You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission

Robert R. Schriver

Follow this and additional works at: https://ir.lawnet.fordham.edu/flr

Recommended Citation
Available at: https://ir.lawnet.fordham.edu/flr/vol70/iss6/29

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.
You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission

Cover Page Footnote
J.D. Candidate, 2003 Fordham University School of Law. I would like to thank Professor Joel R. Reidenberg for his guidance in selecting a proper Note topic, Professor Steve Thel for his input, and Professor Robert Clark of University College Dublin for introducing me to the topic during the summer of 2001.
YOU CHEATED, YOU LIED: THE SAFE HARBOR AGREEMENT AND ITS ENFORCEMENT BY THE FEDERAL TRADE COMMISSION

Robert R. Schriver*

INTRODUCTION

In May 1999, officials from the Spanish Data Protection Authority carried out an inspection of Microsoft's subsidiary in Spain. The Authority found that Microsoft possessed a database filled with the personal information of their Spanish consumers. In July 2000, the Authority charged Microsoft with improperly storing and handling personal data. Microsoft was convicted and assessed a fine of fifty million pesetas (approximately $250,000), which was later reduced to ten million pesetas ($57,000).

Microsoft was one of the first American businesses to feel the effects of new European Union laws concerning data protection. The European Union's Directive on Data Protection had gone into effect on October 25, 1998. Few outside of the European Union ("EU")

---

* J.D. Candidate, 2003 Fordham University School of Law. I would like to thank Professor Joel R. Reidenberg for his guidance in selecting a proper Note topic, Professor Steve Thel for his input, and Professor Robert Clark of University College Dublin for introducing me to the topic during the summer of 2001.

2. Id.
4. Kuner, supra note 1, at 84.
5. Id.
6. In the interests of clarity and consistency, this Note will use the term "European Union" throughout to refer to both the former European Economic Community and the European Union that came into existence after the Treaty on European Union, signed in Maastricht on February 7, 1992. The Member States of the European Union are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. See The Member States of the European Union, at http://europa.eu.int/abc/eu_members/index_en.htm (last visited Mar. 11, 2002).
took notice, and fewer still anticipated the consternation, argument, posturing, proselytizing, and theorizing it would cause. It soon became apparent that the Directive would change the face of privacy protection not only in Europe, but also in the United States and the rest of the world.

The Directive was passed in response to growing concerns about the improper use, collection, and dissemination of personal information. In Europe, privacy is “not a subject you can bargain about”8—it is considered a fundamental human right.9 The Directive was passed in order to harmonize the various privacy laws10 that had been enacted throughout the Member States of the European Union.11 The Directive has come to have particular importance in the area of e-commerce, as the Internet has allowed personal data to be easily—and secretly—collected and sold.12


10. See infra notes 48-62 and accompanying text.


12. See U.S.-EU “Safe Harbor” Data Privacy Arrangement, in Contemporary Practice of the United States Relating to International Law, 95 Am. J. Int'l L. 156, 156 (Sean D. Murphy ed., 2001) [hereinafter “Safe Harbor” Arrangement] (stating that the Directive was passed “in recognition of the ease with which personal data on Europeans can be transferred electronically”). The Safe Harbor agreement (an agreement reached between the United States and the EU after the Directive was passed) applies to online and offline collection and processing of personal data, as long as it has been “recorded in any form.” See U.S. Dep't of Commerce, Safe Harbor Principles, July 21, 2000 [hereinafter Safe Harbor Principals], at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm. The FTC, of course, can regulate both online and offline deceptive trade practices, but in recent years
It is perhaps no surprise that the United States views privacy rights quite differently than the European Union. Americans and Europeans think of privacy in "fundamentally different ways." For the United States to adopt the European regulatory approach would be a "jarring change" from the current privacy regime. Most American companies simply do not see privacy as a normal cost of doing business. They reject international privacy standards and have a basic "distaste for legislation." For its part, the U.S. Congress has passed no overarching privacy law; explanations for this have ranged from First Amendment concerns and the free flow of information to the promotion of commerce and wealth, to "a healthy distrust for governmental solutions." As one commentator pointedly put it: "Congress has granted drug abusers greater privacy protection than lawful users of the Internet." This distrust, however, does not seem to extend to the general, Internet-using public. In its 2000 report to Congress, the Federal Trade Commission ("FTC") found that ninety-two percent of respondents did not trust even privacy policies posted on companies' websites, and eighty-two percent recommended legislation to change the situation.

And the situation is changing. Piece by piece, American consumers (and Internet users in particular) have been gaining privacy protections. Additionally, the European Directive may prove impossible to ignore. The trade in personal information between the United States and the EU was valued at $120 billion in 2000. As this

have focused on deceptive practices in the online world, see infra notes 197-302, and it is in the online context that the Directive and the Safe Harbor agreement are usually discussed.

13. Fromholz, supra note 9, at 470. The terms used by Americans and Europeans "reflect[] this deep disparity: Americans tend to use the term 'privacy,' while Europeans discuss 'data protection.'" Id.

14. Id.


21. See infra notes 171-97 and accompanying text.

Note will demonstrate,²³ the Directive places virtually this entire trade at risk.²⁴ U.S. firms doing business in Europe could be just as constrained. U.S. companies have approximately nine million employees in the EU,²⁵ and in 1995, "U.S. affiliates in Europe produced $1.2 trillion of goods and services."²⁶ These affiliates also fall under the Directive’s purview, and few abide by European privacy standards.²⁷

The potential for trade disruption is grand. In 1997, for example, U.S. sales via direct marketing (which thrives on the unrestrained trade of personal data) were $1.2 trillion, while such sales were only $125 billion in the European Union, which has a larger population.²⁸ European privacy standards may have something to do with that. U.S. companies subject to the Directive, it has been said, risk “astronomical” losses if they simply ignore the regulations and have their data flows shut off by the EU.²⁹

The Clinton administration recognized the threat and began negotiating with the European Commission shortly after the Directive went into effect. The result was the Safe Harbor agreement, which was approved in July 2000.³⁰ Under the Safe Harbor agreement, U.S. firms agree to abide by basic privacy principles similar to those contained in the European Directive on Data Protection.³¹ Those that do so will be presumed to provide “adequate protection,” and the European data-protection authorities will allow their transatlantic data transfers to continue unchallenged.³² Europe fears the agreement might be too lenient, especially concerning enforcement.³³ U.S. companies fear the agreement might be too strict.³⁴

²³. See infra notes 77-83 and accompanying text.
²⁴. Kuner, supra note 1, at 82 (stating that almost “all types of data and processing are covered by EU data protection law”).
²⁶. Shaffer, supra note 8, at 39.
²⁸. Shaffer, supra note 8, at 18.
³². See Midge M. Hyman & Sandra N. S. Covington, European Privacy and the Safe Harbor, N.Y. L.J., Apr. 30, 2001, at 66 (“By voluntarily certifying adherence to the Safe Harbor principles... an organization is deemed compliant with EU privacy standards and may freely engage in the transfer of personal information from EU member states.”).
³³. See, e.g., Pearce & Platten, supra note 9, at 2048 (“From a European perspective, the key weakness of the U.S. model lies in its... still half-hearted
Accordingly, U.S. reaction to the Safe Harbor was tepid. But with lessons such as those learned by Microsoft, the Safe Harbor may yet become an important part of many corporations' business plans. In 2000, "lack of consumer trust cost e-businesses $16 billion in lost sales." Those are numbers e-commerce cannot afford to ignore. The added threat of data-flow shutoffs from Europe makes the Safe Harbor an increasingly attractive option.

But what if someone cheats? What if a company lies to the U.S. and EU authorities and says it is compliant when it is not? How will the agreement be enforced? Opinions about the validity—and necessity—of the Safe Harbor itself have varied widely. This Note will attempt to steer clear of tempestuous policy arguments, and focus instead on the enforcement of the Safe Harbor, in particular, on the role of the FTC, the agreement's principal governmental enforcement body. What would an enforcement action look like? Is the FTC up to the task? Does it even have the legal ability to bring an enforcement action on behalf of foreign consumers? Finally, are there ways of augmenting the FTC's enforcement powers to create more effective privacy protection?

This Note argues that the FTC is willing and able to enforce the Safe Harbor agreement through its power to prohibit deceptive trade practices under section 5 of the Federal Trade Commission Act ("FTCA"). Part I of this Note will give a brief history of the Safe Harbor agreement, beginning with the history of the enactment of the Directive by the European Union, and continuing with a description of the Safe Harbor negotiations and eventual agreement. This part will then examine existing privacy protections in the United States, beginning with an examination of federal legislation protecting privacy rights, and continuing with a review of the FTC's efforts in the past few years fighting for greater privacy protection for American consumers. Finally, this part will examine the legal actions the FTC
has taken pursuant to its section 5 powers to prohibit deceptive practices by online companies.\textsuperscript{43}

Part II of this Note will examine criticisms of the Safe Harbor agreement, in particular the recent challenges to the effectiveness and validity of FTC enforcement.\textsuperscript{44}

Part III of this Note will discuss what an FTC action undertaken to enforce the Safe Harbor would look like. It will argue that the FTC is well-suited to enforce the Safe Harbor, and that rulemaking under the FTCA is necessary to clarify the FTC's legal authority to enforce the Safe Harbor.\textsuperscript{45} This part will propose that the FTC enact a rule pursuant to its powers under section 18 of the FTCA to define as a deceptive trade practice an institution's failure to abide by its obligations under the Safe Harbor agreement.\textsuperscript{46} This part will conclude by arguing that federal legislation is the only way to ensure absolutely that the FTC will be able to prosecute the cheaters and liars mentioned in the title, who conceal their noncompliance with the Safe Harbor to gain an unfair economic advantage.\textsuperscript{47}

I. HISTORY OF THE SAFE HARBOR AGREEMENT

A. Privacy Legislation in Europe


Europe was the scene of the first data-protection statute, enacted by the German state of Hesse in 1970.\textsuperscript{48} Sweden enacted the first national privacy legislation in 1973.\textsuperscript{49} In 1978, France passed its charmingly named Law Concerning Data Processing, Files, and Liberty, which granted individuals some measure of privacy protection.\textsuperscript{50} These early privacy statutes were a response to a privacy movement in the United States during the 1960s and 1970s.\textsuperscript{51}

The first attempt to articulate a broad set of basic privacy principles was made by the Organisation for Economic Co-operation and

\textsuperscript{43} See infra notes 231-313 and accompanying text.
\textsuperscript{44} See infra notes 314-37 and accompanying text.
\textsuperscript{45} See infra notes 338-98 and accompanying text.
\textsuperscript{46} See infra notes 399-401 and accompanying text.
\textsuperscript{47} See infra notes 402-04 and accompanying text.
\textsuperscript{49} Assey & Eleftheriou, supra note 18, at 149; Cate, supra note 48, at 180.
\textsuperscript{50} Assey & Eleftheriou, supra note 18, at 149.
\textsuperscript{51} Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L.J. 771, 782 (1999); see also Safe Harbor Hearings, supra note 11, at 33 (testimony of Stefano Rodotà) ("Europe accepted the modern idea of privacy protection coming from the United States.").
Development ("OECD"). The OECD passed its non-binding Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. The OECD Guidelines were intended to be a model that various countries could use to enact legislation to facilitate the free flow of information between them without running afoul of each other's privacy regulations. They called for adherence to "eight basic principles that govern the handling of personal information." As such, it was an early, non-binding attempt at harmonization of European privacy legislation. The United States endorsed the Guidelines, but did not pass any legislation implementing them.

