sample of sites with greater than 39,000 unique visits (Random Sample), and a

⁴⁷ *Id.* at 12.

⁴⁸ *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress* (May 2000), <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> (hereinafter *2000 Report*) (last visited Aug. 16, 2004).

⁴⁹ *1999 Report*, *supra* note 40, at 1-2.

⁵⁰ *Id.* at 4.

⁵¹ *Id.* at 9-13.

⁵² *Id.* at 20 & 51 n.127.

⁵³ *Id.* at 20.

⁵⁴ *Id.* at 38.

⁵⁵ See The Progress and Freedom Foundation, *About PFF*, at <http://www.pff.org/about/> (describing its mission) (last visited Aug. 16, 2004); see also PFF, *Supporters*, at <http://www.pff.org/about/supporters.html> (listing corporate supporters) (last visited Aug. 16, 2004).

⁵⁶ William F. Adkinson, Jr. et al., *Privacy Online: A Report on the Information Practices and Policies of Commercial Websites v* (Mar. 2002) (herein the *PFF Survey*), available at <http://www.pff.org/publications/ecommerce/0302privacyonlinereport.pdf>. (last visited Aug. 16, 2004).

⁵⁷ *Id.* at v.

subset of the Random Sample consisting of the top 5,625 sites (Refined Random Sample).⁵⁸ With respect to fair information principles, the *PIF Survey* tested for notice, choice, and security practices, but excluded access practices because of the difficulty of formulating the questions and because the researchers questioned the value of the access principle itself.⁵⁹

In summarizing the data, the researchers concluded:

Overall, the findings here suggest evolutionary, not revolutionary, changes in the privacy practices and policies of commercial Web sites. Information continues to be collected, notices continue to be posted, choices continue to be offered, generally in proportions comparable to those found by the FTC 21 months earlier.⁶⁰

A BRIEF HISTORY OF PRIVACY REGULATION: THE EU

In contrast to the approach taken by the U.S., privacy protection in the EU is a part of its regulatory activity. After World War II, many individual nations passed laws attempting to protect personal privacy.⁶¹ The Council of Europe's (COE)⁶² adoption of the *Convention on Human Rights* (with its privacy provisions) was one of the first efforts to create a multinational basis for personal privacy protection.⁶³

The OECD Guidelines

In 1980 the Organisation for Economic Co-operation and Development (OECD)⁶⁴ made a second major attempt to articulate a multinational set of privacy practices. The OECD recommended to its member states the *Guidelines on the Protection of Privacy and Transborder Data Flows* (Guidelines).⁶⁵ The Guidelines were an attempt to harmonize national laws to accomplish both the protection of the fundamental right of privacy while enabling the free flow of data across

⁵⁸ *Id.* at vii.

⁵⁹ *Id.* at 12.

⁶⁰ *Id.* at 27.

⁶¹ Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 *Fordham L. Rev.* 2777, 2782-84 (describing the legislation in Europe predating the 1995 privacy directive).

⁶² The COE was founded in 1949 for purposes of creating European unity in defending human rights, parliamentary democracy and the rule of law. Originally founded by the ten countries of Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden, and the United Kingdom, it now includes forty-five countries, including 21 from Central and Eastern Europe. It is separate and distinct from the EU, but all EU countries are members of COE. See Council of Europe, *The COE in Brief*, at <http://www.coe.int/defaultEN.asp> (last visited Aug. 16, 2004).

⁶³ Convention for Human Rights, *supra* note 14.

⁶⁴ The OECD is an organization of thirty member nations who develop and define economic and social policies designed to address common problems of globalization and to promote democratic government and market economies. It issues both binding agreements and nonbinding recommendations. See Organisation for Economic Co-operation and Development, *About OECD*, at <http://www.oecd.org> (last visited Aug. 16, 2004).

⁶⁵ Organisation for Economic Co-operation and Development: Council Recommendation Concerning Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data, (Sept. 23, 1980) available at http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html (last visited Aug. 17, 2004). The Guidelines took the form of a recommendation to member states and represent a consensus on basic principles that should be incorporated into national legislation dealing with the transborder transfer of personal information.

national borders and removing unjustified obstacles to these data flows.⁶⁶ The Guidelines identify the following principles as the “basic principles of national application”: collection limitation, data quality, purpose specification, use limitation, security safeguarding, openness, individual participation, and accountability.⁶⁷ Since the Guidelines are only a recommendation, there is no requirement that member nations implement them with national legislation.

