Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement

Daniel R. Leathers

Follow this and additional works at: https://scholarlycommons.law.case.edu/jil
Part of the International Law Commons

Recommended Citation
Available at: https://scholarlycommons.law.case.edu/jil/vol41/iss1/8

This Note is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Journal of International Law by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.
GIVING BITE TO THE EU-U.S. DATA PRIVACY SAFE HARBOR: MODEL SOLUTIONS FOR EFFECTIVE ENFORCEMENT

Daniel R. Leathers

In 1998, the European Union (EU) and the United States (U.S.) set out on an ambitious project to develop a program by which U.S.-based companies could conform to the strict EU data privacy directive when transferring EU citizens’ data. In effect, the program sought to reconcile EU and U.S. privacy laws when a U.S.-based company used or transferred EU citizens’ data. After two years of negotiations, the U.S. and the EU finalized a program now commonly known as the EU-U.S. Safe Harbor.

Yet, since the Safe Harbor’s inception, the program has been subject to heavy criticism from privacy advocates and an EU oversight committee. The heaviest criticism is levied against the Safe Harbor’s inadequate internal and external enforcement mechanisms.

This Note proposes several improvements and modifications to the Safe Harbor’s enforcement mechanisms, while acknowledging and addressing various U.S. law impediments.

I. INTRODUCTION

II. DIFFERING APPROACHES TO PRIVACY REGULATION AND ENFORCEMENT MECHANISMS

III. GENESIS OF THE PROBLEM: EU-U.S. DATA PRIVACY SAFE HARBOR PROGRAM

A. EU Data Transfers to Non-EU Nations

B. The Safe Harbor

C. Government Data Protection Enforcement Mechanisms

IV. THE GOOGLE-DDOUBLE CLICK MERGER: A CASE STUDY IN THE EUROPEAN UNION’S DETERIORATING TRUST IN THE U.S. PRIVACY REGULATORY SCHEME

A. Google’s Significant Collected Data

B. Initial European Union Concerns with Google’s Data Retention Practices

C. The Google-DoubleClick Merger

D. Future EU Regulation of Google, Search Engines, and

* This Note is current as of March 2008.
† Executive Articles Editor, Case Western Reserve Journal of International Law. B.A., The Pennsylvania State University (2005); J.D., Case Western Reserve University School of Law (2009).
Behavioral Advertising ................................................................. 218
E. Significance of European Union and Federal Trade
Commission Differences ................................................................. 219

V. SAFE HARBOR ENFORCEMENT LIMITATIONS AND PROPOSED
SOLUTIONS ...................................................................................... 220
A. Initial Registration Oversight by the U.S. Department of Commerce .......................................................... 220
B. The Enforcement Principle ........................................................... 224
C. Government Agency Enforcement through the Federal Trade Commission ..................................................... 231

VI. CONCLUSION ........................................................................... 242

I. INTRODUCTION

Privacy no longer can mean anonymity . . . it should mean that govern-
ment and businesses properly safeguards people’s private communications and financial information.

—Donald Kerr, Principal Deputy Director of U.S. National Intelligence

Everyday millions people in the European Union access websites owned and operated in the United States. They upload personal photos, log into bank accounts, make payments with credit cards, and input search in-
quiries. Massive amounts of data leave the control of consumers, and, more importantly, the jurisdictional reach of the European Union.

In 1998, the European Union (EU) and the United States (U.S.) set out on an ambitious project to develop a program by which U.S.-based multi-
tnational companies and data processors (Companies) could conform to the strict EU data privacy directive (Data Directive) when transferring EU member-state citizens’ (EU Citizens) data. In effect, the program sought to reconcile EU and U.S. privacy laws when a Company used EU Citizens’ data within the U.S. or transferred EU Citizens’ data to or from the U.S.

---

After two years of negotiations, the U.S. and the EU finalized the program and in the Safe Harbor Agreement (Safe Harbor) in late July 2000.

Yet, since the Safe Harbor’s inception, the program has been subject to heavy criticism from privacy advocates and an EU oversight committee. The heaviest criticism is levied against the Safe Harbor’s inadequate internal and external enforcement mechanisms. The Safe Harbor designates the Federal Trade Commission (FTC) as the primary external enforcement arm of the program, but as of 2004, the FTC had not prosecuted a single Company for violating the Safe Harbor’s protection of EU Citizens’ privacy rights.

The lack of enforcement has left citizens of EU member states, who ordinarily rely on enforcement by national privacy agencies, to become their own police agents and report Safe Harbor violations on their own. For example, a data breach at a Company could lead to thousands of stolen identities. Within the United States, data breach notification laws vary widely; and worse, under the Safe Harbor, a Company has no requirement to

---


7 See infra Part V.


10 See infra Part III.C.i.

11 See infra Part V.

notify affected EU Citizens. An EU Citizens’ data could be lost or sold and the end effects would be obvious to the EU Citizen, but it would be impossible to pinpoint the Company that was the source of the data breach. Without knowing which Company was victimized, an EU Citizen would be prevented from utilizing any of the Safe Harbor’s enforcement protections.13

Various U.S. failures to protect privacy, such as the Google-Double Click merger case study addressed in Part IV, have led to a deterioration of trust between EU and U.S. enforcement agencies.14 The EU views the U.S. and Companies as failing to adhere to the intent of the Safe Harbor.15 Nevertheless, it should be of little surprise to EU regulators that Companies and U.S. agencies do not take the Safe Harbor seriously. The Safe Harbor, which is self-regulatory in nature, fails to obligate enforcement and establishes oversight in U.S. agencies that are unaccountable to the citizens whose data flows they are supposed to protect. Together, the Safe Harbor’s internal enforcement mechanisms and U.S. agency enforcement—through the FTC—fail to provide the guarantee of a complete investigation, which is what EU laws secure. In summation, the Safe Harbor is a poor attempt to reconcile the differences between U.S. and EU privacy regulatory efforts.

This Note proposes several improvements and modifications to the Safe Harbor. These adjustments will better reconcile EU and U.S. privacy laws through effective Safe Harbor enforcement mechanisms, while acknowledging and addressing various U.S. law impediments. Therefore, this Note engages in a statutory analysis that seeks to strengthen the current law for the benefit of U.S. and EU citizens alike; however, this Note does not address the far-reaching implications of a “right to privacy.”16 Part II analyzes the differing approaches to privacy regulation between the U.S. and the EU and suggests that these differences are roadblocks to effective privacy regulation cooperation. Part III explains the details of the Safe Harbor program and its enforcement mechanisms. Part IV compares the level of regulatory scrutiny the U.S. and the EU applied to the Google-DoubleClick merger and suggests the differing approaches are evidence of the EU’s deteriorating trust in the U.S. privacy self-regulatory scheme. Part V outlines criticisms of the Safe Harbor’s limited enforcement mechanisms, recommends several solutions, and responds to potential criticisms.

13 See infra Part V.B.4.a (elaborating the data breach example). See also infra Part V.C.2.a (completing the analysis of the data breach example).
14 See infra Part IV.
15 See EU Safe Harbor Criticism, supra note 8, at 13–14.
16 Scattered throughout this Note are several examples of ends-based implications of a right to privacy. For example, Part IV addresses some of the real-world consequences of the Google-DoubleClick merger. See infra Part IV. This Note also discusses the events of data breaches. See infra Part V.B.4.a. See also Part V.C.2.a.
II. **DIFFERING APPROACHES TO PRIVACY REGULATION AND ENFORCEMENT MECHANISMS**

U.S. regulation of governmental collection and use of personal data are confined to the limited categories enumerated in federal statutes.\(^\text{17}\) U.S. regulation of private data collection is often called “sectoral” because only a few federal statutes regulate specific industries in limited circumstances.\(^\text{18}\) This leaves vast, unregulated gaps in the protection of data collected by private parties in the U.S.\(^\text{19}\) What Joel Reidenberg observed in 1995, remains true today:

> Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector. Legal rules have developed on an ad hoc, targeted basis, while industry has elaborated voluntary norms and practices for particular problems. Over the years, there has been an almost zealous adherence to this ideal of narrowly targeted standards.\(^\text{20}\)

The U.S. “sectoral” approach to privacy regulation, therefore, views statutes as a means to the end of privacy protection. For example, U.S. privacy legislation protecting medical and banking records is a means towards the end purpose of preventing possible abuse of the information.

In contrast, in the EU, regulation of the use, transfer, and processing of private data about identifiable persons is covered in sweeping “omnibus” data statutes.\(^\text{21}\) EU member states officially recognized the danger of private data collection as early as 1981.\(^\text{22}\) More recently, in 1995, the EU enacted the Data Directive,\(^\text{23}\) which regulates the exchange and transfer of any private data, including handwritten and oral communications.\(^\text{24}\) In contrast to the U.S. “sectoral” approach to privacy, the EU “omnibus” approach to privacy regulation views privacy as an ends with respect to its inherent nature;


\(^{19}\) **CHRISTOPHER WOLF, PROSKAER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE** 14-3 (Christopher Wolf ed., Practicing Law Institute 2007).


\(^{21}\) WOLF, supra note 19, at 14-6.

\(^{22}\) See Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 (giving individuals the right to ensure their person data is being used lawfully by private parties).

\(^{23}\) Data Directive, supra note 3.