The European Union officially got into the act in 1981, when the Council of Europe promulgated a Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Its provisions were similar to the OECD Guidelines. The European Union continued to work on a Union-wide Directive to harmonize the various privacy laws of its Member States and to further the aims of the Common Market. It was negotiated "within the context of the threat of data transfer bans from certain EU Member States with protective data privacy laws (such as France and Germany) to other EU Member States with less stringent laws (such as Italy)." The European Commission produced the first draft of the Directive in July


54. Cate, supra note 48, at 180.


56. Anna Shimanek, Note, Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles, 26 Iowa J. Corp. L. 455, 463 (2001); Reidenberg, supra note 51, at 773 (noting that the United States endorsed the OECD Guidelines).


58. Cate, supra note 48, at 180-81; Fromholz, supra note 9, at 467.

59. Cate, supra note 48, at 181. "By requiring similar data privacy protection throughout the European Union, the EU Directive concurrently removed the threat to unhindered data flows between Member States." Shaffer, supra note 8, at 10.

60. Shaffer, supra note 8, at 10.
1990.61 The European Parliament eliminated the draft's distinction between the public sector and the private sector and then "overwhelmingly approved the draft directive" on March 11, 1992.62

2. Passage of the Directive

The European Union adopted the Data Privacy Directive on October 24, 1995, and it went into effect on October 25, 1998.63 At the time of its adoption, six Member States had drafted or already passed data-protection laws.64 The Directive, like the OECD Guidelines before it, aimed to allow the "free flow of personal data among" Member States and to provide a "firewall" against third countries "who fail to provide adequate protection of privacy rights."65

The Directive instructs all Member States to enact laws that "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."66 The core of the Directive is Article 6, which sets forth the following principles:

A. Personal data shall be "processed fairly and lawfully."67

B. Personal data shall only be "collected for specified, explicit and legitimate purposes."68

C. The data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."69

D. The data must be accurate and up to date. Data that are inaccurate or no longer current are to be "erased or rectified."70

E. Data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."71

61. See Cate, supra note 48, at 181.
62. Id.
64. Id.
65. Raysman & Brown, supra note 22, at 3; see also Data Privacy Directive, supra note 7, pmbl. at (20) ("[T]he fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive ... and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected ... ").
67. Id. art. 6.
68. Id.
69. Id.
70. Id.
71. Id.
Article 7 lists the circumstances under which personal data may be processed, and Article 8 prohibits the processing of "special categories of data," such as race, ethnicity, political affiliation, union membership, religious beliefs, sexual orientation, or medical data, without "explicit consent."

Implementing the provisions of the Directive can have dramatic effects in a Member State. Italy, for example, had no data-protection law before the Directive was passed. In the four years since Italy passed its law to comply with the Directive, the new Italian Data Protection Commission has received almost 100,000 consumer reports. Consumers complained about breaches directly to private companies as well.

Potentially the most important—and certainly the most controversial—feature of the Directive is Article 25. The European Union recognized that the easiest way for Member States to avoid the strictures of the Directive was to simply send their data to a third country to be processed. It was, in fact, a "common practice" for Member States to send data to countries with little or no data-protection law to be processed to avoid the rigors of European privacy laws. Article 25 therefore prohibits transfer of personal data to a third country for processing purposes unless that country has been found to provide an "adequate level" of privacy protection. The immediate questions, therefore, were what constituted adequate protection, and which countries met that standard. The Directive does not define the term "adequate," but rather establishes a Working Party of the European Parliament to investigate the privacy laws of other countries, and to certify them as adequate if found to properly comply with the Directive. At the time the Directive went into

72. Id. art. 7.
73. Id. art. 8.
74. See Safe Harbor Hearings, supra note 11, at 9 (testimony of Stefano Rodotà).
75. See id.
76. See id. ("4 million customers asked banks not to send them commercial advertising.").
77. See George et al., supra note 25, at 759.
78. See Data Privacy Directive, supra note 7, pmbl. at (6) ("The increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks... necessitate and facilitate cross-border flows of personal data.").
79. Pearce & Platten, supra note 9, at 2027; see also Data Privacy Directive, supra note 7, pmbl. at (4) ("Frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity... information technology is making the processing and exchange of such data considerably easier.").
80. Data Privacy Directive, supra note 7, art. 25(1). Article 25 was quickly dubbed "the Great Wall of Europe." Safe Harbor Hearings, supra note 11, at 13 (statement of Stefano Rodotà).
81. Shaffer, supra note 8, at 21; see also Data Privacy Directive, supra note 7, arts. 29-30.
effect, "the whole world" was considered to be noncompliant.\textsuperscript{82} Even within the European Union, only five Member States had "adequate" legislation in place.\textsuperscript{83}

3. Reaction to the Directive

The Directive binds all Member States of the European Union to pass legislation complying with its provisions.\textsuperscript{84} On January 11, 2000, however, the European Commission began enforcement proceedings against Ireland, Germany, France, Luxembourg, and the Netherlands for failing to comply with the Directive.\textsuperscript{85} Over a year later, enforcement proceedings were still pending against all except the Netherlands,\textsuperscript{86} and even as late as November 2001, the Commission found France, Germany, and Luxembourg to be noncompliant.\textsuperscript{87}

Shortly after the passage of the Directive, the European Union began discussions with other countries on the adequacy of their data protection. By April 1999, the EU was negotiating with the United States, Japan, Australia, and New Zealand.\textsuperscript{88} One year later, Canada, Australia, Taiwan, Norway, Iceland, Hong Kong, Poland, Hungary, and Switzerland all had either implemented privacy legislation or were in the process of doing so.\textsuperscript{89} On July 26, 2000, the EU approved the privacy laws of Switzerland and Hungary, along with the Safe Harbor agreement, as providing adequate protection.\textsuperscript{90} Argentina

\textsuperscript{82} See Susan Binns, Technical Briefing for Journalists on Data Protection— the EU/U.S. Dialogue (Dec. 10, 1998), http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/euus.htm. Ms. Binns noted that Switzerland already had a "perfectly good data protection law which looks pretty much like" the EU model, but because there had not been time to make a formal finding of adequacy, Switzerland at that point was presumed to be noncompliant. \textit{Id.}

\textsuperscript{83} Fromholz, supra note 9, at 467-68.

\textsuperscript{84} Data Privacy Directive, \textit{supra} note 7, art. 32. For an example of Member State Data Protection Act, see Safe Harbor Hearings, \textit{supra} note 11, at 18-23 (statement of David Smith) (describing the provisions of the UK Data Protection Act 1998).


\textsuperscript{87} See Reidenberg, \textit{supra} note 19, at 733. \textit{But see} Safe Harbor Hearings, \textit{supra} note 11, at 32 (testimony of Stefano Rodotà) ("The fact that they have not implemented the directive does not mean that they have no data protection. They have data protection. France and Germany have very well-established... data protection laws.").


\textsuperscript{89} Pearce & Platten, \textit{supra} note 9, at 2050-51.

enacted its privacy law in late 2000, and Canada’s law went into effect on January 1, 2001. Discussions with Japan and Australia continued through October 2000, and were ongoing as of November 2001.

Reaction in the United States was somewhat muted. American officials, it was said, agreed in principle about the right to privacy, but disagreed as to how it should be implemented. Europeans generally thought of U.S. privacy protection as being “over reliant on voluntary self-regulation,” while U.S. businesses thought the European regime was “unduly heavy handed and bureaucratic.” The method adopted by the Directive—a “top-down approach”—has not been well-received in the United States, which has “an entire industry” set up around the accumulation, collection, and analysis of personal data. This industry would be threatened by strict privacy rules, and American companies fear that American consumers would use privacy legislation as “a weapon of nuisance making” that would create enormous costs. The Directive, however, did not pass by (announcing that the Swiss law provides adequate protection); Commission Decision 2000/519/EC of July 26, 2000, 2000 O.J. (L 215) 4. http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm (announcing that the Hungarian law provides adequate protection); Christopher Paul Boam, The Internet, Information and the Culture of Regulatory Change: A Modern Renaissance, 9 CommLaw Consp ectus: J. Comm. L. & Pol’y 175, 185 (2001).

91. See Tamara Loomis, European Union Safeguards Get Scant Response Here, N.Y. L.J., Nov. 30, 2000, at 5 [hereinafter Loomis, Safeguards]. Argentina’s law is described as superior to privacy protection in the United States. See id.


93. Raysman & Brown, supra note 22, at 3.


95. See Andrews, supra note 63.

96. Pearce & Platten, supra note 9, at 2025.

97. See Andrews, supra note 63 (internal quotation marks omitted).

98. Binns, supra note 82; see also Safe Harbor Hearings, supra note 11, at 6 (statement of the Hon. W. J. “Billy” Tauzin) (noting potential litigation concerns: “Europeans do not view lawsuits as an answer to problems. In the U.S., lawsuits are filed at the drop of a hat.”); Blanke, supra note 53, at 85 (“There was much concern from industry about repetitious or vexatious requests for access.”). Complaining about increased costs, of course, is nothing new, and one commentator has argued that industry estimates of the costs of privacy legislation are “staggeringly specious.” Reidenberg, supra note 19, at 724. Nor is the complaint unique to the United States: the British Banking Association claimed that it would cost each major bank more than £150 per customer to comply with the terms of the Directive. Shaffer, supra note 8, at 17. The European Commission (of course) performed its own study and “concluded that the financial impact would be minimal.” Id. In Italy, “the private
unnoticed. The possibility that a country would cut off a transatlantic data transfer had existed in the past under the privacy laws of various Member States, but it was the passage of the Directive that got the attention of U.S. authorities. The Clinton administration wanted to create a "safe harbor" agreement that would satisfy European concerns about data protection and concerns voiced by American business about intrusive bureaucracy and increased costs. However, there was no rush to do so—as a contemporary New York Times article put it, "[i]n the short term, government and industry officials predict that nothing much will happen." They were right.