The Data Processing Convention

The COE acted again in 1981 when it passed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Data Processing Convention).⁶⁸ “(I)t is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.”⁶⁹ The Data Processing Convention acknowledged that economic unification required data to flow across national boundaries, and data could only flow if there was harmony in the various privacy laws among member states. The core principles of data collection were identified as: quality of the data, safeguards for sensitive data, data security, ability of data subject to access and correct data, and sanctions and remedies for violations.⁷⁰ Both the OECD and the Commission of the European Communities (EEC) were in close collaboration in drafting the Data Processing Convention.⁷¹

The Privacy Directive

From the brief histories of privacy protection, it is evident that the European model and the U.S. model have significant and perhaps irreconcilable differences. These differences became most apparent when the EU adopted its most recent form of regulation: EU Directive 95/46/EC of 24 October 1995 (Data Protection Directive).⁷² The Data Protection Directive (DPD) is part of the European plan to eliminate barriers to “economic and social progress by common action . . . on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.”⁷³ These fundamental freedoms of natural persons include “in particular their right to privacy with respect to the processing of personal data.”⁷⁴ To comply with the DPD, each of the nations belonging to the EU (Member States) must create national legislation to implement its requirements⁷⁵ and create a public authority to monitor compliance.⁷⁶ Many of the privacy

⁶⁶ *Id.* at Preface.

⁶⁷ For definitions of each of the Guidelines principles, *see id.* at paras. 7-14.

⁶⁸ *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108, <http://conventions.coe.int/Treaty/en/Treaties/HTML/108.htm> (last visited Aug. 16, 2004).

⁶⁹ *Id.* at Art. 1.

⁷⁰ *See id.* at Arts. 5-10 (defining and explaining the core principles).

⁷¹ *See Explanatory Report*, in Convention, *supra* note 68, paras. 14-16, <http://conventions.coe.int/Treaty/en/Reports/HTML/108.htm> (last visited Aug. 16, 2004).

⁷² Council 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, 1995 O.J. (L281) 31, http://europa.eu.int/comm/internal_market/privacy/law_en.htm. A directive is a legislative act of the European Commission that establishes regional policy, but leaves specific legislation to implement the policy to each member state. *See* RALPH H. FOLSOM, EUROPEAN UNION LAW IN A NUTSHELL 34-37 (1999).

⁷³ *Id.* at 31.

⁷⁴ *Id.* at 38.

⁷⁵ *Id.* at 49.

⁷⁶ *Id.* at 47.

principles mandated by the DPD can be traced to the principles and practices adopted in the Guidelines and the Data Processing Convention. The EU privacy principles include: notice, choice, onward transfer, security, data integrity, access, and enforcement.⁷⁷

The DPD governs personal information data flows and is very broad in scope. Its provisions apply to all methods of collecting and storing information, whether electronic or manual. It applies to both commercial and noncommercial entities and to EU and non-EU nations. For example, it can apply to non-EU companies where an individual's personal information is processed by or on behalf of that company, using equipment located in the EU. It can also apply to non-EU companies where the company has an office or other facility in the EU or acquires a corporate entity within the EU that is processing the personal information of individuals. Furthermore, Article 25.1 of the DPD (Article 25.1) states that "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if ... the third country in question ensures an adequate level of protection."⁷⁸ Article 25.1 creates difficulties for the many nations whose privacy protection regulations do not, in the opinion of the EU, provide an adequate level of protection.