\(^{24}\) WOLF, supra note 19, at 14-6.
the EU views privacy as a protected state-of-being that is representative of individual autonomy.\footnote{See Daniel J. Solove, The Future of Reputation 130 (2007) ("The disclosure of personal information can severely inhibit a person’s autonomy and self-development."). See also, Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373 (2000); Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609 (1999).} 

In the U.S., the vast majority of privacy regulation is enforced through private civil suits.\footnote{See Francesca Bignami, European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining, 48 B.C. L. Rev. 609, 684 (2007).} These suits must be initiated, researched, and litigated all at the expense of the plaintiff. Under the Data Directive, however, member state data protection authorities (Data Protection Authorities) have direct power to inspect private data processors and begin administrative proceedings against potential violators, which may result in fines or injunctions.\footnote{See id. at 648.} Therefore, under the Data Directive, individuals whose privacy may have been violated are not forced to bear a heavy monetary burden in order to pursue their cases. The Safe Harbor sought to reconcile these differences.

III. GENESIS OF THE PROBLEM: EU-U.S. DATA PRIVACY SAFE HARBOR PROGRAM

A. EU Data Transfers to Non-EU Nations

The Data Directive specifically prohibits sending personal data to any country without a “level of data protection” considered “adequate” by EU standards.\footnote{Data Directive, supra note 3, art. 25(1).} The determination of adequacy of foreign data protection involves the weighing of several non-exclusive factors, including the nature of that data, the purpose for processing, the duration of processing, the destination country’s laws on data privacy, and the security measures in place at the destination country.\footnote{Id. art. 25(2).} Based on these factors, the EU has designated only three major non-EU countries’ protections as adequate.\footnote{The three countries are those of Argentina, Canada, and Switzerland. See European Commission, Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, http://europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm (last visited Mar. 10, 2008).} The EU has never viewed U.S. privacy law as “adequate” to protect privacy rights because of its piecemeal privacy regulations.\footnote{See James A. Harvey, Struggle Continues with EU Personal Data Protection Directive, EuroWatch, Jan 15, 1999.} Initially, EU officials had hoped to convince U.S. lawmakers to adopt a broad privacy regime similar
to the Data Directive, but this effort failed due to fundamentally differing conceptions of liberty. Since the U.S. was unwilling to pass comprehensive data protection legislation that the EU would view as “adequate,” Companies were conflicted. When Companies transferred data to EU member states, they were in violation of the Data Directive. Companies could not affect the EU opinion of U.S. privacy law adequacy, nor could Companies realistically lobby the U.S. government to implement a broad privacy regime similar to the Data Directive. Companies instead ignored the Data Directive and continued to transfer data to EU member states. Fortunately for the Companies, the EU informally suspended Data Directive enforcement against Companies in 1998 and 1999.

As a solution, the EU allows each Company to serve, in effect, as its own country with respect to the Data Directive, by committing itself to one of three options. The first option requires a Company to bind itself to one of three pre-approved contracts that limit data transfers. The contracts essentially require the Company to act as if it were under the control of the Data Directive. The second option allows a Company to adopt binding corporate rules (Binding Corporate Rules).

Both of the first two methods leave much to be desired. The model contracts are too simplistic for Companies to use in complicated international transfers. The Binding Corporate Rules require a large investment and are unlikely to be used because they require Companies to open up their

---

32 See id.
33 See generally, Bignami, supra note 26.
34 See Harvey, supra note 31, at 8–9.
35 See id.
36 See id.
37 The EU Commissioner approved three types of contracts in three separate decisions. Commission Decision 2001/497/EC on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2001 O.J. (L 181) 19 (regulating controller to controller data transfers); Commission Decision 2002/16/EC on Standard Contractual Clauses for the Transfer of Personal Data to Processor Established in Third Countries, 2002 O.J. (L 6) 52 (regulating controller to processor data transfers); Commission Decision 2004/915/EC Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74 (creating a second contract option for controller to controller data transfers).
38 This option is directly approved by the Data Directive. See Data Directive, supra note 3, art. 26(4).
39 This option was created by the Data Protection Working Party, which is an advisory body that was created by article 29 of the Data Directive. See Data Directive, supra note 3, art. 29.
40 See WOLF, supra note 19, at 14-32.
41 See id.
internal files to routine inspections by EU member states’ Data Protection Authorities.42

The third option, which is the subject of this Note, is the Safe Harbor. In 1998, the U.S. Department of Commerce (DOC) and the European Commission began discussing the creation of a program for Companies to bind themselves to the Data Directive’s requirements.43 After two years of negotiations, the DOC and the EU eventually came to an agreement and created the Safe Harbor. The DOC promulgated a rule44 on July 24, 2000 adopting the Safe Harbor into U.S. law.45 The compromise was ratified by the EU on July 26, 2000 in a special “decision” that did not require individual EU member state ratification.46

B. The Safe Harbor

The Safe Harbor is an abnormal regulation that consists of several separate documents put together as one. The document sections include: (1) the European Commission’s decision that the Safe Harbor program is “adequate;” (2) a description of seven privacy principle requirements that Companies must follow to fulfill the agreement; (3) fifteen frequently asked questions and answers that help with statutory interpretation of the seven privacy principles; (4) a European Commission memorandum on the sufficiency of the FTC’s enforcement powers; (5) a European Commission memorandum on private causes of action for privacy breaches available within the U.S.; (6) a letter from the FTC to the European Commission clarifying the agency’s enforcement powers; (7) a letter from the Department of Transportation to the European Commission clarifying the agency’s enforcement powers; and (8) a list of U.S. agencies the European Commission has approved to properly enforce the agreement’s requirements.47

44 Rulemaking is procedure under administrative law where a U.S. governmental agency creates a rule that has the force of law after a notice and comment period. See 5 U.S.C. § 553 (2006). Further discussion on the requirements of rulemaking and administrative law are beyond the scope of this Note.
45 Safe Harbor Privacy Principles, supra note 5.
46 Safe Harbor, supra note 6.
47 Id.
The Safe Harbor is a voluntary self-certification system that is unique to the U.S. and requires Companies to treat data on EU Citizens as if that data were physically in Europe and subject to the Data Directive.

1. Safe Harbor registration

The DOC regulates the self-certification registration of Companies under the Safe Harbor and maintains a list of all registered Companies, including Companies whose membership has lapsed. The DOC reviews both the initial applications for the Safe Harbor and the mandatory annual renewals.

To register for the Safe Harbor, a Company simply completes an online registration form that requires several disclosures, including a description of the Company’s data collecting activities, a list of EU countries that the Company transfers data to or from, and—most importantly—a description of the Company’s privacy policy. A Company’s privacy policy must incorporate and address all of the Safe Harbor privacy principles. The Safe Harbor privacy principles are identical to those of the Data Directive: (1) Notice; (2) Choice; (3) Onward Transfer; (4) Security; (5) Data Integration; (6) Access; and (7) Enforcement.

A Company must swear to the accuracy of the online form it submits. The online form submission therefore is an affirmative representation of compliance with the Safe Harbor, similar to an affidavit. An affirmative representation is critical because the FTC can only “take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments.”

---

48 The Safe Harbor is voluntary because companies can choose to use model contracts to Binding Corporate Rules. See supra Part III.A.
49 Safe Harbor, supra note 6, pmbl.
52 Safe Harbor Overview, supra note 50.
54 See WOLF, supra note 19, at 14-27.
55 See Safe Harbor, supra note 6, annex I.
57 See WOLF, supra note 19, at 14-27. See also Safe Harbor Certification Information, supra note 53.
58 Safe Harbor, supra note 6, annex III.
The DOC tests the online privacy policies of registering Companies “to the greatest extent possible.”\textsuperscript{59} The DOC, however, admits that when a Company’s privacy policy is not readily available online, it merely “confirm[s] with the contact point that the policy is available upon request.”\textsuperscript{60} The DOC rejects approximately fifty-percent of all initial Safe Harbor applications due to deficiencies in at least one area.\textsuperscript{61}

2. The Safe Harbor Notice, Choice, Onward Transfer, Security, Data Integration, and Access Principles

The Notice Principle requires a Safe Harbor Company to “inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, [and] the types of third parties to which it discloses the information.”\textsuperscript{62} This disclosure must occur prior to using collected information and preferably before individuals are asked to provide personal information.\textsuperscript{63}

The Choice Principle requires a Safe Harbor Company to allow customers to either “opt-in” or “opt-out” of information sharing depending on the nature of the information. For highly personal information,\textsuperscript{64} the Choice Principle requires customers to affirmatively “opt-in” to information sharing with a third party. For all other types of information, a Company still must give the customer the choice to “opt-out.”