B. The Safe Harbor Agreement

1. Negotiations

In an April 1998 address to U.S. business leaders, John Mogg, Director General of the European Commission, said of existing American privacy law: "[M]ost of what we see is not meaningful... the industry codes we have seen have no teeth." Something else was needed, and negotiations were soon underway between Mogg and David Aaron, U.S. Undersecretary for Commerce, for a bilateral agreement. Mogg and Aaron originally planned to finish negotiations by December 1998, and in fact, the "basic form" of the agreement "evolved quickly." As of April 1999, the two sides were "edging toward" an agreement, and were said to be "quite close" to reaching a satisfactory solution. Negotiations then broke down over the issues of enforcement and remedy.

The fact that only seven out of fifteen Member States had implemented the Directive reduced the pressure on the two parties. One month later, however, the negotiations were in trouble, with Aaron implying that the EU would not yield on the issue of sector... [did] not at all suffer[ ] the dramatic consequences foreseen by some interested [parties]" after the national privacy law enforcing the Directive went into effect. Safe Harbor Hearings, supra note 11, at 9 (testimony of Stefano Rodotà).
Mogg, however, insisted that "the gap is consistently narrowing." Before the new millennium arrived, the United States had submitted six Safe Harbor drafts to the European Union, which rejected them all.

A preliminary proposal was finally completed on March 14, 2000, nearly a year and a half after the Directive went into effect. The EU, through Mogg, declared that the preliminary Safe Harbor proposal did indeed constitute "adequate protection." American privacy advocates, for their part, were already calling it "largely meaningless," and some Member States had reservations as well. Although the European Parliament gave the draft proposal a thumbs down, its rejection was not legally binding, and the Member States approved the agreement on June 1, 2000. The European Commission formally certified the Safe Harbor agreement as providing adequate protection on July 26, 2000.


a. Benefits

The Safe Harbor "provide[s] a streamlined means for U.S. organizations to comply with the Directive." By signing on to the agreement, a company certifies to EU customers and organizations that it provides adequate privacy protection for personal data

110. Edmund L. Andrews, U.S.-European Union Talks on Privacy Are Sputtering, N.Y. Times, May 27, 1999, at C6. Aaron said that the EU was insisting that the U.S. "invent a regime that looks like theirs .... Well, we aren't going to do that." Id. (internal quotations omitted).
111. Id. (internal quotations omitted).
112. See Shimanek, supra note 56, at 472.
115. Id.
116. Margret Johnston, EU Vote on Privacy Agreement Due This Week, IDG.net, Mar. 27, 2000, at www.idg.net/crd_idgsearch_156896.html.
117. Shimanek, supra note 56, at 458.
118. U.S. and Europe Agree on Privacy, N.Y. Times, June 2, 2000, at C4. Aaron later said that the Commission's decision was passed over "the outright opposition of the European Parliament." Safe Harbor Hearings, supra note 11, at 43 (testimony of David Aaron).
according to the terms of the Directive.121 Such a company's protections will be "deemed adequate" simply by signing on, and data transfers to the company will continue uninterrupted.122 If a Member State requires prior approval of data transfers, the requirement "either will be waived or approval will be automatically granted" for a U.S. company in the Safe Harbor.123 Joining the Safe Harbor also allows an American company to avoid negotiations with the data-protection authorities of each Member State in which it does business.124 Signing on is easy, and can be done via the Commerce Department's website.125

b. Requirements

So much for the benefits. What are the requirements? Membership, it bears stating, is voluntary.126 Companies that agree to the Safe Harbor must comply with its requirements, and annually certify with the Commerce Department that they are in compliance.127 The company must also indicate in its published privacy policy that it adheres to the Safe Harbor principles.128 The principles are as follows:

Notice—participants must tell individuals why information about them is being collected and what it is being used for. Participants must also reveal their contact information, the types of third parties to which they disclose personal information, and any means by which the individual can choose to limit the use and disclosure of his information.129

121. Id.
122. Id.
123. Id.
124. See id.
126. See Safe Harbor Overview, supra note 120. A company can "join a self-regulatory privacy program," such as TRUSTe or BBBonline. Id.; U.S. Dep't of Commerce, Safe Harbor FAQs, FAQ No. 11: Dispute Resolution and Enforcement, [hereinafter FAQ No. 11], at http://www.export.gov/safeharbor/FAQ11FINAL.htm (last visited Nov. 2, 2001). Alternatively, a company can create its own privacy policy in accordance with the Safe Harbor principles. See Safe Harbor Overview, supra note 120. This Note focuses on the consequences of a company joining the Safe Harbor and enjoying its benefits (all the while certifying to the Commerce Department and the European Union that they follow the principles) without in reality providing the necessary privacy protection. For the purposes of this Note, the way in which a company chooses to join is irrelevant.
127. See Safe Harbor Overview, supra note 120.
129. See id.
Choice—participants must allow individuals to choose whether their personal information will be disclosed to a third party or used for a purpose other than that for which it was collected.130

Onward Transfer/Transfer to Third Parties—participants must abide by the notice and choice principles before disclosing personal information to a third party.131

Access—individuals must be given access to their personal information and the ability to correct or delete inaccurate information.132

Security—participants must take “reasonable precautions” to ensure the security of any personal information collected.133

Data Integrity—personal data “must be relevant for the purposes for which it is to be used,” and it must be “accurate, complete, and current.”134

Enforcement—participants must make dispute-resolution procedures available to individuals, with verification procedures and remedies that are “sufficiently rigorous to ensure compliance.”135

Thus, the Safe Harbor requirements are similar to, but less onerous than, those imposed by the Directive.136 These principles also need only be observed in business dealings with the EU137—not in dealings with U.S. customers. But it should also be remembered that signing up for the Safe Harbor is equivalent to a promise—to the Commerce Department, the European Union, and European consumers—that a company will abide by the Safe Harbor’s terms. This promise carries great weight when it comes to enforcement.138

c. Enforcement

What happens if a company cheats? Enforcement will first be “carried out primarily by the private sector,” which will be “backed up as needed by government enforcement of . . . unfair and deceptive statutes.”139 The “private sector enforcement” will be according to

130. Id.
131. See id.
132. Id.
133. Id.
134. Id.
135. Id.
136. See Sykes & de Bony, supra note 114 ("Those [European] laws are much stricter than the safe harbor principles . . . .").
137. See id.
138. See U.S. Dep't of Commerce, Safe Harbor Enforcement Overview: Federal and State "Unfair and Deceptive Practices" Authority and Privacy, July 14, 2000, at http://www.export.gov/safeharbor/ENFORCEMENTOVERVIEWFINAL.htm [hereinafter Safe Harbor Enforcement Overview] ("[W]here a company certifies that it will safeguard the privacy of information and then fails to do so, such action would be a misrepresentation and a 'deceptive practice' within the meaning of Section 5.").
139. Safe Harbor Overview, supra note 120.
whatever dispute-resolution process the participant has put in place in accordance with the Enforcement Principle. Assuming these measures fail, enforcement then lies with the FTC, the Federal Communications Commission ("FCC"), or the Department of Transportation ("DOT"), "[d]epending on the industry sector."[144]

Under the Federal Trade Commission Act, "a company's failure [to comply with the Safe Harbor] might be considered deceptive and actionable by the Federal Trade Commission."[142] The FTC may move to enforce the agreement "even where an organization adhering to the safe harbor principles relies entirely on self-regulation to provide . . . enforcement."[143] Penalties that may be applied pursuant to the FTCA are administrative cease-and-desist orders, injunctions and restraining orders, and fines of up to $12,000 per day.[144] Participants who continuously violate the terms of the agreement will be dropped.[145]

3. The Response to the Safe Harbor

After the Safe Harbor was approved by U.S. and European authorities, a so-called "standstill agreement" went into effect, under which no enforcement action would be taken by the EU while U.S. companies registered for and began to comply with the terms of the Safe Harbor agreement.[146] This agreement was set to expire on July 1, 2001,[147] but an "informal grace period" continued through November 2001.[148] To date, Member States have blocked only a few data transfers,[149] and the overall European reaction to the Safe Harbor seems to be muted.[150]

The American reception was not clamorous, either. Few companies were interested in the program, and fewer still signed up. By January 2001, six months after the program went into effect, only twelve

---

140. The enforcement principle establishes only the somewhat nebulous requirement that participants create a dispute resolution process that is "sufficiently rigorous to ensure compliance." Safe Harbor Principles, supra note 12.
141. See Safe Harbor Overview, supra note 120. The DOT has jurisdiction over transportation companies. See id. The FCC has jurisdiction over telecommunications. See Safe Harbor Enforcement Overview, supra note 138. For brevity's sake, this Note will only address enforcement by federal authorities, not private dispute resolution, and only with those companies that fall under the jurisdiction of the FTC.
142. Safe Harbor Overview, supra note 120 (emphasis added).
143. Id.
144. See id.; see also Safe Harbor Enforcement Overview, supra note 138.
145. See Safe Harbor Overview, supra note 120.
146. See Dennis Kelly, U.S. Financial Services to Meet With European Union Over Privacy, BestWire, May 9, 2001.
147. Id.
148. Brunts, supra note 27.
149. See Loomis, Safeguards, supra note 91. As of November 2000, France and Sweden, which have some of the stricter data-protection laws, had blocked transfers to the United States. Id.
150. See Safe Harbor Hearings, supra note 11, at 50 (statement of Jonathan Winer) ("Neither the U.S. nor the EU sought a trade war over privacy.").
companies had entered the Safe Harbor. A few months later, thirty firms were on the list. By August 2001, industry bellwethers Procter & Gamble, Microsoft, and Intel had all joined, bringing the total to somewhat less than 100 companies. More companies glided into the harbor over the ensuing months, but as of March 2002, only 168 firms had registered.