RECONCILING THE REGULATORY AND THE SELF-REGULATORY APPROACHES

The DPD took effect October 25, 1998. It prohibits the transfer of data from Member States to countries that do not adequately protect personal data. The prohibition is not limited to commercial exploitation of personal data. It includes, for example, employee data collected by employers. When General Motors put together a company phone book including employees in all domestic and international offices, it took six months to meet the regulatory requirements in each of the Member States.⁷⁹

At the time the DPD was passed, the U.S. with its self-regulatory scheme and patchwork legislative approach to privacy protection and data collection did not provide adequate protection to personal data. To avoid trade disruption, the U.S. Department of Commerce (DOC), and the European Union Commission (EC) entered into negotiations to create ways in which U.S. companies could choose to comply with the DPD and stay in the information transfer loop. One of the methods of compliance the DOC negotiated was a safe harbor agreement (Safe Harbor) which allows U.S. companies to voluntarily comply with the seven privacy principles described in the DPD (Safe Harbor Privacy Principles). The agreement also contains fifteen frequently asked questions (FAQs) explaining how companies effect and evidence such compliance. The Safe Harbor Privacy Principles and the FAQs were approved by the EC on July 28, 2000 and were deemed to provide adequate protection for purposes of Article 25.1.⁸⁰

⁷⁷ See *id.* at 39-45 (defining and explaining the data privacy principles).

⁷⁸ *Id.* at 45-46.

⁷⁹ David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL ST. J., Oct. 10, 2003, at A1.

⁸⁰ Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 O.J. (L215) 7, 10-12, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_215/l_21520000825en00070047.pdf.

The Safe Harbor Registration

To use the Safe Harbor, organizations register with the DOC by completing a certification form with the organization's name, address, name of officer certifying compliance, contact person and means by which to communicate, a description of the activities and type of personal information received from the EU, a description of the organization's privacy policy and where it is available to the public, the method of verifying compliance and the recourse mechanism to investigate and resolve complaints, and information about sales and the number of employees. All of the information (except that about sales and employees) is posted to the DOC registry and is publicly available through the DOC website.⁸¹ The DOC maintains the registry of organizations which chose to self-certify their compliance, but it is the FTC and the US Department of Transportation (DOT) that monitor compliance. An organization's self-certification and inclusion on the safe harbor list "constitute a representation to the Department of Commerce and the public that it adheres to a privacy policy that meets the safe harbor framework."⁸²

Safe Harbor Privacy Policy

To qualify under the Safe Harbor, an organization must adopt a privacy policy. The privacy policy must reflect all of the Safe Harbor Privacy Principles and include a statement that the organization complies with them.⁸³ Under FAQ 6, an organization registering under the Safe Harbor must:

1. Indicate where its privacy policy is available for viewing by the public and its effective date of implementation,
2. Designate a contact office for the handling of complaints, access requests, and any other issues arising under the Safe Harbor,
3. Identify 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,
4. Identify any privacy programs in which the organization is a member,
5. Have a procedure in place to verify the organization's compliance with the Safe Harbor Privacy Principles (e.g. in-house, third party), and
6. Have an independent recourse mechanism used to resolve complaints (e.g. the seal programs) or choose to cooperate with the European Union Data Protection Authorities (DPAs).⁸⁴

⁸¹ See U.S. Dept. of Commerce, *Safe Harbor List*, <http://www.export.gov/safeharbor/index.html> (June 29, 2004).

⁸² *Id.* It is worth noting that the Safe Harbor meets the requirements of Article 25.1, but companies must still comply with the national laws of the Member States where the data is located. See Commission Decision, *supra* note 78, at 10.

⁸³ See U.S. Dept. of Commerce, *Safe Harbor Workbook*, <http://www.export.gov/safeharbor/index.html> (June 29, 2004).

⁸⁴ See Commission Decision; *supra* note 80, at 15; see also, U.S. Dept. of Commerce, *Helpful Hints Prior to Self-Certifying to the Safe Harbor*, <http://www.export.gov/safeharbor/index.html> (June 29, 2004).

The Safe Harbor Privacy Principles

The Safe Harbor Privacy Principles must be incorporated into a company's privacy policy in order for it to be compliant with the Safe Harbor.⁸⁵ Briefly, the Safe Harbor Privacy Principles are:

1. **Notice:** Organizations must inform individuals in clear and conspicuous language about the purposes and uses of the data, the types of third parties to whom the data is disclosed and who to contact with any inquiries, complaints or requests to limit the use and disclosure of the data. The notice must be given when the data is first collected and again if the data is used for a purpose that differs from the original purpose.
2. **Choice:** Individuals must have an opportunity to opt out of having their personal data disclosed to a third party or used for a purpose that is inconsistent with the original purpose for collecting the data. There must be a mechanism in place to exercise this choice and the mechanism must be clear and conspicuous and readily available and affordable.