The Onward Transfer Principle requires a Safe Harbor Company to ensure that either the Safe Harbor or the Data Directive binds any “middle-man” third party agent that receives the data at issue.\textsuperscript{65} Alternatively, the Company and a “middle-man” agent may sign an agreement incorporating all of the Safe Harbor principles.\textsuperscript{66}

The Security Principle, although only one sentence in length, is critical to the Safe Harbor. It requires a Company to “take reasonable precau-

\textsuperscript{60} Id.
\textsuperscript{61} Id.
\textsuperscript{62} Safe Harbor, supra note 6, annex I.
\textsuperscript{63} Id.
\textsuperscript{64} Highly personal information is defined as “personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.” Id.
\textsuperscript{65} Id.
\textsuperscript{66} Id.
tions to protect [all data] from loss, misuse and unauthorized access, disclosure, alteration and destruction.\textsuperscript{67}

The Data Integration Principle requires a Safe Harbor Company to process data only in a manner compatible with “the purposes for which it has been collected or subsequently authorized by the individual.”\textsuperscript{68} Additionally, a Safe Harbor Company must ensure that all data collected is “reliable for its intended use, accurate, complete, and current.”\textsuperscript{69}

The Access Principle requires a Company registered with the Safe Harbor to make its files available upon request to any EU Citizen the Company has collected information about. An EU Citizen may request to view, correct and amend his or her information in the Company’s files.\textsuperscript{70} A Company may charge a reasonable fee for providing access.\textsuperscript{71} There are several exceptions to the Access Principle,\textsuperscript{72} but they are beyond the scope of this Note and will not be discussed here.

3. The Safe Harbor Enforcement Principle

For the purposes of this Note, the most important provision is the Enforcement Principle. At its basic level, the Enforcement Principle has three components: (1) a resolution system using an “independent recourse mechanism;” (2) a privacy policy verification mechanism; and (3) a guarantee to remedy.\textsuperscript{73} The first component, the “independent recourse mechanism,” must be “readily available and affordable” to a potential complainant.\textsuperscript{74} Second, a Company must have a verification mechanism that shows all privacy practice assertions are true and implemented.\textsuperscript{75} Finally, a Company must obligate itself to resolve any issues that arise from a determination made by the “independent recourse mechanism.”\textsuperscript{76}

a. The Enforcement Principle’s independent recourse mechanism requirement

The Enforcement Principle’s “independent recourse mechanism” is likely a result of EU concessions to DOC negotiators. The “independent

\textsuperscript{67} Safe Harbor, supra note 6, annex I.
\textsuperscript{68} Id.
\textsuperscript{69} Id.
\textsuperscript{70} Id.
\textsuperscript{71} Id. annex II.
\textsuperscript{72} Safe Harbor, supra note 6, annex II.
\textsuperscript{73} Id. annex I.
\textsuperscript{74} Id.
\textsuperscript{75} Id.
\textsuperscript{76} Id.
recourse mechanism” parallels other U.S. privacy laws that exclusively re-
medy violations through civil suits.\textsuperscript{77} As its name implies, an “independent
recourse mechanism” uses private-sector organizations to help Companies
“self-regulate” their data collection and uses.

The Enforcement Principle allows Companies to use one of four
types of “independent recourse mechanisms.”\textsuperscript{78} First, several private-sector
privacy programs are available which meet the Safe Harbor requirements\textsuperscript{79}
such as BBBOnline\textsuperscript{80} or TRUSTe.\textsuperscript{81} Second, a Company can commit to
cooperate with the EU member states’ Data Protection Authority.\textsuperscript{82} Third,
Companies may seek out other private sector “independent recourse me-
chanism” bodies that “meet the requirements of the Enforcement Principle
and the FAQs.”\textsuperscript{83} Finally, the Safe Harbor allows Companies to “compl[y]
with legal or regulatory supervisory authorities that provide for handling of
individual complaints and dispute resolution.”\textsuperscript{84} While at least one leading
authority on privacy law ignores this option,\textsuperscript{85} some Companies interpret
this language to include a Company’s own internal complaint process as an
“independent recourse mechanism.”\textsuperscript{86}

b. The Enforcement Principle’s Verification Requirement

The Enforcement Principle’s Verification Requirement obligates
Companies to verify that their stated privacy practices are implemented.\textsuperscript{87} A
Company registering for the Safe Harbor can verify its privacy policies in
one of two ways. The first option allows a Company to submit to annual

\begin{footnotesize}
\begin{enumerate}
\item See Bignami, supra note 26, at 684.
\item Safe Harbor, supra note 6, annex II.
\item See id.
u.asp (last visited Aug. 30, 2008) (describing BBBOnline’s self-regulatory Safe Harbor
compliance program).
\item See TRUSTe, http://www.truste.org/businesses/eu_safe_harbor_seal.php (last visited
\item Safe Harbor, supra note 6, annex II.
\item Id.
\item Id.
\item See WOLF, supra note 19, at 14-26.
\item See, e.g., Safe Harbor Registration of Adaptec, Inc., http://web.ita.doc.gov/safeharbor
/shlist.nsf/5624c34187d9c4d4ce85256960005ce648/b0893a8186c1fd0885256b7200572945?Op
enDocument (last visited Mar. 30, 2008) (listing its “independent recourse mechanism” as
“Consumer or Adaptec employee complaints will generally be escalated internally to the
Adaptec corporate legal department which will consult with management on appropriate
response or action depending on the facts at issue”). Only after going through Adaptec’s
process unsuccessfully will they refer the matter to a Data Protection Authority. This troubl-
ing interpretation is discussed in Part V of this Note. See infra Part V.B.1.b.iii.
\item Safe Harbor, supra note 6, annex II.
\end{enumerate}
\end{footnotesize}
outside compliance reviews. Additionally, the Safe Harbor suggests that Companies submit themselves to “without limitation auditing, random re-
views, [and] use of ‘decoys.’” The other option allows a Company to “self-verify.” Under this option, a Company must merely submit an annual written verification—signed by a corporate officer or authorized representa-
tive—stating that the Company’s published privacy policy is “accurate, comprehensive, prominently displayed, completely implemented and ac-
cessible.” Additionally, the “self-verification” document must list internal procedures for periodically conducting objective reviews of compliance with the Safe Harbor.

c. The Enforcement Principle’s Guarantee to Remedy Requirement

The Enforcement Principle’s Guarantee to Remedy Requirement is usually satisfied through a Company’s “independent recourse mechanism.” When a Company’s chosen “independent recourse mechanism” determines there is a violation, the Safe Harbor suggests several remedies of varying degree based on the level of the violation. At a minimum, any remedy should reverse the effects of the violation, ensure future processing complies with the Safe Harbor Principles and publish the non-compliance findings. Any “independent recourse mechanism,” however, must notify both the DOC and the governmental body with applicable jurisdiction—usually the FTC—if a Company fails to comply with the procedures and remedies demanded by its “independent recourse mechanism.” The Safe Harbor suggests “independent recourse mechanism” bodies use further sanctions, such as, stopping the processing of the complainant’s personal data, deleting the data at issue, removing an “independent recourse mechanism[’]s” privacy program seal, and compensating a complainant for any losses incurred.

The Enforcement Principle’s self-regulatory means of enforcement through an “independent recourse mechanism,” verification, and a guaran-
tee to remedy, however, is only one part of the Safe Harbor’s overall en-
forcement scheme.

---

88 Id.
89 Id.
90 Id.
91 See infra Part V.B.2 (discussing how “self-verification” is contrary to the intent of the Safe Harbor).
92 Safe Harbor, supra note 6, annex II.
93 Id.
94 Id.
95 Id.
96 See infra Part III.C.2.a (explaining the “big picture” of the Safe Harbor “layer” method of enforcement).
C. Government Data Protection Enforcement Mechanisms

1. Data Directive enforcement in the EU

The Data Directive requires enforcement solely through a government agency. Accordingly, each EU member state is required to create a Data Protection Authority. The Data Protection Authority is a government agency whose sole responsibility is to protect privacy through the enforcement of the Data Directive and other data protection laws. Some EU member states’ Data Protection Authorities require all data collectors and processors to file annual reports. For example, France’s Data Protection Authority goes so far to require data collectors and processors to be approved prior to beginning operations. The Data Protection Authorities are required to be proactive, self-initiate an investigation, and enforce possible or potential violations in data processing operations. Under the Data Directive EU Citizens must be given the right to object to their data being processed and a data processor must have an objection process that does not charge a fee. Additionally, EU Citizens can initiate private rights of action, and Data Protection Authorities give prior privacy adjudications a res judicata effect when litigating new cases.

2. Safe Harbor Enforcement in the United States

a. Safe Harbor enforcement—the big picture

Enforcement under the Safe Harbor follows a multiple “layer” approach. The Enforcement Principle only encompasses one “layer” of the Safe Harbor’s means of enforcement. The first enforcement “layer” is the initial Safe Harbor registration and subsequent annual Safe Harbor registration renewals, run by the DOC. The second “layer” is the Enforcement Principle’s “independent recourse mechanism.” The final “layer” is government intervention, usually through the FTC.

---

97 Data Directive, supra note 3, art. 28.
98 Id. art. 28(1).
99 See id. art. 28(1).
101 Wolf, supra note 19, at 14-14.
102 See Data Directive, supra note 3, art. 20. See also id. art. 28.
103 Id. art. 14.
104 Id. art. 22–24.
105 See id. art. 28(5).
106 See supra Part III.B.3.
107 See supra Part III.B.1.
108 See supra Part III.B.3.a.
To resolve a complaint, an EU Citizen should first directly contact a Company. Second, he or she could seek recourse through the Enforcement Principle by referencing the Company’s privacy policy and contacting the Company’s “independent recourse mechanism.” Finally, if a Company fails to fulfill the remedy, if any, demanded by its “independent recourse mechanism,” then the “independent recourse mechanism” must refer the matter to the U.S. governmental agency that has jurisdiction over the Company, usually the FTC. The last “layer,” U.S. agency enforcement, is discussed in the next section.

b. U.S. Agency Safe Harbor enforcement

As part of each Company’s initial registration for the Safe Harbor with the DOC, each Company must state which “[s]pecific statutory body . . . has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy.” Since the inception of the Safe Harbor, only two government agencies have assured the European Commission that they will take enforcement actions against Companies that fail to abide by their Safe Harbor commitments. The two agencies are the FTC and the Department of Transportation.