Why have so many companies stayed away? Explanations abound. Commentators have suggested that American businesses first wanted to see the consequences of not signing up, particularly as to liability. Other theories included the sheer novelty of the deal, the "logistical challenge of getting up-to-speed," bureaucratic delays, and a "reluctance to step into the spotlight." Some companies simply consider the rules "costly, unworkable and unfair given the failure of [the European Union] to aggressively enforce data privacy violations by European organizations." And, as always, companies want to be sure that the benefits of Safe Harbor outweigh the costs.


152. Hyman & Covington, supra note 32.
153. See Loomis, supra note 15.
155. See Johnston, supra note 151.
156. Hyman & Covington, supra note 32.
159. Loomis, Safeguards, supra note 91.
160. Assey & Eleftheriou, supra note 18, at 158. Additionally, U.S. companies may not believe European authorities will even have the necessary resources to enforce the laws, Kuner, supra note 1, at 88.
161. Loomis, Safeguards, supra note 91. Companies also may be concerned that the Safe Harbor website itself is not secure: In July 2001 the website accidentally posted privileged information about some of the companies on the Safe Harbor list, including confidential information such as revenue and employee data. See Patrick Thibodeau, Safe Harbor Data Security Eyed after Web Site Glitch, ComputerWorld, July 9, 2001, at http://www.computerworld.com/storyba/0,4125,NAV47_STO62076,00.html.
162. See generally Safe Harbor Hearings, supra note 11. From Europe, Professor Stefano Rodotà, Chairman of the EU Data Protection Working Party, and Mr. David Smith, Assistant UK Information Commissioner, appeared to explain and defend the Directive. From Canada, Denis E. Henry, Vice President of Regulatory Law, Bell Canada, testified about Canada's new privacy law. David L. Aaron, U.S. negotiator of the Safe Harbor agreement, now with Dorsey & Whitney LLP; Jonathan M. Winer,
Opinions of the Safe Harbor program were sharply divided among both the witnesses and committee members. Shortly after the hearings, a member of the U.S. Chamber of Commerce went so far as to say that the Commerce Department never had the authority to negotiate the deal in the first place. Rep. Cliff Stearns (R-Fl.) mentioned the possibility of a full-blown trade war between the United States and the EU as a result of disagreements over the Safe Harbor. Nevertheless, the Safe Harbor is still with us, despite the changeover in administrations in January 2001, and observers predict that it "will eventually catch on," especially when (or if) the European Union begins to enforce the Directive.

The agreement gained some momentum (and notoriety) in June 2001, as Microsoft entered the Safe Harbor following its conviction and fine in Spain. Dun & Bradstreet joined the Safe Harbor agreement partly because Sweden had cut off a transatlantic data transfer. Given the history of these sporadic enforcement actions, many companies may be tempted to ignore the Directive, hoping that enforcement will be directed only at "egregious cases" and large companies. On the other hand, smaller companies may be "eager" to join the Safe Harbor for precisely that reason: They gain its benefits, but the enforcement authorities will not focus on them. Indeed, the history of privacy protection in the United States is spotty at best.

Counsel of Alston and Byrd LLP; Barbara Lawler, Customer Privacy Manager for Hewlett Packard, Inc.; and Professor Joel R. Reidenberg of Fordham University School of Law appeared on behalf of the United States. Id. at 3. The hearings provide an excellent introduction to the Directive and the Safe Harbor, and make for not only informative but also rather entertaining reading.

163. See id.
165. Peronet Despeignes & Deborah Hargreaves, EU-U.S. Clash over Personal Data: Private Right or Commercial Opportunity?, Financial Times, Mar. 29, 2001, at 14; see also Safe Harbor Hearings, supra note 11, at 5-6 (statement of the Hon. W. J. "Billy" Tauzin, Chairman, Committee on Energy and Commerce) ("[T]he EU Privacy Directive could be the imposition of the [sic] one of the largest free trade barriers ever seen.").
166. Loomis, Safeguards, supra note 91.
167. See supra notes 1-5 and accompanying text.
168. Loomis, Safeguards, supra note 91.
169. Despeignes & Hargreaves, supra note 165.
170. HRIS Data Protection, supra note 3, at 3.
C. Privacy Enforcement in the United States Today

1. Current Federal Privacy Statutes

The United States does not have a unified, "overarching" regime of privacy protection, but rather a "patchwork" of privacy legislation. There are many patches in this privacy quilt. The following statutes regulate the collection, use, and dissemination of personal information.

Statutes that apply to the federal government include the Federal Privacy Act ("FPA"), which limits the ways the federal government can collect and store the personal information of federal employees. Additionally, the Internal Revenue Service may not disclose information on income tax returns, and the Census Bureau cannot disclose certain census data. The first computer privacy policy was promulgated by the U.S. Department of Health and Education in 1973.

There are also numerous privacy statutes that apply to the private sector. The Fair Credit Reporting Act of 1970 extensively regulates the collection and dissemination of personal data by credit agencies. The Fair Credit Billing Act of 1974 provides further protection to consumers, and the Fair Debt Collection Practices Act of 1977 restricts the disclosure of sensitive personal data to certain third parties.

The "broadest set of privacy rights in any federal statute" appeared with the Cable Communications Policy Act of 1984. The Act gave sweeping privacy rights to cable subscribers regarding the...
collection, storage, and disclosure of personal data. Other legislation includes the Electronic Communications Privacy Act of 1986, which provides certain privacy rights to those engaged in electronic communication (such as by telephone, fax, or e-mail), and the Video Piracy Act of 1988, which grants consumers privacy rights in the area of videotape rentals. In the 1990s, the Telephone Consumer Protection Act of 1991 “allow[ed] consumers to opt out of unsolicited marketing calls” on a case-by-case basis; the Driver’s Privacy Protection Act of 1994 regulated state Departments of Motor Vehicles in disseminating personal information; and the Telecommunications Act of 1996 contained a few provisions protecting consumer privacy.

Two of the most important laws were passed in the late 1990s in response to concerns about consumer privacy protection. The Children’s Online Privacy Protection Act ("COPPA") restricts the online collection of information about children under 13. The FTC later passed a rule, as we shall see, enabling it to enforce COPPA. The Financial Services Modernization Act (commonly known as Gramm-Leach-Bliley) was passed on November 12, 1999, and requires financial service companies to create, post, and enforce a

182. The Act allows the consumer access to his data, and requires the cable provider to inform the consumer at least once a year of the data it is collecting, with whom it might be sharing the data, and how long it is being stored. 47 U.S.C. § 551(a)(1) (A)-(E). Additionally, the consumer may win damages for violations. Id. § 551(f); see Cate, supra note 48, at 214.


184. Cate, supra note 48, at 214.

185. 18 U.S.C. § 2710 (2000). This statute is commonly known as the “Bork Bill.” after Judge Robert Bork’s video rental record was introduced in his contentious Supreme Court nomination hearings. As a result of the Act, “video rentals are afforded more federal protection than are medical records.” Shaffer, supra note 8, at 25 (quoting Sheri Albert, Smart Cards, Smarter Policy: Medical Records, Privacy and Health Care Reform 13 (1993)).


189. Shaffer, supra note 8, at 24-25, 25 n.90. The Act was inspired by the stalking and murder of an actress. See id. at 25. Indeed, most U.S. privacy laws are enacted in reaction to public scandals, which partially explains their patchwork quality. See id.; Reidenberg, supra note 51, at 774.


191. Cate, supra note 48, at 214.


193. Cate, supra note 48, at 216.

194. 16 C.F.R. § 312 (2001); see infra notes 264-68 and accompanying text.

privacy policy. The FTC later issued a rule interpreting Gramm-Leach-Bliley "broadly" by extending its coverage "to include any personal information gathered by a financial institution" and again enabling the agency to use its power to enforce the Act.

Congress, therefore, has passed legislation giving Americans privacy protections, but only in certain contexts. In recent years, however, the push for greater privacy protections has come not from Congress, but from the FTC.

2. The FTC and Privacy

The FTC has "taken the lead among federal agencies in advocating greater data privacy protection in the United States." The FTC has sought greater consumer privacy protection in both words and deeds.

a. Words

In recent years, the FTC has given privacy reports to Congress. In 1998, the FTC delivered a report on online privacy. The report identified "five core principles of privacy protection" and "fair information practices." It also contained the results of a survey by the FTC on Internet privacy, and concluded that industry self-regulation was not yet effective. The FTC recommended the passage of legislation to protect the privacy of children.

The FTC delivered another report to Congress in the summer of 1999. In this report, the FTC noted that e-commerce was "booming" and that the Internet was a "rich source of information about online customers" as well as for online customers. The report found that online customers were concerned about threats to their privacy online, and about having their personal data sold to third

---

196. Boam, supra note 90, at 182.
197. Id.; 16 C.F.R. § 313.
198. Shaffer, supra note 8, at 56.
201. See 1998 FTC Privacy Report, supra note 199, at 19-38 (examining the online practices of personal information collection, the frequency of disclosure of such collection, and the nature of disclosure).
202. See id. at 41 ("To date, however, the Commission has not seen an effective self-regulatory system emerge.").
203. See id. at 42-43.
205. Id. at 1-2.
It did recognize the existence of industry self-regulation via "seal programs," but noted that "[o]nly a small minority of commercial Web sites" had joined them. The FTC concluded, however, that legislation mandating greater privacy protection was "not appropriate at this time."

The FTC changed that position in its 2000 report to Congress. The 2000 report contained the FTC's most far-reaching proposals to date. It began by noting the continuing "exponential" expansion of "the online consumer marketplace." The report delivered the results of a new online survey, which concluded that "industry efforts alone have not been sufficient." The FTC instead recommended federal legislation to "ensure adequate protection of consumer privacy online," and to implement four "widely-accepted fair information practices": notice, choice, access, and security. The report repeated widespread consumer privacy concerns. Ninety-two percent of online consumers, according to the FTC's survey, were concerned "about the misuse of their personal information online." In 1999, $2.8 billion in potential online sales were lost due to this lack of trust. And eighty-two percent of online shoppers "agreed that government should regulate how online companies use personal information." The report examined the collection of personal information: ninety-seven percent of websites collected at least "an email address or some other type of personal identifying information." Of the four recommended privacy principles, the FTC found that only twenty percent of commercial websites followed even one of them. The FTC reiterated its power under section 5 of the FTCA to combat deceptive practices, such as failing to abide by a stated privacy policy, but conceded that it could not require companies to adopt privacy policies in the first place. Accordingly, the FTC proposed federal legislation that "would set forth a basic level of privacy protection for all visitors" and would provide the FTC with authority to issue privacy regulations.