With respect to data that is classified as "sensitive information," individuals must affirmatively choose (opt-in) to have the information disclosed to a third party or used for a purpose other than the purpose for which it was originally collected. Sensitive information includes information about medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or sex life.

3. **Onward Transfer:** Disclosing data to a third party is subject to the notice and choice principles explained above. An organization may transfer personal data to a third party that is acting as an agent if it first determines that the third party is providing appropriate privacy protection, in accordance with the Safe Harbor Privacy Principles. If the party transferring data complies with this onward transfer principle and takes reasonable steps to verify correct processing, it will not be liable for mishandling of information by the third party.
4. **Security:** Organizations must take reasonable precautions to protect information from loss, misuse and unauthorized access, disclosure, alteration or destruction.
5. **Data Integrity:** Information collected should be relevant for the stated purpose and used consistently with and be reliable for that purpose, and be accurate, complete, and current.
6. **Access:** Individuals must have access to their data and be able to correct, amend, or delete information where it is inaccurate, so long as the burden of providing access is neither disproportionate to the privacy risks nor would violate the rights of other persons.
7. **Enforcement:** There must be an enforcement mechanism and sanctions in place to ensure compliance with the Safe Harbor Privacy Principles and to address complaints. The mechanisms must include a procedure to investigate complaints, decide disputes and award damages when applicable, a procedure to verify that the privacy policy is followed by the organization, and effective remedies and sanctions for failure to comply with the Safe Harbor Privacy Principles.

⁸⁵ For more detailed definitions and explanations of the Safe Harbor Privacy Principles, see Commission Decision, *supra* note 80, at 10-12.

THE SURVEY

Both the Safe Harbor Privacy Principles and the FTC fair information practice principles require that a privacy policy be disclosed to website visitors. Previous FTC surveys used the publicly available policies to track compliance with its fair information principles. The policies were also used as a basis on which to conduct this survey.

The Issue

The existence of a group of U.S. companies that have certified their compliance with the EU's DPD via the Safe Harbor Agreement (Safe Harbor companies) provides an opportunity to test the following question: is there any difference between the data protection nominally provided by the online privacy policies of Safe Harbor companies and the data protection provided by the online privacy policies of those companies that have chosen to self-regulate? In other words, does a regulatory system result in greater protection (as represented by online privacy policies) of a person's personal data than does a system based on self regulation? To explore this issue a survey was conducted of the privacy disclosures posted on internet websites by two groups of companies: those that have chosen to comply with the regulatory provisions of the Safe Harbor Agreement and those that have chosen to self-regulate.

The Companies

As of February 27, 2004 a total of 463 companies were registered under the Safe Harbor. Eighty of these companies whose privacy policies are posted on internet websites were randomly selected from the list of registered firms maintained by the DOC. For purposes of comparison, a group of eighty companies who choose to self-regulate was generated by randomly selecting forty companies from the list of Fortune 500 companies⁸⁶ and forty companies from the list of INC 500 companies.⁸⁷ None of the companies selected from the Fortune 500 and INC 500 groups was self-certified under the Safe Harbor.

For a company to make the Fortune 500 list its financial information must be publicly available and the company must be subject to U.S. Securities and Exchange (SEC) regulation. The companies must file annual reports of information (10Ks), but they are not required to be publicly traded. The INC 500 companies are the fastest growing small to mid-size companies in the U.S. Their growth is evaluated by calculating the percentage growth in net sales over a four-year period. The financial data is obtained from statements prepared by independent accountants. No publicly traded companies are included in the INC 500. Including companies from each of these two lists provides a broad sample of self-regulating companies.

The Questions:

The Safe Harbor requires U.S. companies to comply with the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. The FTC fair information practices principles (FTC Fairness Principles) are: notice, choice, access, and security. Again, although the FTC no longer identifies it as a core fair information practice principle, enforcement is still essential to ensure the protection nominally provided by the other

⁸⁶ See Fortune, *Fortune 500*, at <http://www.fortune.com> (listing the Fortune 500 companies as of Feb. 27, 2004 and describing the criteria used to determine the listing) (last visited Aug. 24, 2004).