This Note will discuss the FTC’s effectiveness under the Safe Harbor in light of its broad authority to regulate any “unfair or deceptive acts or practices in or affecting commerce” under the Federal Trade Commission Act (FTC Act). In contrast, the Department of Transportation’s authority is limited to the much smaller subset of common carrier issues, and thus the Department of Transportation’s enforcement authority will not be discussed in this Note.

The FTC can only initiate action against companies that have first made a representation. Therefore, as previously discussed, A Company’s Safe Harbor registration acts as an affirmative representation by a

109 See Safe Harbor, supra note 6, annex II.
110 Safe Harbor Certification Information, supra note 53.
111 See Safe Harbor Overview, supra note 50.
112 Safe Harbor, supra note 6, annex VII.
115 See Safe Harbor, supra note 6, annex III. (“[T]he Federal Trade Commission … [can only] take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments.”) (emphasis added).
116 See supra Part III.B.1.
Company, similar to an affidavit. If a Company fails to comply with its Safe Harbor commitment, then the FTC has the power to prosecute the false representation as a deceptive action.

The FTC can seek several types of remedies on behalf of consumers. After conducting a formal hearing, the FTC may issue a cease and desist order, seek restraining orders or injunctions, and—in more severe cases—may promulgate an administrative rule barring an act or practice as per se unfair or deceptive. The FTC may fine a Company up to $10,000 for each failure to comply with a FTC order or for violating a FTC rule.

IV. THE GOOGLE-DOUBLE CLICK MERGER: A CASE STUDY IN THE EUROPEAN UNION’S DETERIORATING TRUST IN THE U.S. PRIVACY REGULATORY SCHEME

EU member states and their citizens are forced to rely on Safe Harbor enforcement “layer” entities that are outside the realm of EU political control. Neither the “independent recourse mechanisms” nor U.S. agencies, such as the FTC, have any incentive to pursue Safe Harbor violation claims because both “independent recourse mechanisms” and the FTC are unaccountable to EU Citizens. It is as if the EU decided to rely on an unpaid mercenary force to protect its data “borders” with the U.S. Therefore, EU Citizens have no choice but to rely on Safe Harbor enforcement bodies that are politically unaccountable to them, have little incentive to pursue claims, and have taken little action over the seven-year period since the Safe Harbor’s inception.

This is not a small problem. In 2004, the U.S. and its top six European trade partners traded approximately $400 billion in goods and services. It is likely that Companies hold some of EU Citizens’ most vulnerable data, yet that data resides where there is poor enforcement, and little in-

---

117 See Wolf, supra note 19, at 14-27. See also Safe Harbor Certification Information, supra note 53.
118 See Safe Harbor, supra note 6, annex III.
124 See infra Part V.
126 The Safe Harbor program includes the registration of over 1600 companies. Safe Harbor List, supra note 51. The business sectors of those companies include market research firms, such as Harris Interactive Inc., and large internet retailers, such as Amazon.com, Inc. Id. (follow links to specific companies listed alphabetically).
centive to invest in protecting the data.\textsuperscript{127} Many EU Citizens question the effectiveness of the U.S. self-regulatory model of privacy regulation and enforcement. The deteriorating trust makes it all the more important for citizens of EU member states to have their confidence reassured by strengthened Safe Harbor enforcement mechanisms.\textsuperscript{128} This section explores the different approaches used by the EU Commission on Competition and FTC Bureau of Competition for regulating Google’s acquisition of DoubleClick, an online advertising company. This example demonstrates the EU’s fading confidence in the U.S. self-regulatory model of privacy regulation and enforcement.\textsuperscript{129}

\textbf{A. Google’s Significant Collected Data}

In August, 2007, 210 million individuals in Europe made 18 billion search requests on the Google search engine.\textsuperscript{130} Google “obsessively files away most every scrap of data it receives,”\textsuperscript{131} but Google recently enacted a policy to “remov[e] identifying data from its search logs after 18 months to two years” and that after eighteen months, the information it collects does not include the personal identity of a user.\textsuperscript{132} While this is technically true, with an average of 86 search inquiries per European citizen in August of 2007 it is not difficult to put separate search patterns together to identify a unique individual.\textsuperscript{133} The longer Google retains data on a person, the more “complete” a picture both Google, and potential data thieves, have about a

\textsuperscript{127} See infra Part V.

\textsuperscript{128} See id.

\textsuperscript{129} Notice that some of the issues raised by the EU over Google’s policies involve additional EU privacy directives that were passed subsequent to the Data Directive. This Note does not discuss the specific legal sections or arguments because they are beyond the scope of this Note.


\textsuperscript{133} For example, the same person may make the following searches: “Fish and chips in Cotswolds,” “Ancestry of sir name Clarkson,” “Ferrari F430,” “Chipping Norton noise pollution laws.” Alone, the searches may mean little. Together, they can pinpoint a specific person, in this case, Jeremy Clarkson, a presenter on BBC Two’s “Top Gear” television program.
person. Google’s goal in retaining consumer data is simple: to gain a unique understanding of its users to target advertising.134

B. Initial European Union Concerns with Google’s Data Retention Practices

As early as April, 2004, the EU began to raise concerns over Google’s data retention practices.135 In May, 2007, the Article 29 Working Party136 sent an official letter137 to Google, asking for an explanation of why it keeps user data for two full years.138 In June 2007, Peter Fleischer, Google’s Chief Privacy Counsel, responded that Google would reduce its data retention to eighteen months.139 Mr. Fleischer argued that data retention serves as an “important tool for law enforcement to investigate and prosecute many serious crimes, such as child exploitation” and he “firmly reject[ed] any suggestions that [Google] could meet [its] legitimate interests in security, innovation and anti-fraud efforts with any retention period shorter than 18 months.”140 Some observers believe that Google is using law enforcement and national security concerns as a cover-up for its actual intentions of targeting advertising.141 In an October 2007 reply, the Article 29 Working Party acknowledged that that Mr. Fleischer had “raised several issues about processing [] personal data” with regard to search engines and that the group would release an opinion on these issues “in early 2008.”142

134 See Posting of Saul Hansell, supra note 131.
136 This group, created by Data Directive article 29, is composed of national officials that advise the EU on privacy policy. Data Directive, supra note 3, art. 29.
140 Id.
C. The Google-DoubleClick Merger

In April 2007, Google bought the online advertising firm DoubleClick for $3.1 billion dollars, its largest acquisition to date. Google and DoubleClick both advertise online, but with slightly different specialties. Google’s advertising division, AdSense, helps display advertising directly on a website, which generates revenue for the website owners. Google crawls the content of the page on which the ad is to be displayed, and AdSense generates advertising for various companies that the website’s visitors would likely be interested in. DoubleClick, however, supplies various advertisers and website publishers with elaborate plans for the delivery, management and reporting of web-displayed ads. It uses “Web surfers’ interaction with ads to determine how to place the most effective display ads.” DoubleClick’s approach to advertising is called “behavioral advertising.” The primary difference is that Google’s AdSense ads are usually text only and relate to the contents of the page on which the ads appear; DoubleClick’s advertisements, in contrast, are usually large image or video banners and are directed to an audience based on prior user viewing habits.

1. The Federal Trade Commission investigation

The Google purchase of DoubleClick raised the ire of several privacy groups because “DoubleClick and Google [could] combine some of their huge databases of information on Internet use.” On April 20, 2007, three privacy advocacy groups—the Electronic Privacy Information Center, the Center for Digital Democracy, and the U.S. Public Interest Research Group—filed a joint complaint with the FTC alleging that the merger would

---

143 Louise Story, Google Buys an Online Ad Firm for $3.1 Billion, N.Y. TIMES, Apr. 14, 2007, at C1.
144 This is a term for when a search engine visits a website and creates a “snapshot” of website’s content.
147 Story, supra note 143.
148 Id.
149 Id.
150 Id. (“You can dive deep into that data and say who were those people, where do they live, what were they doing when they looked at those ads?”).
give Google access “to more information about the Internet activities of consumers than any other company in the world.”

Despite the privacy groups’ concerns, mergers and acquisitions are evaluated under anti-trust law. Both the FTC Bureau of Competition and the Department of Justice can review anti-trust allegations. The FTC Bureau of Competition was selected to review the Google-DoubleClick merger in late May 2007. This was a significant and favorable development for the privacy groups because although “[c]onsumer protection issues are not considered as factors in whether the Department of Justice or the FTC Bureau of Competition is chosen to review a merger,” once the FTC Bureau of Competition is selected, it can take account of possible violations of section five of the FTC Act.

Adding to the controversy, politicians and a newspaper editorial raised privacy concerns about the merger. On June 13, 2007, the New York Times featured an editorial calling on the FTC to address the privacy implications of the merger, in addition to the anti-trust implications. The editorial stated that “[p]rivacy is too important to leave up to the companies that benefit financially from collecting and retaining data.” The editorial forewarned that Google's acquisition of DoubleClick could mean that the post-merger Google “could track more sensitive information—like what diseases users have, or what political causes they support.”