206. See id. at 2.
207. Id. at 9-12.
208. Id. at 12.
209. Id.
211. Id. at i.
212. Id. at ii.
213. Id. at iii.
214. Id. By now these "fair information practices" are familiar to us.
215. Id. at 2.
216. See id.
217. Id.
218. Id. at 9.
219. Id. at 12.
220. Id. at 33-34.
221. Id. at 36.
With a new administration, however, came a new agenda. In a “marked departure from the policy of his predecessor,” the new FTC Chairman, Timothy Muris, announced that the agency would seek to expand enforcement of *existing* laws rather than call for new legislation.\(^{222}\) Muris announced what he called “an ambitious, positive, pro-privacy agenda” that included increasing “resources devoted to privacy protection by 50 percent.”\(^{223}\) “[I]t is too soon to conclude that we can fashion workable legislation,” Muris said. “[W]e need more law enforcement, not more laws.”\(^{224}\) At an address to Congress the next month, Muris repeated these announcements to the House Subcommittee on Commerce, Trade, and Consumer Protection.\(^{225}\) Muris stated that the FTC was “primarily a law enforcement agency” which “best carries out its consumer protection mission” through “aggressive enforcement of the basic laws of consumer protection.”\(^{226}\) The FTC staff will conduct “Surf Days,” in which they search the Internet for websites with deceptive practices.\(^{227}\) In addition, the Commission created a new toll-free hotline for consumer complaints.\(^{228}\) Finally, Muris told the Subcommittee that “[a] majority of the Commission does not support online privacy legislation.”\(^{229}\) The Commission did, however, “intend[] to increase substantially the resources dedicated to privacy protection,” paying particular attention to deceptive trade practices, the Safe Harbor, and COPPA.\(^{230}\)

The FTC, therefore, continues to focus on consumer privacy, but it is not likely to call again for privacy legislation in the near future, whether applicable to all web users or Europeans alone.

---

224. *Id.* Despite the success of COPPA, Muris gave four reasons why legislation would not be “workable”: 1) it is too “difficult” to draft useful legislation; 2) commercial online expansion had slowed recently; 3) the costs of such legislation are not fully understood; and 4) the existing laws are adequate. See *id*.
226. *Id.* Which “basic laws” he meant, Muris did not say.
227. See *id.*; see also infra notes 272-89 and accompanying text (giving examples of COPPA enforcement actions).
229. *Id*.
230. *Id.*
b. Deeds

The FTC has pursued a number of enforcement actions in recent years in the area of online privacy. Although none of the cases progressed very far before a settlement was reached, they were all brought under the theory of deceptive trade practices, in violation of section 5 of the FTC Act. They therefore give us an idea of what an enforcement action under the Safe Harbor would look like.

"[T]he first FTC case involving [I]nternet privacy" was In re GeoCities. The FTC filed a complaint in 1998 alleging that GeoCities had engaged in two counts of deceptive practices in violation of the FTC Act. It charged GeoCities with misrepresenting "the uses and privacy of the information it collect[ed]" from consumers—specifically that the website had "sold, rented or otherwise marketed and disclosed" personal data "to third parties who have used this information for purposes other than those for which members have given permission," contrary to an express promise made (via a stated privacy policy) to consumers. The FTC also charged that GeoCities had made "misrepresentations involving sponsorship" when it stated that it maintained and collected children's personal information for an online club, when in fact third parties were collecting and maintaining the personal data. In both counts, the FTC alleged that GeoCities was engaging in "unfair or deceptive acts or practices" in violation of section 5 of the FTC Act.

The matter was quickly settled. The consent order required GeoCities to clearly post a privacy notice "telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information." Children's personal data, moreover, must be collected only with prior parental consent.

In another case involving the collection of personal data from children, the FTC filed a complaint in 1999 against Liberty Financial...
Companies, Inc., alleging that its Young Investor website "falsely represented that personal information collected from children in a survey would be maintained anonymously," when "[i]n fact, the personal information ... was maintained in an identifiable manner."239 This failure to abide by the stated terms of a privacy policy, the FTC alleged, violated section 5 of the FTCA.240 As in GeoCities, the defendant quickly settled. The settlement and consent order "prohibit[ed] Liberty Financial from making any false statements about the collection or use of personal information from children."241 For children under thirteen, parental consent would be required before any information at all was collected.242

In late 1999, DoubleClick attempted to merge its database of personal data with Abacus, sparking consumer outrage.243 DoubleClick, as of September 2001, had "amassed 100 terabytes of information and about 100 million consumer profiles,"244 and the combination with Abacus would have "create[d] a super-database capable of matching users’ online activities with their names and addresses."245 Prompted by several consumer complaints,246 the FTC opened an investigation into the matter, causing DoubleClick to abandon the plan in March 2000.247

The FTC next filed suit against ReverseAuction.com, an auction site that had registered with eBay, promised that it would not use any personal information of eBay users to send "spam",248 and then did precisely that.249 This, according to the FTC, was a deceptive trade practice.250 ReverseAuction.com also settled and agreed to a consent

242. Id.
246. See Boam, supra note 90, at 180.
247. See DoubleClick, 154 F. Supp. 2d at 505; Roiter, supra note 243. The FTC ultimately ended its investigation on January 22, 2001, concluding that DoubleClick had not merged the two databases and therefore had not engaged in any unfair or deceptive trade practices. DoubleClick, 154 F. Supp. 2d at 505. A federal class-action lawsuit against DoubleClick was also dismissed with prejudice on March 29, 2001. DoubleClick, 154 F. Supp. 2d at 526-27.
249. Id. ¶ 16.
250. Id. The FTC also for the first time alleged that the misrepresentation was an unfair trade practice. See id. ¶ 17. In a concurring and dissenting statement to the
order in January 2000. The settlement barred it from engaging in such conduct in the future, required it to notify all those whom it had spammed of what it had done, and ordered it to delete all wrongfully obtained eBay user information.

Toysmart.com was a “popular” website that sold children’s toys, and also “collected detailed personal information about its visitors” through its website, including “the names and birthdates of children.” It had a posted privacy policy stating that any personal information it collected would “never” be shared with third parties. Toysmart.com eventually went bankrupt and tried to sell its database of customer information as an asset. On July 10, 2000, the FTC filed suit in District Court in Boston to enjoin the sale.

Rather than fight the FTC, Toysmart settled eleven days later. The settlement agreement prohibited it from selling its customer list “as a stand-alone asset.” The agreement did allow, however, the sale of the information to a buyer “in a related market” that agreed to “abide by the terms of the Toysmart privacy statement.”

Commissioners Anthony and Swindle believed that the settlement did not do enough “to protect consumer privacy.” As Commissioner Swindle said, “‘never’ really means never.” TRUSTe, the online seal program, also “objected to the settlement because it did not sufficiently protect the promise embodied in the Toysmart privacy statement and Toysmart’s contractual obligation as a participant in the TRUSTe program.”

consent agreement, two Commissioners rejected this theory as not legally colorable; the deceptive practice theory was enough. See Press Release, FTC, Online Auction Site Settles FTC Privacy Charges (Jan. 6, 2000) [hereinafter ReverseAuction Press Release], http://www.ftc.gov/opa/2000/01/reverse4.htm.

251. See ReverseAuction Press Release, supra note 250.


254. Id.

255. Id.


258. Id.

259. Id.

260. Id.

261. Id.


263. Walter W. Miller, Jr. & Maureen O’Rourke, Bankruptcy Law v. Privacy
what was viewed as a publicity move, The Walt Disney Company eventually purchased the customer list and destroyed it.  

c. COPPA: The FTC Gets More Muscle

The one large piece of Internet privacy regulation that Congress has passed is COPPA—the Children's Online Privacy Protection Act of 1998. COPPA was enacted after "a three-year effort" by the FTC, culminating in a March 1998 survey of 212 websites aimed at children. Eighty-nine percent of those websites collected personal data from children, but only twenty-four percent had posted privacy policies. Furthermore, "only one percent required parental consent to the collection or disclosure of children's information."  

COPPA was signed into law on October 21, 1998. The statute directed the FTC to promulgate regulations that require websites that collect personal information from children to do the following: (1) "provide notice... of what information is collected," how such information is used, and how it is disclosed to third parties; and (2) "to obtain verifiable... consent" from the children's parents before "the collection, use, or disclosure" of the children's personal data. The statute also provides for a rule that requires websites to do as follows: (1) provide parents, at the parents' request, with a description of the personal data collected from their child; and (2) cease collecting or maintaining information about the child if the parent refuses permission to the website. Other rules contemplated would forbid websites from "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity," and would require websites "to protect the confidentiality, security, and integrity" of the personal data they collect from children.


264. See id.
267. Id.
268. Id.
270. Id. § 6502(b)(1)(A)(i).
271. Id. § 6502(b)(1)(A)(ii).
272. Id. § 6502(b)(1)(B)(i).
273. Id. § 6502(b)(1)(B)(ii).
274. Id. § 6502(b)(1)(C).
275. Id. § 6502(b)(1)(D).
COPPA calls on the FTC to enforce the regulations as well.\textsuperscript{276} Violations of the regulations issued by the FTC and proscribed under COPPA are to be considered unfair and deceptive trade practices.\textsuperscript{277} The FTC issued its proposed rule implementing COPPA on April 27, 1999, and the rule became effective on April 21, 2000.\textsuperscript{278} The final rule\textsuperscript{279} implements all of the statutory provisions by requiring the following: clear posting of a privacy notice, verifiable parental consent, choice regarding disclosure to third parties, and enforcement authorization.\textsuperscript{280}

Shortly after the rule went into effect, the FTC began surfing the Internet and checking children's websites to see if they were complying with the rule.\textsuperscript{281} About three-fourths of the websites the FTC visited collected personal data from children; of those, "roughly half appeared to have substantial compliance problems."\textsuperscript{282} The FTC sent these sites a warning e-mail.\textsuperscript{283}

The first enforcement of the COPPA rule came quickly. In its July 2000 complaint against Toymart.com, the FTC alleged violations of the COPPA rule, along with deceptive trade practices.\textsuperscript{284} Less than a year later, the FTC went to court again to enforce the rule. The FTC sued Looksmart Ltd., Monarch Services, Inc. and Girls Life, Inc., and Bigmailbox.com, Inc.,\textsuperscript{285} charging them with violations of the Children's Online Privacy Protection Rule and with unfair or deceptive acts or practices in violation of section 5 of the FTCA.\textsuperscript{286} Not surprisingly, the websites settled.\textsuperscript{287} The settlement agreements provided that each website delete all personal data collected from

\textsuperscript{276} Id. § 6505(a).
\textsuperscript{277} Id. § 6502(c).
\textsuperscript{278} See COPPA Press Release, supra note 266.
\textsuperscript{279} 16 C.F.R. § 312 (2001).
\textsuperscript{280} See COPPA Press Release, supra note 266.
\textsuperscript{282} Id.
\textsuperscript{283} Id.
\textsuperscript{289} Id.
children since COPPA became law. The websites were required to post a privacy policy and a link to the FTC's web page offering "helpful information about COPPA." Further, Bigmailbox.com was barred "from making deceptive claims in its privacy policy." Girlslife.com was fined $30,000; Bigmailbox.com and Looksmart Ltd. were each fined $35,000.