⁸⁷ See INC Magazine, *INC 500*, at <http://www.com> (listing the INC 500 companies as of Feb. 27, 2004 and describing the criteria used to determine the listing) (last visited Aug. 24, 2004).

core principles. The number of the Safe Harbor Privacy Principles is greater than the FTC Fairness Principles, and all of the FTC Fairness Principles and an enforcement requirement are included in the Safe Harbor Privacy Principles. Thus, if a company has chosen to comply with the requirements of the Safe Harbor, it is simultaneously complying with the FTC Fairness Principles.

The online privacy policies of all 160 companies were evaluated on two dimensions: 1) whether or not they were in compliance with all four of the FTC Fairness Principles (notice, choice, access, and security) and 2) whether or not the privacy policies direct the visitor to an enforcement mechanism.

Survey Results: The FTC's Fairness Principles

Table 1 indicates the number of companies in each category whose online privacy policies are in compliance with all of the FTC Fairness Principles. Of the total 160 companies sampled, there are 61 companies in compliance and 99 that are not in compliance. When examined by category, 45 of the 80 Safe Harbor companies but only 16 of the 80 self-regulating companies are in compliance with all of the FTC Fairness Principles.

SEE TABLE 1

Table 2 indicates the percentage of companies in each category whose online privacy policies are in compliance with all of the FTC Fairness Principles. More than half (56.25%) of the Safe Harbor companies are in compliance with all four. Only 20% of the self-regulating companies are in compliance.

SEE TABLE 2

Although the percentage difference is wide, this alone does not indicate whether there is a significant difference between the online privacy policies of the Safe Harbor companies and those of the self-regulating companies. To make that evaluation these data were also subjected to a chi square analysis.⁸⁸

Hypothesis 1- Safe Harbor Companies and Self-Regulating Companies

The null form of the first hypothesis tested is as follows: the privacy policies of Safe Harbor companies and those that have not registered under the Safe Harbor (self-regulating companies) are equally likely to comply with all four of the FTC Fairness Principles. The actual occurrences of companies that are compliant and those that are not are displayed in Table 1. The analysis resulted in a chi square of 22.28. Given the one degree of freedom allowed by the 2 by 2 comparison, this chi square of 22.28 indicates, at a probability level of 0.001, that the null hypothesis should be rejected. In other words, based on these samples, there is less than one chance in a thousand that the Safe Harbor companies and the self-regulating companies are equally likely to comply with all four of the FTC Fairness Principles.

Hypothesis 2- Safe Harbor Companies and Self-Regulating Fortune 500 Companies

Does size make a difference? In order to evaluate whether there is any significant difference between the online privacy policies of Safe Harbor companies and those of the larger Fortune 500 self-regulating companies, an additional hypothesis was tested. The null form of the second

⁸⁸ Chi square analysis is a nonparametric statistical technique appropriate for use with categorical variables. It compares actual frequencies of occurrences with expected frequencies. The resulting chi square statistic is compared with a table of the critical values of the chi square distribution in order to determine significance.

hypothesis is as follows: the privacy policies of Safe Harbor companies and those of Fortune 500 self-regulating companies are equally likely to comply with all four of the FTC Fairness Principles.

As the self-regulating companies had been a combination of those selected from the Fortune 500 and those selected from the INC 500, the 40 Fortune 500 companies were extracted and compared with Safe Harbor companies. To make the sample sizes equal 40 of the 80 Safe Harbor companies were randomly selected for purposes of these comparisons.

The comparison of the 40 Safe Harbor companies and the 40 Fortune 500 self-regulating companies resulted in a chi square of 4.178. This is significant at a probability level of 0.05 or less. Based on these samples, there are fewer than five chances in a hundred that the Safe Harbor companies and the Fortune 500 self-regulating companies are equally likely to comply with all four of the FTC Fairness Principles. The null hypothesis is rejected at the 0.05 level.

Hypothesis 3- Safe Harbor Companies and Self-Regulating INC 500 Companies

The null form of the third hypothesis is as follows: the privacy policies of Safe Harbor companies and those of INC 500 self-regulating companies are equally likely to comply with all four of the FTC Fairness Principles. To evaluate this hypothesis the 40 INC 500 companies and the 40 Safe Harbor companies were analyzed. The comparison resulted in a chi square of 16.81. As this is significant at a probability level of 0.001 or less, the null hypothesis is rejected.