In September 2007, during a U.S. Senate Judiciary Committee meeting on the merger, Senator Herbert Kohl stated that he believes the Committee should consider the privacy implications of the merger, in opposition the beliefs of some anti-trust regulators. Sen. Kohl continued, say-

---

151 Complaint and Request for Injunction, Request for Investigation and for Other Relief, Google, Inc. and DoubleClick, Inc. (FTC 2007), http://epic.org/privacy/ftc/google/epic_complaint.pdf. The groups subsequently filed supplements in June and September. Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, Google, Inc. and DoubleClick, Inc. (FTC 2007), http://epic.org/privacy/ftc/google/supp_060607.pdf; Second Filing of Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, Google, Inc. and DoubleClick, Inc. (FTC 2007), http://epic.org/privacy/ftc/google/supp2_091707.pdf.


155 Id.

156 Id.

ing that the anti-trust laws were written for the purpose of limiting “undue concentrations of economic power for our society as a whole, and not just merely their effects on consumers’ pocketbooks.” At the same meeting, Senator Patrick Leahy supplemented the statements of Sen. Kohl. Sen. Leahy said that “Most online users are unaware of how and when information about their online activity is being used,” and companies that collect personal data “have an obligation to safeguard such data.”

Google responded to the concerns of politicians and privacy groups at the same U.S. Senate Judiciary Committee meeting. David Drummond, Google’s Senior Vice President for Corporate Development and Chief Legal Officer, spoke on Google’s behalf. In his testimony, Mr. Drummond argued that competition is what keeps Google’s privacy practices in line, stating that “[u]ser interests effectively regulate our behavior.” Google subsequently published several documents on its public policy blog, including talking points on the merger and quotes from various sources that have commented positively about Google’s acquisition of DoubleClick.

During the FTC Bureau of Competition’s investigation of the Google-DoubleClick merger, an officer in the FTC Bureau of Competition itself became a target of the same privacy groups that filed the original complaint. On December 12, 2007, the privacy groups called for FTC Chairperson Deborah Platt Majoras to recuse herself because her husband, John Majoras, works as a partner in the anti-trust section of the Jones Day law firm—a firm that represents DoubleClick in international mat-

158 Id.
159 Id. (statement of Sen. Patrick Leahy).
160 Id. (statement of David Drummond, Senior Vice President of Corporate Development and Chief Legal Officer, Google).
Ms. Majoras nevertheless refused to recuse herself, stating that her husband has no financial interest in the outcome of the merger regulator decision because he is no longer an equity partner at Jones Day, and therefore she has no conflict of interest.\textsuperscript{166}

On December 21, 2007, the FTC Bureau of Competition approved the merger of Google and DoubleClick, without condition, in a 4–1 opinion.\textsuperscript{167} The FTC Bureau of Competition ignored privacy concerns, stating that Google is only a small part of the online advertising world and privacy issues “extend to the entire online advertising marketplace.”\textsuperscript{168} The majority opinion of the FTC Bureau of Competition stated that it “lack[ed] legal authority to require conditions to this merger that do not relate to antitrust, [and] regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry.”\textsuperscript{169} The decision lacked any substantive analysis of the privacy issues at stake, and in three short sentences dismissed all privacy concerns:

We investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as consumer privacy. We have concluded that the evidence does not support a conclusion that it would do so. We have therefore concluded that privacy considerations, as such, do not provide a basis to challenge this transaction.\textsuperscript{170}

FTC Commissioner Jon Leibowitz issued a concurring statement that addressed the privacy concerns more directly.\textsuperscript{171} Mr. Leibowitz stated that “industry participants must stop being coy and start being more forthcoming about their practices, the consumer information they collect, and how they

\textsuperscript{169} Id.
\textsuperscript{170} Id. at 2–3.
use it.”\footnote{Id at 2.} Mr. Leibowitz recommended two actions. First, he said that the FTC should use its power to subpoena information from Companies that have large troves of data when they are not forthcoming with how they use the data.\footnote{See id. at 2 n.3.} Second, the FTC should require that consumers must “opt-in” to receive targeted advertising.\footnote{See id. at 3.}

FTC Commissioner Pamela Jones Harbour was the lone dissent. Ms. Harbour stated that the FTC Bureau of Competition closed its investigation too soon to address all competition and privacy issues.\footnote{\textit{Fed. Trade Comm’n, FTC File No. 071-0170, Dissenting Statement of Commissioner Pamela Harbour in the Matter of Google/DoubleClick}, http://www.ftc.gov/os/caselist/0710170/071220harbour.pdf (last visited Mar. 30, 2008) (“If the Commission closes its investigation at this time, without imposing any conditions on the merger, neither the competition nor the privacy interests of consumers will have been adequately addressed.”).} She condemned the FTC’s failure to follow its dual role for protecting against both consumer violations and anti-trust violations. She stated that “the Commission could have utilized the full scope of its statutory powers to ensure competition was not harmed, while also addressing the privacy issues.”\footnote{Id. at 13.}

Commissioner Harbour directly addressed the privacy advocates’ concerns and stated that she was “uncomfortable accepting the merging parties nonbinding representations at face value. . . . The merger creates a firm with vast knowledge of consumer preferences, subject to very little accountability.”\footnote{Id. at 9–10 (emphasis added).} She added that there is a “disconnect between the financial incentives of advertisers and publishers (i.e., to exploit data) and the privacy incentives of some consumers (i.e., to protect data).”\footnote{Id. at 11–12.} Finally, Commissioner Harbour suggested that the U.S. Congress should consider “whether comprehensive privacy legislation (including, but not limited to, behavioral advertising) is needed.”\footnote{Id. at 12.}

Google and its opponents reacted as expected. Google hailed the ruling stating that it “firmly believe[s] the transaction will increase competition and bring substantial benefits to consumers, web publishers, and online advertisers.”\footnote{Posting of David Drummond to Google Public Policy Blog, \textit{Analysis: The FTC Clears Our Acquisition of DoubleClick}, http://googlepublicpolicy.blogspot.com/2007/12/analysis-ftc-clears-our-acquisition-of.html (Dec. 20, 2007, 13:49 PST).} The Electronic Privacy Information Center condemned the ruling, stating it was a mistake for the Commissioners “to ignore the privacy
implications of the Google-DoubleClick merger and to propose instead the same self-regulatory approach to privacy protection that has repeatedly failed American consumers.  

2. European Union Investigation

Google also had to pass an investigation by the EU Commission on Competition to complete its acquisition of DoubleClick. On September 21, 2007, Google applied to the EU Commission on Competition for permission to merge with DoubleClick. Yet before receiving Google’s official application, the EU Commission on Competition took the “unusual step of sending questionnaires to Google customers before the company officially” sought permission to acquire DoubleClick.

Early in the EU Commission on Competition’s investigation, Google’s chances of acquiring DoubleClick appeared grim. In June 2007, long before Google filed its merger application, a European consumer group, BEUC, petitioned the Commission to prevent the merger. Later, in late September 2007, the Data Protection Commissioner of the German federal state of Schleswig-Holstein sent a letter, to the EU Commission on Competition recommending the agency reject the merger. In the letter, the German Data Protection Commissioner stated that it had to assume that in the event of a takeover of DoubleClick the databases of that company will be integrated into those of Google, with the result that fundamental provisions of the European Data Protection Directive will be violated. The German Data Protection Commissioner also stated that if the merger occurred, a wealth of user data and detailed individual profiles would be created without the knowledge of the individuals concerned, and individuals

---

185 Schreiben des Leiters des ULD Dr. Thilo Weichert an die Kommissarin der Europäischen Kommission Neelie Kroes zum Wettbewerbsverfahren wenn der Übernahme des Internet Werbemarkters DoubleClick durch Google [Letter from Dr. Thilo Weichert, the Head of the ULD, to Commissioner Neelie Kroes, European Commissioner] (Sept. 26, 2007), https://www.datenschutzzentrum.de/suchmaschinen/20070926-doubleclick-google.html.
186 Id.
would be without the ability to assert their rights. Finally, the German Data Protection Commissioner stated that it was of no significance that both Google and DoubleClick are members of the Safe Harbor because the merging of data and the evaluation and the use of personalized advertising takes place in the U.S., and data merging is specifically against the European data protection directive.

Google fought back in October 2007 by promising to “keep certain DoubleClick business practices unchanged,” meaning that Google would segregate its own AdSense advertising division from the newly acquired DoubleClick. The EU Commission on Competition announced on November 13, 2007 that it would prefer to have the issue debated further and opened an in-depth investigation, postponing a decision to April 2, 2008. Nevertheless, Google remained confident following its merger approval in the U.S. and hoped that the EU Commission on Competition would follow suit.