Recently, the FTC initiated two more actions. In September 2001, the FTC filed suit against Lisa Frank, Inc., alleging violations of the Children's Online Privacy Protection Rule and section 5 of the FTCA. The website's privacy policy made "false or misleading statements" pertaining to parental consent. Lisa Frank, Inc. settled, agreed to abide by COPPA in the future, and paid a $30,000 penalty. On February 13, 2002, the FTC filed suit against American Pop Corn Company for violating the Children's Online Privacy Protection Rule by collecting personal data on its website from children under thirteen years of age without parental consent. The matter was settled the very next day. In the settlement agreement, American Pop Corn Company agreed not to violate the Rule in the future and to pay a civil penalty of $10,000.

d. Gramm-Leach-Bliley

The Financial Services Modernization Act (popularly known as Gramm-Leach-Bliley) was passed on November 12, 1999. The Act "created sweeping deregulation in the financial services industry while putting in place greater regulation to protect the privacy of consumers' non-public personal information." Like COPPA, the Act required the FTC to promulgate privacy regulations. The FTC issued the Privacy of Consumer Financial Information Rule in May 2000, implementing the three requirements of the Act's provisions.

290. Id.
291. Id.
292. Id.
293. Id.
295. Id. ¶ 20.
298. See id.
299. Id.
301. See Boam, supra note 90, at 182.
302. Wolf & Hochman, supra note 9, at 10.
303. Id.
First, a financial institution must give notice to its customers "about its privacy policies and practices"—in particular, its practices regarding the disclosure of personal information to third parties. Second, a financial institution "must provide its customers with annual notices of its privacy policies and practices." Third, financial institutions must give customers the ability to "opt out"—to request that their personal information not be disclosed to third parties. Although the Rule went into effect on November 13, 2000, the deadline for compliance was extended to July 1, 2001.

At first, the Act "created a great deal of confusion among companies" over the meaning of "financial institution." The Rule interprets the Act broadly and defines "financial information" as "any personal information gathered by a financial institution." Nevertheless, the privacy provisions of the Act have not been without their critics. "[A]ny privacy policy is meaningless unless it is enforceable." The Safe Harbor relies on the FTC for its enforcement. Whether or not the FTC has the legal capacity, however, to enforce the Safe Harbor has been a matter of dispute.

II. CRITICISMS OF THE SAFE HARBOR'S ENFORCEMENT MECHANISM

This part will examine three criticisms of the proposed FTC enforcement of the Safe Harbor agreement: (1) that no one knows what an enforcement action will look like; (2) that the FTC does not have the resources and expertise to enforce the agreement effectively; and (3) that the FTC does not have the statutory authority to enforce the agreement.

First, the mechanism established to enforce the Safe Harbor has been "criticized both within and outside the United States" as "loose" and "unclear." Even a United States Representative has called the Safe Harbor's legal status "highly questionable." U.S.

305. Id.
306. Id.
307. Id.
308. Id.
309. Gensch, supra note 222.
310. Boam, supra note 90, at 182.
311. See, e.g., Safe Harbor Hearings, supra note 11, at 39 (testimony of the Hon. Edward J. Markey) ("The privacy provisions of that Act are a pathetic joke."); id. at 98 (testimony of Joel R. Reidenberg) ("I think it is nonsense that Gramm-Leach-Bliley meets the standards contained in the European directive.").
312. Id. (testimony of the Hon. Edolphus Towns).
313. Reidenberg, supra note 19, at 745.
315. Despeignes & Hargreaves, supra note 165; see also Hyman & Covington, supra note 32 ("It is unclear at this time how the sanctions will be enforced . . . .").
316. Safe Harbor Hearings, supra note 11, at 6 (statement of W. J. "Billy" Tauzin).
privacy advocates claim it will be "meaningless" if challenged.\textsuperscript{317} The European Union Working Party that was established to investigate the adequacy of other countries' privacy laws described the Safe Harbor enforcement mechanisms as "very confusing" and "simply a series of recommendations which can lead to a fragmented and uneven implementation."\textsuperscript{318} The confusion may arise from the fundamentally different ways in which Europeans and Americans view privacy, and in their respective approaches to protecting it. As previously discussed, the European model of data protection is a top-down, bureaucratic approach,\textsuperscript{319} while the American model of privacy protection is a combination of industry self-regulation and a "patchwork" of federal privacy legislation.\textsuperscript{320} It is understandable that European citizens—as well as their American counterparts—might be unfamiliar with the sometimes labyrinthine regulatory structure of federal administrative agencies.

Second, criticism has focused on the role of the FTC itself, instead of the overall enforcement structure. Specifically, "the FTC was not created for such a task and does not have the expertise or authority to effectively monitor or enforce privacy issues on the Internet. Furthermore, the FTC has many other duties and is thus unable to commit sufficient resources to the protection of individuals' privacy on the Internet."\textsuperscript{321} The question is whether the FTC, which has a variety of other responsibilities and functions, will be able to act as an effective watchdog.

Finally, Professor Joel R. Reidenberg has provided the most precise criticism of the enforcement mechanism. Specifically, he claims that the "Safe Harbor faces a serious jurisdictional obstacle to its enforcement .... [T]he underlying legal authority of the FTC to enforce [the] Safe Harbor is questionable."\textsuperscript{322} Professor Reidenberg notes that the "stated Congressional purpose" of the FTCA was to prohibit "unfair and deceptive acts and practices which deceive and defraud the public generally."\textsuperscript{323} The "public," however, means the American public: the FTCA and its subsequent amendments "at no
time contemplated protecting... foreign consumers." Professor Reidenberg calls "the assertion" that the FTC has the statutory authority to bring enforcement actions on behalf of European consumers "a radical departure from the stated legislative purposes of the statute." Section 5(a)(1) of the FTCA declares that "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." Section 5(a)(2) then charges the FTC with preventing "persons, partnerships, or corporations... from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." As discussed above, the FTC's recent enforcement actions in the area of online privacy have used the power bestowed by section 5 to prohibit deceptive practices. Specifically, in each case the FTC has alleged that, when a company provides consumers with a stated privacy policy, and then fails to abide by the terms of that policy, it is engaging in a deceptive trade practice.

But what, exactly, is a deceptive trade practice? The FTCA "does not define 'deception,' thus leaving it to the courts and the FTC to determine the meaning of that word." Indeed, "Congress has delegated enormous power to the FTC in this field." Courts, additionally, "treat Commission decisions with great deference." In sum, "it has fallen largely to the FTC to decide what constitutes deception."

In the context of the Safe Harbor, the FTC has defined a deceptive practice as "a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion." In the context of an enforcement action, a company's public statement that it adheres to the principles of the Safe Harbor is a representation. Subsequently failing to adhere to them in processing personal data is a practice, one that is "likely to mislead" in light of the stated privacy policy. It is arguable that this practice misleads "in a material fashion," as consumers might be less willing to purchase goods online.

324. Id.
325. Id.
327. Id. § 45(a)(2).
328. See supra notes 231-52, 281-99 and accompanying text.
330. Id.
331. Id.
332. Id.; see also George et al., supra note 25, at 777 (noting that the FTCA gives the FTC "comprehensive powers" to prohibit deceptive practices).
without adequate privacy assurances. The only criterion in question is whether such a practice misleads consumers.

What, then, is meant by "consumer"? Again, the FTCA does not use the term, the Safe Harbor agreement does not define it, and it is certainly arguable that the term "consumer" was not meant to cover citizens of the European Union. The question is important because the Safe Harbor applies only to data collected from European citizens—participants are under no obligation as far as American consumers are concerned.

Consider the following hypothetical:

Horatio decides to drop out of law school and join the information technology revolution. He rents a small suite in an office park in Little Rock, Arkansas, and forms a company called Super Crunchy Data Crunchers. He leases computer equipment and software, and hires staff for his data processing operation.

Horatio's good friend, Hamlet, works for a large Danish corporation, Claudius Corp., where he is in charge of the customer relations department. A direct-marketing company based in Poland, Fortinbras Inc., has been contacting him, asking to purchase Claudius Corp.'s consumer database. Denmark's Directive-compliant data-protection statute prohibits this, so Hamlet decides to enlist Horatio and Super Crunchy in a scheme. Super Crunchy will register for the Safe Harbor, so that it will be presumed to provide adequate protection, and the transfer of the consumer database from Denmark to the United States will proceed without hindrance. Super Crunchy then will process the Danish data, transfer it to Fortinbras Inc., and split the proceeds with Claudius Corp.

Super Crunchy has no American customers; it does not advertise, do business, or otherwise have any contact with anyone but Claudius Corp. and Fortinbras Inc. One of Hamlet's disgruntled business associates, Ophelia, gets wind of the scheme and notifies the Danish data-protection authority, which then notifies the FTC. The FTC

334. See, e.g., Safe Harbor Hearings, supra note 11, at 45 (statement of David L. Aaron) (noting that, in 2000, e-business lost $16 billion in potential sales due to lack of consumer trust); id. at 26 (testimony of Towns) (citing a Kearny Management Group survey reporting $6 billion in lost online sales: "[I]nvasive information requests are blamed for 52 percent of sales that fall apart, followed by reluctance to enter credit cards, 46 percent."); id. at 26 (testimony of David Smith, Assistant Commissioner, Office of the UK Information Commissioner) ("Your figures are supported by a whole range of studies . . .").


336. See Safe Harbor Hearings, supra note 11, at 67 (statement of Joel R. Reidenberg) ("Congress has yet to specifically authorize the FTC to protect foreign consumers.").