Hypothesis 4-Self-Regulating Fortune 500 Companies and Self-Regulating INC 500 Companies

The final analysis of compliance with FTC Fairness Principles focused on a comparison of the two groups of self-regulating companies. The null form of the fourth hypothesis is as follows: the privacy policies of Fortune 500 self-regulating companies and those of INC 500 self-regulating companies are equally likely to comply with all four of the FTC Fairness Principles. The comparison of the 40 Fortune 500 self-regulating companies and the 40 INC 500 self-regulating companies resulted in a chi square of 5. This is significant at a probability level of 0.05 or less. The null hypothesis is rejected at this level.

Table 3 summarizes the results for the four hypotheses related to compliance with the FTC Fairness Principles. Larger chi squares indicate more significant differences. Thus, the strongest difference is between the Safe Harbor companies and the self-regulating companies (Hypothesis 1). However, in every case the null hypotheses are rejected at the 0.05 or the 0.001 level.

SEE TABLE 3

Survey Results: Direction to an Enforcement Mechanism

The second major question of the survey was whether or not the companies' online privacy policies provide information about enforcement mechanisms. With regard to this issue, Table 4 indicates the number of companies in each category. Table 5 indicates the percentage of companies in each category whose online privacy policies provide direction. Fewer than half (45%) of the Safe Harbor companies direct the reader to an enforcement mechanism. Only 5 % of the self-regulating companies do so.

SEE TABLES 4 AND 5

Again, although the percentage difference is wide, this alone does not indicate whether there is a significant difference between the Safe Harbor companies and the self-regulating

companies. To make that evaluation these data were also subjected to a chi square analysis. The hypotheses related to the various categories compared are parallel to those used in evaluating compliance with the FTC Fairness Principles.

Hypothesis 5- Safe Harbor Companies and Self-Regulating Companies

The null form of the fifth hypothesis is as follows: the privacy policies of Safe Harbor companies and those of the self-regulating companies are equally likely to direct the website visitor to an internal or external enforcement contact. The comparison of the 80 companies in each group resulted in a chi square statistic of 34.13. As this is significant at the 0.001 level, the null hypothesis is rejected.

Hypothesis 6- Safe Harbor Companies and Self-Regulating Fortune 500 Companies

Again, the possible impact of the size of companies on the results was evaluated by subdividing the groups. The null form of the sixth hypothesis is as follows: the privacy policies of Safe Harbor companies and those of Fortune 500 self-regulating companies are equally likely to direct the visitor to an internal or external enforcement contact.

The comparison of the 40 Safe Harbor companies and the 40 Fortune 500 self-regulating companies resulted in a chi square of 10.912. This is significant at a probability level of 0.001 or less. The null hypothesis is rejected at the 0.001 level.

Hypothesis 7- Safe Harbor Companies and Self-Regulating INC 500 Companies

The null form of the seventh hypothesis is as follows: the privacy policies of Safe Harbor companies and those of INC 500 self-regulating companies are equally likely to direct the visitor to an internal or external enforcement contact.

To evaluate this hypothesis the 40 INC 500 self-regulating companies and the 40 Safe Harbor companies were compared. The analysis resulted in a chi square of 21.59. As this is significant at a probability level of 0.001 or less, the null hypothesis is rejected.

Hypothesis 8- Self-Regulating Fortune 500 Companies and Self-Regulating INC 500 Companies

The null form of the eighth hypothesis is as follows: the privacy policies of Fortune 500 self-regulating companies and those of INC 500 self-regulating companies are equally likely to direct the visitor to an internal or external enforcement contact.

The comparison of the 40 Fortune 500 self-regulating companies and the 40 INC 500 self-regulating companies resulted in a chi square of 4.21. This is significant at a probability level of 0.05 or less. The null hypothesis is rejected at this level.

The results of the evaluation of hypotheses 5 through 8 are summarized in Table 6. Again, larger chi squares indicate more significant differences. The strongest difference is, once again, between the Safe Harbor companies and the self-regulating companies (Hypothesis 5). In three cases the null hypotheses are rejected at the 0.001 level. In the remaining case, the null is rejected at the 0.05 level.