On March 11, 2008, the EU Commission on Competition approved the Google-DoubleClick merger. Similar to the FTC Bureau of Competition’s anti-trust analysis, the EU Commission on Competition did not evaluate or take into account the privacy implications of the merger. The

---

187 Id.


189 Letter from Dr. Thilo Weichert, supra note 185.


195 See Associated Press, Europe Clears Google DoubleClick Bid, N.Y. TIMES, Mar. 11, 2007, http://www.nytimes.com/2008/03/11/technology/apre-google.html (“Regulators said their decision was based exclusively on the economic aspects of the deal and it had no bear-
European Commission on Competition stated that the “decision to clear the proposed merger is based exclusively on its appraisal under the EU Merger Regulation.”\textsuperscript{196} The European Commission on Competition stressed that its decision was “without prejudice to the merged entity’s obligations under EU legislation in relation to the protection of individuals and the protection of privacy with regard to the processing of personal data.”\textsuperscript{197}

D. Future EU Regulation of Google, Search Engines, and Behavioral Advertising

Although Google cleared all anti-trust regulatory bodies in the U.S. and Europe, Google still will face other EU governmental bodies that will continue to scrutinize its privacy practices, now that it has acquiredDoubleClick. For example, on January 21, 2008, the European Parliament conducted a formal hearing entitled “Data protection on the Internet” that primarily focused on the proposed Google-DoubleClick merger.\textsuperscript{198} Interestingly, Ms. Pamela Harbour, the lone dissent in the FTC Bureau of Competition’s ruling on the Google-DoubleClick merger,\textsuperscript{199} testified on behalf of the FTC at the European Parliament hearing.\textsuperscript{200} At the hearing, Peter Schaar, head of Germany’s Data Protection Authority, made the significant assertion that internet protocol addresses (IP addresses)\textsuperscript{201} should be treated as personal information.\textsuperscript{202} If later EU interpretations of the Data Directive hold that IP addresses are personal information, it would mean that Google,ing on the companies’ obligations under E.U. personal privacy protection rules or how personal data is processed.”).  

\footnotesize{\textsuperscript{196} Press Release, European Commission on Competition, supra note 194.  
\textsuperscript{197} Id.  
\textsuperscript{199} FED. TRADE COMM’N, supra note 175.  
\textsuperscript{200} European Parliament, Google-DoubleClick entire hearing program, supra note 198.  
\textsuperscript{201} An IP address is a unique number that identifies each computer on the internet. An IP address can reveal the city and country a person is physically located in and which internet service provider a person is using. Posting of Saul Hansell to N.Y. Times Bits Blog, Europe: Your I.P. Address Is Personal, http://bits.blogs.nytimes.com/2008/01/22/europe-your-ip-address-is-personal/ (Jan. 22, 2008, 15:31 EST).  
\textsuperscript{202} Aoife White, IP Addresses Are Personal Data, E.U. Regulator Says, WASH. POST, Jan. 22, 2008, at D1.}
along with all other search engines and online providers, would have to comply with Data Directive before collecting data on web surfing habits. Google argues that IP addresses are not personally identifiable information because IP addresses only identify a computer and not the person using it. The Article 29 Working Party expects to release a report in April 2008 on the application of the Data Directive to search engine data retention and targeted advertising, resolving the issue over IP addresses. The report will refine a November 2006 resolution, passed at a conference of Data Protection Authorities, which briefly analyzed the privacy issues of search engines and behavioral advertising.

E. Significance of European Union and Federal Trade Commission Differences

The EU applied a much higher level of scrutiny when reviewing the Google-DoubleClick merger. The EU Commission on Competition initiated a longer and more in-depth investigation than the FTC Bureau of Competition’s investigation, after early public attention. Google knew that the EU Commission on Competition investigation would be more in-depth than the FTC Bureau of Competition’s investigation, and it therefore made concessions early in the investigation. Although the EU Commission on Competition approved the merger under EU anti-trust law, it stated that other EU bodies, such as the Article 29 Working Party would continue to

---


208 See Letter from Dr. Thilo Weichert, supra note 185.

209 See Victoria Shannon, Europe Delays Google Deal for DoubleClick, N.Y. TIMES, Nov. 14, 2007, at C7 (stating that Google would “keep certain DoubleClick business practices unchanged”).

210 Press Release, European Commission on Competition, supra note 194.
review Google’s privacy practices.\textsuperscript{211} The FTC Bureau of Competition’s majority ruling on the Google-DoubleClick merger, however, ignored all privacy concerns raised by various parties and failed to ensure that the FTC Bureau of Consumer Protection would continue to closely watch Google’s practices that impact privacy.\textsuperscript{212}

V. SAFE HARBOR ENFORCEMENT LIMITATIONS AND PROPOSED SOLUTIONS

As previously discussed, the Data Directive relies entirely on government enforcement mechanisms, whereas the Safe Harbor has a multiple “layer” approach, incorporating primarily private-sector enforcement with governmental action as a means of last resort.\textsuperscript{213} The Safe Harbor’s “layered” approach seems, on its face, to give more protection. This section seeks to counter this impression by showing that a multiple “layer” approach is both less efficient and counter to the objective of protecting privacy.

A. Initial Registration Oversight by the U.S. Department of Commerce

1. Safe Harbor Registration Processing Limitations

a. Problem

As previously discussed, EU member states and the DOC use vastly different pre-operation methods of enforcement.\textsuperscript{214} Some EU member states take a pro-active approach to enforcement. For example, France’s Data Protection Authority limits all data operations of a company or organization until it gives explicit approval that all of the Data Directive’s requirements are met.\textsuperscript{215} The U.S. pre-operation enforcement arm for the Safe Harbor, the DOC,\textsuperscript{216} however, does not rigorously enforce Safe Harbor registrations. A leading privacy treatise states that the DOC role is only to approve applications\textsuperscript{217} without any scrutiny.\textsuperscript{218} Similarly, a 2004 EU commission found

\textsuperscript{211} Europe Clears Google DoubleClick Bid, supra note 195 (“Regulators said their decision was based exclusively on the economic aspects of the deal and it had no bearing on the companies’ obligations under E.U. personal privacy protection rules or how personal data is processed. European privacy regulators are now examining if the data protection policies of search engines comply with existing E.U. law.”).

\textsuperscript{212} Press Release, Marc Rotenberg, supra note 181.

\textsuperscript{213} See supra Part III.C.2.a.

\textsuperscript{214} See supra Part III.C.

\textsuperscript{215} WOLF, supra note 19, at 14-14.

\textsuperscript{216} See supra Part III.B.1.

\textsuperscript{217} Safe Harbor Certification Information, DEPARTMENT OF COMMERCE, http://www.export.gov/safeharbor/SH_Cert_Info.asp (lists the requisite information to fill-out the online certification form).
that the DOC failed to properly oversee Safe Harbor registrations because a “substantial minority” of Companies the DOC certified for the Safe Harbor did not have “visible” privacy policies.\textsuperscript{219} The DOC rejected these criticisms and has stated that it tests the online privacy policies of Companies “to the greatest extent possible.”\textsuperscript{220} The Department admits, though, that when a Company’s privacy policy is not readily available online it merely “confirm[s] with the contact point that the policy is available upon request.”\textsuperscript{221} The DOC insists that its review is so rigorous that it eventually rejects approximately fifty-percent of all initial Safe Harbor applications due to deficiencies in at least one area.\textsuperscript{222} The rejection figure, however, may be due to very mundane deficiencies, such as failure include a Company officer’s fax number.\textsuperscript{223}

The Safe Harbor’s failure to include any formal process for application review is surprising. The Safe Harbor, therefore, does not even require the U.S. DOC to verify the existence of a Company’s privacy policies. This is of great concern because it means that the FTC does not have the power to punish websites that fail to publish required privacy statements.\textsuperscript{224} Courts have interpreted that a failure to make a statement is not within the FTC Act’s bar on deceptive practices.\textsuperscript{225}

b. Proposed Solution

If the DOC’s review process is as rigorous as it claims to be, then it should use methods that are more transparent to EU Citizens—the people the Safe Harbor purports to protect. This should involve a publicly disclosed Safe Harbor acceptance review procedure that details, at a minimum, how privacy policies are verified. Currently, if a Company’s privacy policy is not readily available online, the DOC merely “confirm[s] with the contact point that the policy is available upon request.”\textsuperscript{226} The DOC should demand that

\begin{itemize}
\item \textsuperscript{218} WOLF, supra note 19, at 14-28 (“[The] safe harbor’s [has] a self-certification system without mandatory independent verification of what a business actually does”).
\item \textsuperscript{219} See EU Safe Harbor Criticism, supra note 8, at 6–7.
\item \textsuperscript{220} U.S.-EU Safe Harbor Framework PowerPoint, supra note 59, notes accompanying slide 10.
\item \textsuperscript{221} Id.
\item \textsuperscript{222} Id.
\item \textsuperscript{223} See Safe Harbor Certification Information, supra note 53 (listing the requisite information to fill-out the online certification form).
\item \textsuperscript{224} Pedersen, supra note 9, at 10.
\item \textsuperscript{225} See Safe Harbor, supra note 6, annex III (“[T]he Federal Trade Commission . . . [can only] take action against those who fail to protect the privacy of personal information in accordance with their representations and/or commitments.”) (emphasis added).
\item \textsuperscript{226} U.S.-EU Safe Harbor Framework PowerPoint, supra note 59, notes accompanying slide 10.
\end{itemize}
any Company’s privacy policy be readily available online and require a Company to demonstrate how it would handle a privacy complaint.

c. Difficulties with Proposed Solution

The first roadblock to a more formal Safe Harbor review process may be the Safe Harbor itself. Companies will probably be unwilling to open up their files for verification of compliance by a government body without a clear legal requirement to do so, which the Safe Harbor lacks. This problem is a running theme in this Note’s proposed solutions. Even if the DOC made a goodwill gesture and invoked more procedures to fulfill the spirit of the Data Directive—and even if those changes were made at the request of EU member states and their Data Protection Authorities—the DOC it has no legal basis to make a change. All that is legally required is outlined in the Safe Harbor.