337. See Safe Harbor Principles, supra note 12 (defining "personal data" and "personal information" as "data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form").
wants to bring a section 5 enforcement action against Horatio and Super Crunchy, but who is the "consumer" in this scenario? There are no Americans involved, and European consumers are implicated only at second remove.

Is this a deceptive trade practice—a representation, omission, or practice that is likely to mislead reasonable consumers in a material fashion—if the accused company's "consumers" are a Polish corporation and a Danish corporation complicit in the data processing scheme? This Note addresses these criticisms in turn, and suggests a solution to the most troubling one: the FTC's possible lack of statutory authority to enforce the Safe Harbor agreement.

III. IN DEFENSE OF THE SAFE HARBOR

A. What a Safe Harbor Enforcement Action Will Look Like

It is clear that the FTC will attempt to enforce the Safe Harbor using section 5 of the FTCA. The FTCA authorizes the FTC to issue complaints and cease-and-desist orders to those it finds to be engaging in a deceptive trade practice. If a company violates a final order, it faces civil fines of up to $11,000 a day. Additionally, if the FTC finds that there is "a widespread pattern" of deceptive practices, it may issue an administrative rule prohibiting the deceptive practice involved.

Over the past few years, the FTC has built a track record of filing complaints against websites that violate their stated privacy policies, COPPA, or both. Each of these complaints has alleged a deceptive trade practice in violation of section 5. Specifically, the complaints alleged that the defendants misled consumers by telling them one thing and then doing another.

Once an organization certifies that it adheres to the Safe Harbor principles, it is subject to FTC supervision. It must also clearly

338. See, e.g., FAQ No. 11, supra note 126 ("If the FTC concludes that it has reason[s] to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect.").
341. 15 U.S.C. § 57(a)(b)(3)(B); Safe Harbor Enforcement Overview, supra note 138. Anyone who knowingly violates an FTC rule is also subject to a fine of up to $11,000 a day. Id.
342. See supra notes 231-64, 281-99 and accompanying text.
343. In its action against ReverseAuction.com, the FTC also alleged unfair acts or practices, but this legal theory was not fully supported by the FTC, and was dropped in subsequent actions. See supra text accompanying notes 233-36.
344. This is simply because a company that publicly declares that it follows the Safe Harbor principles, but fails to do so, is engaging in a deceptive trade practice. See
signify in its privacy statement (if it does not have a privacy statement, it must create one) that it adheres to the principles. If the organization then fails to do so, it is making misrepresentations to consumers just as GeoCities, Liberty Financial Companies, ReverseAuction.com, Toysmart.com, Looksmart and GirlsLife.com, Lisa Frank, and the American Pop Corn Company were making misrepresentations to their consumers. Lack of adherence to the Safe Harbor is just as much a deceptive practice and actionable under section 5 as those companies' practices were.

So far, so good. But all the cases begun by the FTC settled quickly—within a day, in one case. We do not know for sure whether this is because the law is clearly on the FTC's side, or because penniless dot-coms chose not to fight one of the most powerful regulatory agencies of the federal government, or because they wanted simply to avoid negative publicity (particularly, one would think, in the case of COPPA violations). Or perhaps the companies involved simply did not know that they were breaking the law. Perhaps the result would be different if an industry giant like Microsoft or Intel chose to fight the FTC in court. But for now, it is clear how the FTC would go about punishing violations of the Safe Harbor: by filing a complaint charging a deceptive trade practice, then seeking injunctive relief through a cease-and-desist order, which would then be followed by a final agreement and perhaps a fine for willful violations.

Pitofsky Letter, supra note 333 ("[I]f a web site falsely claims to comply with a stated privacy policy . . . Section 5 of the FTC Act provides a legal basis for challenging such a misrepresentation as deceptive.").

346. See supra text accompanying notes 231-38.
347. See supra text accompanying notes 239-42.
348. See supra text accompanying notes 248-52.
349. See supra text accompanying notes 253-64.
350. See supra text accompanying notes 285-93.
351. See supra text accompanying notes 294-96.
352. See supra text accompanying notes 297-99.
354. With the availability of more funds for enforcement actions, see supra note 223 and accompanying text, the FTC will not have to focus solely on "extreme" cases. Gensch, supra note 222, at 5.
355. See generally notes 231-64 and accompanying text (describing past FTC privacy enforcement actions).
B. Can the FTC Act as an Effective Watchdog?

1. The FTC Was Created for Such a Task

The FTC was created to be a consumer-protection agency. The FTC has two missions: to enforce the antitrust laws and to provide consumer protection.356 The FTCA was passed in 1914 to protect consumers from unfair competition.357 The FTC’s consumer protection authority was expanded by Congress in 1938 and again in 1975.358

Moreover, the FTC has shown a consistent willingness both to call for greater privacy protection for consumers359 and to enforce privacy rights in the courts.360 The FTC has presented special reports concerning online privacy to Congress,361 was instrumental in getting a major privacy statute (COPPA) enacted,362 and has called for further legislation to protect consumers.363

2. The FTC Does Have the Expertise or Authority to Effectively Monitor or Enforce the Safe Harbor

So far, only 168 firms have joined the Safe Harbor364—it cannot be that hard to monitor them. The FTC relies on referrals from consumers themselves as well as their own investigative activities. Consumers can complain to the FTC directly via a form on their website365 or their toll-free hotline.366 Additionally, participants in the

358. Reidenberg, supra note 19, at 740-41.
359. See supra Part I.C.2.a.
360. See supra Part I.C.2.b.
361. See supra notes 199-230 and accompanying text.
362. See COPPA Press Release, supra note 266 (“The COPPA was enacted following a three-year effort by the Commission . . . . The Commission recommended that Congress enact legislation concerning children . . . .”); see also Press Release, FTC, FTC Releases Report on Consumers’ Online Privacy (June 4, 1998), http://www.ftc.gov/opa/1998/9806/privacy2.htm (summarizing the 1998 FTC Privacy Report and listing “Recommendations for Protecting Children’s Privacy Online” that later were included in COPPA).
363. See supra text accompanying note 221.
364. See supra text accompanying note 154.
365. See Federal Trade Commission Consumer Complaint Form, OMB #3084-0047, at http://www.ftc.gov/dod/woisolcq3.startup?Z_ORG_CODE=PU01 (last visited Mar. 20, 2002). Consumers may also forward unsolicited e-mail (spam) to the e-mailbox UCE@ftc.gov. Id.
366. Challenges Facing The Federal Trade Commission, supra note 225. The FTC took action against DoubleClick, see supra notes 243-47, after receiving several such complaints. See Boam, supra note 90, at 180. Through its toll-free number and its website, the FTC “receives over 10,000 consumer complaints about fraudulent and deceptive business practices each week.” FTC, Privacy Agenda (Oct. 4, 2001) [hereinafter Privacy Agenda], http://www.ftc.gov/opa/2001/10/privacyagenda.htm.
Safe Harbor will be subject to "spot checks" by European data-protection authorities, who will then refer violations to the FTC.\textsuperscript{367}

As for enforcement expertise, the FTC has brought approximately 100 privacy actions so far.\textsuperscript{368} It should also be noted that there are no other federal agencies that have the FTC's extensive experience with consumer protection and deceptive trade practices or that focus on enforcing the privacy rights of consumers. For now, the FTC is the only game in town.\textsuperscript{369}

3. The FTC Is Able to Commit Sufficient Resources to Enforce the Safe Harbor

Again, there are only 168 companies in the Safe Harbor so far—not a number that requires an extraordinary commitment of resources, particularly when EU authorities and consumers also play their parts.\textsuperscript{370} Additionally, the privacy actions the FTC has undertaken to date settle very quickly.\textsuperscript{371} Although the new chairman, Timothy J. Muris, has backed off from his predecessor's call for federal legislation,\textsuperscript{372} he has proposed that the resources dedicated to enforcing existing rules—including the Safe Harbor—be increased by fifty percent.\textsuperscript{373} In its 2002 Privacy Agenda, the FTC specifically promised "[n]ew efforts [to] focus on cases involving . . . the failure of companies to meet commitments made under the European Union Safe Harbor program to provide privacy protections."\textsuperscript{374} Indeed, the FTC has promised to enforce Safe Harbor violations on a priority basis.\textsuperscript{375}

Finally, FTC actions would have a deterrent effect, and most companies will be easily persuaded to follow the Safe Harbor requirements than risk the wrath of a full regulatory battle—and all the ensuing publicity. "Companies do heed the words of the FTC and do respond to problems the FTC identifies through its enforcement actions."\textsuperscript{376} As one commentator put it, being subject to a FTC section 5 action is "like facing a nuclear bomb in a food fight."\textsuperscript{377}

\textsuperscript{367} Messmer, supra note 158, at 8.
\textsuperscript{368} George et al., supra note 25, at 748 n.56.
\textsuperscript{369} See Sovern, supra note 329, at 1321 ("[O]nly the FTC itself can enforce the FTC Act" upon which the Safe Harbor is based).
\textsuperscript{370} See supra notes 364-67 and accompanying text.
\textsuperscript{371} See supra note 353.
\textsuperscript{372} See supra text accompanying note 224.
\textsuperscript{373} See Muris, supra note 223; supra text accompanying note 223.
\textsuperscript{374} Privacy Agenda, supra note 366.
\textsuperscript{375} Muris, supra note 223; see also Sykes & de Bony, supra note 114 ("The safe harbor principles also mandate that the [FTC] expedite complaints by EU citizens about how their data was handled in the United States, processing them faster than complaints from U.S. citizens . . . ."); Pitofsky Letter, supra note 333.
\textsuperscript{376} Gensch, supra note 222; see also Gladstone, supra note 55, at 28 ("Upon the recommendation of the FTC many web sites now publish their privacy policies . . . .").
\textsuperscript{377} Gensch, supra note 222.
C. Whether the FTC Has Statutory Authority to Enforce the Safe Harbor Agreement

1. “Consumer”

As discussed above, the FTC has defined a deceptive trade practice as a representation, omission, or practice that is likely to mislead reasonable consumers in a material fashion. But what is a consumer? The FTCA does not define the term; neither does the Safe Harbor agreement itself. The Safe Harbor, however, does offer the following definition: “[p]ersonal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded “in any form.” Therefore, the Safe Harbor’s provisions apply only to data that has been transferred from the EU—that is, the personal data of European consumers.