SEE TABLE 6

Summary of Survey Results

Table 7 summarizes the survey results across both the question of compliance with the FTC Fairness Principles and the question of direction to an enforcement mechanism. Based on

the samples analyzed there is less than one chance in a thousand that the privacy policies of Safe Harbor companies and those of self-regulating companies are equally likely either to comply with the FTC Fairness Principles or to provide direction to an enforcement mechanism. These results of the survey provide evidence that a regulatory approach is more effective than a self-regulating approach to the protection of personal data gathered on companies' websites.

SEE TABLE 7

In addition, the survey indicates that this is true whether the comparison is made between the privacy policies of Safe Harbor companies and the larger companies of the Fortune 500 or between the privacy policies of the Safe Harbor companies and those of the smaller companies of the INC 500.

Finally, although both the Fortune 500 companies and the INC 500 companies represent the self-regulating approach, there are significant differences between the privacy policies of the two groups. This is true both for compliance and for enforcement mechanisms.

CONCLUSION

The survey results seem to indicate that a regulatory system is of greater benefit to consumers than is a system of industry self-regulation. In analyzing online privacy policies, however, the survey analysis presented has the same challenges as those conducted by the FTC, primarily the difficulty in interpreting what often is confusing, and sometimes contradictory, language in the privacy policy itself.⁸⁹ In addition, the Safe Harbor companies are subject to a stronger enforcement requirement than the self-regulating companies. While there is debate about how strongly the DPD in general is enforced, there are at least theoretical legal consequences for noncompliance.⁹⁰

⁸⁹ See 2000 Report, *supra* note 48, at 24-26.

⁹⁰ See Soma, *supra* note 25, at 208-09 (questioning the efficacy of FTC enforcement of the Safe Harbor Agreement); David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First year*, 12 IND. INT'L. & COMP. L. REV. 265, 292 (2001) (questioning EU enforcement efforts).

TABLE 1			
Number of Companies in Compliance With All Four FTC Fairness Principles			
	Safe Harbor Companies	Self-Regulating Companies	Totals
Compliant	45	16	61
Non-compliant	35	64	99
Totals	80	80	160

TABLE 2		
Percentage of Companies in Compliance With All Four FTC Fairness Principles		
	Safe Harbor Companies	Self-Regulating Companies
Compliant	56.25%	20%
Non-compliant	43.75%	80%
Totals	100%	100%

Table 3				
Chi Square Evaluation of Compliance with FTC Fairness Principles				
	Groups compared	N	Chi square	Significant at
1	Safe Harbor versus All Self-regulating	160	22.28	0.001 or less
2	Safe Harbor versus Fortune 500 Self-regulating	80	4.178	0.05 or less
3	Safe Harbor versus INC 500 Self-regulating	80	16.81	0.001 or less
4	Fortune 500 Self-regulating versus INC 500 Self-regulating	80	5	0.05 or less

TABLE 4			
Number of Companies Directing to an Enforcement Mechanism			
	Safe Harbor Companies	Self-Regulating Companies	Totals
Direction	36	4	40
No Direction	44	76	120
Totals	80	80	160

TABLE 5		
Percentage of Companies Directing to an Enforcement Mechanism		
	Safe Harbor Companies	Self-Regulating Companies
Direction	45%	5%
No Direction	55%	95%
Totals	100%	100%

Table 6				
Chi Square Evaluation of Direction to Enforcement Mechanism				
	Groups compared	N	Chi square	Significant at
1	Safe Harbor versus All Self-regulating	160	34.13	0.001 or less
2	Safe Harbor versus Fortune 500 Self-regulating	80	10.912	0.001 or less
3	Safe Harbor versus INC 500 Self-regulating	80	21.59	0.001 or less
4	Fortune 500 Self-regulating versus INC 500 Self-regulating	80	4.21	0.05 or less

Table 7		
Summary of Results – Significance Levels at Which Null Hypotheses Were Rejected		
Groups compared	Compliance with Fairness Principles	Direction to an Enforcement Mechanism
Safe Harbor versus All Self-regulating	0.001 or less	0.001 or less
Safe Harbor versus Fortune 500 Self-regulating	0.05 or less	0.001 or less
Safe Harbor versus INC 500 Self-regulating	0.001 or less	0.001 or less
Fortune 500 Self-regulating versus INC 500 Self-regulating	0.05 or less	0.05 or less