The only way for EU member states to create a legal requirement for change is for the EU to directly reverse itself and find that the current Safe Harbor protections are not adequate. Only then could EU member states force U.S. agencies back to the negotiating table to enact greater enforcement protections. Nevertheless, an EU reversal regarding the adequacy of the Safe Harbor protections would be a significant revocation that would likely harm any later negotiations.

The second roadblock to a more formal Safe Harbor review process is the budget for DOC. The DOC devotes only twenty minutes to review each online Safe Harbor application and forty minutes for each paper application. Additionally, the DOC will only commit 550 hours annually to the Safe Harbor. The DOC has only allotted itself $190,250 annually for the entire Safe Harbor program.

2. Few Safe Harbor registrants

a. Problem

The DOC must also overcome the lack of Safe Harbor registrants. Initially, the DOC estimated 1,500 Companies would register annually; however, after more than seven years, the Safe Harbor program currently has only 1,300 Companies, of which approximately one-fifth have failed to

\[228\] Id.
\[229\] Id. The Federal Register has a typo that indicates the dollar amount as “$19,0250,” which should read “$190,250.”
\[230\] Id.
complete the required annual re-certification. These “numbers are insignificant and a poor return for the effort that was put into establishing the Safe Harbor framework.” A 2004 EU commission on the Safe Harbor similarly found that the “number of registered [Safe Harbor] organisations is lower than initially anticipated and this is a cause of disappointment.” In March 2005, the DOC attempted to resolve the lack of registrants by lowering the Safe Harbor registration fee from between $150–500 annually, based on annual revenue, to only $50 across the board. Such a small cost, however, was likely not a barrier for any multi-million or multi-billion dollar Company.

b. Proposed solution

The DOC should eliminate all Safe Harbor registration fees and further educate Companies that registering for the Safe Harbor can limit a Company’s liability. The DOC is heading in the right direction and recently completed a two-day information session for Companies on the various methods of complying with the Data Directive, including the Safe Harbor. Unfortunately, the event was limited to only 150 attendees and most of the presentations on the Safe Harbor only described the basic registration requirements and failed to highlight the benefits of the Safe Harbor. One of the presenters at the conference—Ms. Joan Antokol, a partner at the Baker & Daniels law firm—specifically highlighted where the DOC should focus its efforts in the future.

Ms. Antokol stated that most companies do not register for the Safe Harbor because there is: (1) a lack of perceived need; (2) hesitation by Company in-house counsel; (3) a lack of

---

231 The list is available online. Safe Harbor List, supra note 51.
232 Pedersen, supra note 9, at 1.
233 EU Safe Harbor Criticism, supra note 8, at 5.
237 Id.
awareness about where to begin; and (4) little or no awareness of the benefits of the program.\footnote{Id.}

B. The Enforcement Principle

There are several problems with the Enforcement Principle’s self-regulatory approach. This section discusses the problems with the Enforcement Principle’s “independent recourse mechanism” and verification requirements. This section concludes that the only viable solution is to eliminate the self-regulatory Enforcement Principle requirements because privacy self-regulation is counter to the goal of protecting privacy.

1. Criticisms of the Enforcement Principle’s independent recourse mechanism and the Guarantee to Remedy requirements

a. Lack of statutory commands

The Enforcement Principle’s “independent recourse mechanism” requirement\footnote{See supra Part III.B.3.a.} allows for an arbitrary level of sanctions because it lacks any traditional statutory language commands. Although the Safe Harbor seems to specify a strict “base” level of remedy, the language of the Safe Harbor is largely suggestive and not obligatory. For example, the Safe Harbor Enforcement Principle states that an “independent recourse mechanism” “should” reverse or correct the effects of non-compliance “in so far as feasible,” and then, “where appropriate, the processing of the personal data of the individual who has brought the complaint will cease.”\footnote{Safe Harbor, supra note 6, annex II (emphasis added).} The Safe Harbor section on “independent recourse mechanisms” goes on to suggest what other sanctions a recourse body “could” include.\footnote{Id. (emphasis added.).}

Similar to the Enforcement Principle’s “independent recourse mechanism,” the Enforcement Principle’s guarantee to remedy requirement\footnote{See supra Part III.B.3.c.} has only one line with traditional statutory language that includes words such as “must” or “shall.” The Enforcement Principle’s guarantee to remedy requirement states that any “independent recourse mechanism” “must” notify both the DOC and the governmental body with applicable jurisdiction if a Company fails to comply with the procedures and remedies demanded by the “independent recourse mechanism.”\footnote{Safe Harbor, supra note 6, annex II (emphasis added.).} The “must” commandment, however, may never become an issue because an “independent recourse mechanism” is not required to impose any level of sanction to begin with.
Therefore, if an “independent recourse mechanism” does not sanction a Company, then an “independent recourse mechanism” never “must” refer the company to any U.S. regulatory agency for non-compliance. The Enforcement Principle, therefore, gives the “independent recourse mechanism” infinite discretion, and hence the Enforcement Principle’s guarantee to remedy is ineffective. Thus, Companies have an incentive to search for an “independent recourse mechanism” that, in the event of a violation, would give the lightest sanctions or no sanctions at all.

b. Types of Independent Recourse Mechanisms

As discussed, the Enforcement Principle’s “independent recourse mechanism” requirement may be fulfilled in one of four ways.246 The following criticisms address the methods of fulfilling the “independent recourse mechanism” requirement.

i. Private-sector privacy programs

First, the Enforcement Principle’s “independent recourse mechanism” requirement allows Companies to use private-sector privacy programs.247 Private-sector privacy programs, such as TRUSTe248 and BBBOnline,249 are organizations that assist Companies create and implement privacy policies. Private-sector privacy programs can be ineffective, though, because the Safe Harbor, as just discussed, has no requisite level of sanctions.250 Companies are free to shop around for private-sector privacy programs that have a history of lenient enforcement. For example, BBBOnline has forty-five Companies registered with its Safe Harbor compliance program.251 The BBBOnline program has large Company participants with data that may be particularly sensitive, such as Careerbuilder.com, which has data on work histories and resumes, and Amazon.com, which has data on purchase histories and credit card payments.252 The BBBOnline has no set rules for sanctions.253 If a Company were to either fail to publish its privacy policy or fail to fulfill its privacy policy, then under the BBBOnline program, a Company has the option of “propos[ing] alternative corrective ac-

246 See supra Part III.B.3.a.
247 Safe Harbor, supra note 6, annex II.
250 See supra Part V.B.1.a.
252 See id.
253 BBBONLINE, SAFE HARBOR PRIVACY DISPUTE RESOLUTION PROCEDURE, § 3.3.1 (Apr. 9, 2003), http://www.bbbonline.org/privacy/DataPrivacyDRRules.pdf.
tion with regard to its privacy policies or practices to remedy the noncompliance.\textsuperscript{254} Additionally, the entire process can take up to six months before BBBOnline reports a violation to a government enforcement agency.\textsuperscript{255}

In 2004, an EU commission on the Safe Harbor raised similar concerns about private-sector privacy programs serving as a Company’s “independent recourse mechanism.” The EU commission on the Safe Harbor found that private-sector privacy programs “do not seem to foresee ways to remedy situations of failure to abide by the Principles.”\textsuperscript{256}

ii. Vague independent recourse mechanisms

Second, the Enforcement Principle’s “independent recourse mechanism” requirement allows Companies to employ other private-sector “independent recourse mechanisms” so long as the “independent recourse mechanisms” “meet the requirements of the Enforcement Principle and the FAQs.”\textsuperscript{257} A new trend is developing in this area, whereby recent Safe Harbor applications of various Companies list arbitration associations as their chosen “independent recourse mechanism.” In a random sampling of fifty of the Safe Harbor Companies, four large Companies—Hard Rock Cafe International, ConAgra Foods, Eastman Kodak Company, and Electronic Arts—list arbitration associations as the Company’s “independent recourse mechanism.”\textsuperscript{258} This is extremely disturbing because arbitrators in the U.S. are under no requirement to follow the letter of the law.\textsuperscript{259} The fact that arbitrators do not have to rule after considering and applying the law bars arbitra-

\textsuperscript{254} \textit{Id.}

\textsuperscript{255} \textit{See id. This is a maximum, but perfectly acceptable both by the Safe Harbor Agreement and the BBBOnline procedure terms. This total was calculated by adding the time a company has to respond to a complaint (§ 3.2.2, 15 business days), the complainant reply process (§ 3.2.4, 10 business days), the response to a reply process (§ 3.2.5, 10 business days), the request for additional information process (§ 3.2.6, 10 business days), the initial decision process (§ 3.3, 20 business days), a request for appeal (§ 4.2.1, 15 business days), a response to the appeal (§ 4.2.4, 10 business days), an appeal decision (§ 4.7.1, 20 business days), a respondent’s statement to add to the appeal decision (§ 4.7.2, 10 business days), the verification of performance process (§ 5, 30 days), and a ten-day warning period (§ 1.12). \textit{Id.}}