All the FTC’s privacy cases have been against domestic companies. The FTC, for its part, insists that it can act on behalf of foreign consumers. As an example, the FTC cites its 1998 enforcement action against Fortuna Alliance, the operator of a worldwide pyramid scheme. The FTC filed a complaint against the website, charging unfair and deceptive acts and practices in violation of section 5—in particular, the promise made to consumers of fabulous returns on their “investment.” A settlement was reached, whereby the website agreed to pay refunds to 15,622 customers in the United States and seventy foreign countries. Over half of the scam’s victims, however, were U.S. citizens, and more than half of the

---

378. Pitofsky Letter, supra note 333.
380. See supra notes 231-99 and accompanying text.
381. See Pitofsky Letter, supra note 333 (“In the past, the Federal Trade Commission has provided redress for citizens of both the United States and other countries. The FTC will continue to assert its authority, in appropriate cases, to provide redress to citizens of other countries who have been injured by deceptive practices under its jurisdiction.” (footnote omitted)).
384. Fortuna Press Release, supra note 382; see also FTC, FTC Refund Program for Fortuna Alliance (listing countries, the total number of consumers defrauded, and the amount of various refunds paid), http://www.ftc.gov/opa/1998/9807/ftcrefund01.htm. Sharp FTC watchers may notice that the list includes such “countries” as “Gibraltar,” Puerto Rico, Scotland, and Wales. Id.
refund money went to them. Moreover, the FTC may not have been able to bring the foreign refunds to pass without outside help.

In our hypothetical, would the FTC be able to punish Super Crunchy for lying to them and cheating on the Safe Harbor? Under the definition of deceptive trade practice the FTC has adopted, it is doubtful. Under that definition, whether or not a company's behavior is a deceptive trade practice—and, therefore, whether or not the FTC has jurisdiction to bring an enforcement action—hinges on the term "consumer." In the hypothetical, Super Crunchy Data Crunchers is the Safe Harbor participant, and its only consumer is Fortinbras Inc., a foreign company. The FTC would be on shaky ground if it attempted to bring an enforcement action based on the current definition of "deceptive trade practice," for Fortinbras Inc. arguably does not fall within the definition of the "public."

2. Rulemaking Under the FTCA

The FTC has rulemaking power under the FTCA to define what it considers a deceptive or unfair trade practice. There must be a "widespread pattern" of deceptive practices, or the FTC must have already issued cease-and-desist orders in like cases, before a rule may be promulgated.

The FTC has used its rulemaking authority in the past to prohibit industry conduct that no one had previously thought of as deceptive. The FTC wields "such broad discretion in defining deceptive and unfair conduct that if the FTC could produce colorable arguments that the [industry conduct] violate[s] the FTC Act, it is very likely that courts would sustain that judgment." For example, the rule that the FTC issued to enforce COPPA simply states that "a violation of [the Commission's rules implementing COPPA] shall be treated as . . . an

385. See FTC Refund Program for Fortuna Alliance, supra note 384. U.S. citizens comprised 8894 of the 15,625 victims, and received $3,175,801 out of the total of $5,501,127 paid. Id.

386. See Fortuna Press Release, supra note 382 ("The FTC used counsel in London, Belize, and Antigua for foreign litigation freezing defendants' offshore bank accounts. The Department of Justice's Office of Foreign Litigation was instrumental in reaching settlement of the foreign actions.").

387. See supra note 333 and accompanying text.

388. See supra notes 323-24 and accompanying text.


391. See, e.g., Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672 (D.C. Cir. 1973). The D.C. Circuit, in an opinion by J. Skelly Wright, reversed a lower court ruling that the FTC did not have the authority under the FTCA to issue rules and regulations having the substantive force of law. Id. at 697-98. The FTC had issued a rule declaring the failure to post octane ratings on a gasoline pump a deceptive act or practice "without the necessity of further proof." Nat'l Petroleum Refiners Ass'n v. FTC, 340 F. Supp. 1343, 1345 (D.D.C. 1972), rev'd, 482 F.2d 672 (D.C. Cir. 1973).

392. Sovern, supra note 329, at 1322.
unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act." 393

The privacy rule passed by the FTC to enforce COPPA operates on a deceptive-practice theory. 394 The Children's Online Privacy Rule does not use the term "consumer," but rather "child." 395 The Rule defines "child" simply as "an individual under the age of 13." 396 The jurisdiction of the FTC is not limited by national boundaries—indeed, "operator" is defined as "any person who operates a website located on the Internet" that collects personal data from children "involving commerce" between the states or with foreign countries. 397 Following Gramm-Leach-Bliley, the Privacy of Consumer Financial Information Rule defines "consumer" as "an individual who obtains or has obtained a financial product or service." 398 Again, no reference is made to "U.S. consumers" or other jurisdictional boundaries, and one would assume that Congress did not intend to exclude foreign nationals with assets in American financial institutions from the protections of the Act. In both Acts, who the consumer or child is, and where they reside, are beside the point. The issue simply is whether that person has been a victim of a deceptive practice.

Therefore, the FTC should promulgate a rule declaring that, a company misrepresenting to its consumers that it follows the principles of the Safe Harbor agreement while not actually doing so is a deceptive trade practice under section 18(a)(1)(B) of the Federal Trade Commission Act. As with COPPA and Gramm-Leach-Bliley, such a rule would apply to any participating company, regardless of who is the "consumer." In doing so, the FTC would benefit from not only the National Petroleum Refiners decision 399 but also from judicial deference under the Chevron Doctrine. Under Chevron U.S.A., Inc. v. Natural Resources Defense Council, 400 the FTC's definition of "deceptive trade practice" would stand if it is "a permissible construction of the statute." 401

COPPA and Gramm-Leach-Bliley are statutory mandates that specifically direct the FTC to create rules to enforce their provision.

394. See supra note 277 and accompanying text.
395. 16 C.F.R. § 312.2.
396. Id.
397. Id.
398. Id. § 313.3(e)(1).
399. See supra note 391 and accompanying text.
401. See id. at 843-44. The Court stated:
   If Congress has explicitly left a gap for the agency to fill, there is an express delegation of authority to the agency to elucidate a specific provision of the statute by regulation. Such legislative regulations are given controlling weight unless they are arbitrary, capricious, or manifestly contrary to the statute.

Id.
The FTC has argued that the reason the statutes were passed in the first place is to require all websites and financial institutions to create and abide by privacy policies, something that was not possible by using its rulemaking power alone. Under the Safe Harbor, participation is voluntary, and all those who have signed on have agreed to abide by its principles. No statute is needed to give the FTC jurisdiction over cheaters and liars; the companies in the Safe Harbor are all American.

Nevertheless, the FTC's current definition of "deceptive trade practice," and the uncertainty of the term "consumer," make FTC enforcement of the Safe Harbor vulnerable to judicial attacks. The surest answer to the problem, of course, is for Congress to pass a statute declaring that cheating on the Safe Harbor constitutes a deceptive trade practice, and granting the FTC authority to issue rules to that effect, pursuant to its power to regulate commerce with foreign nations. Given Congress's past failure to enact a broad privacy statute, and given the new FTC Chairman's focus on more enforcement, not more legislation, this should not be expected in the near future. But, it remains the only available way to fully eliminate the doubts of the European Union—and American privacy advocates—as to whether the Safe Harbor can be effectively enforced.

CONCLUSION

The remaining criticism, not fully treated in this Note, of the Safe Harbor and the European Directive is that it will cost American business—and therefore, American consumers—money. Its requirements, however, are not all that burdensome. Under COPPA, websites that collect personal data already have to operate under an entirely different set of rules for an entire segment of the population—children under thirteen. In practice, COPPA has not proven to be unworkable. Compliance with the Safe Harbor is not all that costly, either. Microsoft, by its own estimate, spent $500,000 to become compliant after its Spanish imbroglio. While that sum could pay for the education of six or seven new lawyers, it is hardly going to hurl Microsoft (or most of the other companies on the Safe Harbor list) into bankruptcy. Finally, the companies that are on that list are

---

402. See supra note 220 and accompanying text.
403. U.S. Const. art. I, § 8, cl. 3.
404. See supra note 222 and accompanying text.
405. See supra note 29.
406. Under the GeoCities Consent Agreement, GeoCities would "collect certain 'limited screening information' from customers attempting to register at the site for the purpose of identifying and blocking children 12 and under from registering without their parent's permission." Geocities Press Release, supra note 231. If a website can "screen" children during registration, it is not far-fetched to propose that it also can screen EU citizens.
there because they signed up. If a company thinks the terms are too onerous, and FTC oversight too harsh, they may withdraw from the Safe Harbor and bet that the European regulatory authorities will be lax in their enforcement.\textsuperscript{408} You pays your money and you makes your choice.

The Safe Harbor is a rather unusual agreement; it provides priority federal enforcement of the rights of foreign citizens—rights that United States citizens do not have. One commentator has argued that enforcing the Safe Harbor will create "a vast legal chasm" and "a double standard" that "might be legal" but "makes for exceptionally poor public policy."\textsuperscript{409} Perhaps. But the fact remains that the Safe Harbor, however else it may be characterized, is one more piece in the federal privacy patchwork. And when it is demonstrated once again that privacy standards can be adopted and enforced without bankrupting the online marketplace, the privacy cause in the United States will be advanced another step. The EU, for its part, realizes that the Directive is somewhat draconian, and some predict that it will "soften it" in the enforcement process.\textsuperscript{410} On the other hand, the EU's enforcement of the Directive has already been described as "lax," while "the U.S. systematically enforces its privacy laws."\textsuperscript{411} There probably will be plenty of adjustments on both sides in the short term to come to an agreement both sides can live with. The long-term industry trend, however, is "toward more enforcement and more compliance."\textsuperscript{412} The Safe Harbor agreement is a good place to start.\textsuperscript{413}

\textsuperscript{408} See Assey & Eleftheriou, \textit{supra} note 18, at 151.
\textsuperscript{409} Clear, \textit{supra} note 29, at 1017.
\textsuperscript{410} Loomis, \textit{Safeguards}, \textit{supra} note 91.
\textsuperscript{411} Safe Harbor Hearings, \textit{supra} note 11, at 46 (statement of Jonathan M. Winer).
\textsuperscript{412} Loomis, \textit{Safeguards}, \textit{supra} note 91.
\textsuperscript{413} See, e.g., Safe Harbor Hearings, \textit{supra} note 11, at 80 (statement of Barbara Lawler, Customer Privacy Manager, Hewlett-Packard Company) ("Joining the Safe Harbor is the next logical step in [Hewlett-Packard's] commitment to privacy protection.").