\textsuperscript{256} \textit{EU Safe Harbor Criticism, supra note 8, at 11.}

\textsuperscript{257} \textit{Safe Harbor, supra note 6, annex II.}

\textsuperscript{258} \textit{See Safe Harbor List, supra note 51.}

\textsuperscript{259} Arbitrations over Safe Harbor disagreements would necessarily be international in scope. International law is solely under the jurisdiction of the U.S. federal government, and therefore any arbitration stemming from a Safe Harbor disagreement would fall under the Federal Arbitration Act. Act of Feb. 12, 1925, ch. 213, 43 Stat. 883 (codified at 19 U.S.C. §§ 1-4 (1994)). Arbitrators under the Federal Arbitration Act are not required to rule based on any law. 3 JAN R. MACNEIL ET AL., FEDERAL ARBITRATION LAW § 37.4.1, at 37:10 (1999) (stating that arbitrators have no obligation under the Federal Arbitration Act “to make findings of fact or conclusions of law, or otherwise to give reasons for their awards”).}
2009] EU-U.S. DATA PRIVACY SAFE HARBOR

In addition, arbitration associations have a strong economic incentive to rule in favor of Companies that provide their work. For example, Mr. Richard Neely, a retired West Virginia Supreme Court chief justice, said that arbitration associations ask for

substantial costs related to the arbitration itself. . . . In one case that I handled, the fees alone amounted to $450. Furthermore, the arbitration company sends the arbitrator a judgment form already filled out so that all the arbitrator need do is check the appropriate box. . . . In my case I did not award the [defendant company] the litigation-related fees. . . . I never got another case! 261

Finally, the Safe Harbor explicitly requires any “independent recourse mechanism” be “readily available, and affordable” to a potential complainant. 262 Arbitration fees can be costly, 263 and neither Hard Rock Cafe International, ConAgra Foods, Eastman Kodak Company, nor Electronic Arts state in their Safe Harbor registrations that they will pay the arbitration fees on behalf of a complainant. 264 Therefore, even if arbitration associations were an acceptable “independent recourse mechanism,” Companies still would have to pay the vast majority of arbitration fees to make complaints “affordable” to an EU Citizen. 265

A 2004 EU commission on the Safe Harbor raised similar concerns about arbitration associations serving as a Company’s “independent recourse mechanism.” The 2004 EU commission on the Safe Harbor stated that arbitration associations “lack transparency insofar as they operate without properly informing individuals as to how the dispute resolution procedure works to file a complaint for alleged failure to abide by the Principles.” 266

iii. Nonexistent independent recourse mechanisms

Third, the Enforcement Principle’s “independent recourse mechanism” requirement allows Companies to use “compliance with legal or regu-

260 See Safe Harbor, supra note 6, annex II.
262 Safe Harbor, supra note 6, annex I.
263 See Neely, supra note 261, at 12.
264 Safe Harbor List, supra note 51.
265 See Safe Harbor, supra note 6, annex II.
266 EU Safe Harbor Criticism, supra note 8, at 11.
atory supervisory authorities that provide for handling of individual complaints and dispute resolution” as an acceptable “independent recourse mechanism” option.\textsuperscript{267} On its face, the Safe Harbor seems to indicate that Companies can hire anyone to listen to and resolve EU Citizen complaints. As previously discussed,\textsuperscript{268} it appears that some Companies have interpreted this language to indicate that an “independent recourse mechanism” can include a Company’s own internal complaint process.\textsuperscript{269} At the outset, to allow a Company’s “independent recourse mechanism” to be the Company itself is a self-contradiction. It is hard to imagine a Company that would discuss a possible Safe Harbor violation directly with its customer and then refer the matter to a government enforcement body after a failure to reach a resolution. Companies that list their own internal resolution measures as their “independent recourse mechanism” fail to understand the Safe Harbor’s intent. The Safe Harbor specifically states that EU Citizens are first “encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms.”\textsuperscript{270} This language shows that the meaning of “independent” clearly excludes the very Company being complained about. Yet the Safe Harbor itself lacks guidance on what it means to be “independent.” The Safe Harbor states only that “[w]hether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record.”\textsuperscript{271}

iv. Conclusion on the types of independent recourse mechanisms

Altogether, the statutory language of the Safe Harbor Enforcement Principle’s “independent recourse mechanism” “layer” of protection is ineffective at ensuring compliance. Many Companies seem content with ignoring the clear intention of the Safe Harbor, and the DOC appears similarly content to allow the Safe Harbor registration of such Companies. “Independent recourse mechanism” sanctions are arbitrary and leave no promise of actual remedy for complainants. The Safe Harbor Enforcement Principle seems to rely on self-regulation to the point of absurdity.

\textsuperscript{267} Safe Harbor, supra note 6, annex II.
\textsuperscript{268} See supra Part III.B.3.a.
\textsuperscript{269} See, e.g., Safe Harbor List, supra note 51. (listing Adaptec, Inc.’s “independent recourse mechanism” as: “Consumer or Adaptec employee complaints will generally be escalated internally to the Adaptec corporate legal department which will consult with management on appropriate response or action depending on the facts at issue.”). Only after going through Adaptec’s process unsuccessfully will it refer the matter to an EU Data Protection Authority.
\textsuperscript{270} Safe Harbor, supra note 6, annex II.
\textsuperscript{271} Id.
2. Criticisms of the Enforcement Principle’s Verification Requirement

As explained earlier, a Company may choose to “self-verify” that its stated privacy practices are actually implemented. Given the choice between annual outside compliance reviews where the Safe Harbor requires “without limitation auditing, random reviews, [and] use of ‘decoys,’” and the choice of “self-verification,” it is not surprising that very few Companies choose to use outside compliance reviews to fulfill the verification requirement of the Enforcement Principle. Although a Company implementing “self-verification” is required to “retain their records on the implementation of their safe harbor privacy practices and make them available upon request in the context of an investigation,” there is no requirement for an “independent recourse mechanism” to employ additional sanctions if a Company falsely “self-verifies.” It is conceivable, and fully within the Safe Harbor guidelines, that a Company that acts willfully and in bad faith will receive the same or lesser sanction than another Company that has attempted to adhere to the Safe Harbor requirements, but has nonetheless committed a unintentional violation. Therefore, allowing “self-verification” to fulfill the verification requirement of the Enforcement Principle seems to dissuade proper implementation.

3. Worst-case scenario

Under the current Enforcement Principle regime, a frugal and risk-avoiding Company may take the following measures. A Company could fail to publish a privacy policy initially, and hope the DOC would accept its Safe Harbor registration, thereby evading FTC jurisdiction. Then a Company could choose an arbitration association that is known for ruling in favor of Companies as its method of “independent recourse mechanism,” thereby forcing a costly burden on an EU Citizen to initiate an action. Finally, the Company could “self-verify” that it is complying with its unpublished privacy practices. Taken one at a time, these possibilities seem troubling; taken together, they add up to a virtual guarantee that EU Citizen’s complaints will be ignored, with no Safe Harbor repercussions.

---

272 See supra Part III.B.3.b.
273 Safe Harbor, supra note 6, annex II.
274 Id.
275 See WOLF, supra note 19, 14–28.
276 Safe Harbor, supra note 6, annex II.
4. Conclusion on the effectiveness of the Enforcement Principle

a. Unintended consequences of the Enforcement Principle

Data breaches provide an example of the unintended consequences of the Safe Harbor’s Enforcement Principle. Identity theft in the U.S. is at an all time high, with a recent survey showing that 8.3 million American adults, or 3.7 percent of all American adults, were victims of identity theft in 2005.\footnote{Press Release, Fed. Trade Comm’n, FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005 (Nov. 27, 2007), http://www.ftc.gov/opa/2007/11/idtheft.shtm.} Thirty-two percent of the fraud complaints the FTC received in 2007 were in regards to identity theft.\footnote{Press Release, Fed. Trade Comm’n, FTC Releases List of Top Consumer Fraud Complaints in 2007 (Feb. 13, 2008), http://www.ftc.gov/opa/2008/02/fraud.shtm.} Although it is impossible to tell what proportion of identity thefts are the result of data breaches at the company level, Companies likely store data from EU Citizens at the same locations—with the same level of security—as the Company’s U.S. customers. Statistics are not available for the entire EU, but identity theft in the United Kingdom is on the rise.\footnote{See FRAUD PREVENTION EXPERT GROUP, REPORT ON IDENTITY THEFT/FRAUD (Oct. 22, 2007), http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf.} In 2006, approximately 100,000 United Kingdom citizens had their identity stolen annually, costing the United Kingdom economy £1.7 billion annually.\footnote{Id. at 8.}

Some U.S. states require companies to notify customers that may be affected by a data-breach, but U.S. state laws vary widely.\footnote{Currently thirty-eight states have data-breach notifications laws, but only a handful of those states provide a private right-of-action. See Scott Berinato, Data Breach Notification Laws, State By State, CSO Disclosure Series, Feb. 12, 2008, http://www.csoonline.com/read/020108/ammmap/ammmap.html. See also Posting of Tanya Forsheit to Privacy Law Blog, Breach Law Data, http://privacylaw.proskauer.com/2007/08/articles/security-breach-notification-i/breach-law-data/ (Aug. 3, 2007).} In contrast, under the Safe Harbor, a Company has no explicit requirement to notify EU Citizens affected by a data-breach. Therefore, an EU Citizen may be able to detect the end result of a data-breach in the form of a stolen identity, but an EU Citizen would be unable to pinpoint which Company was the source of infraction. Without knowing which Company is responsible, an EU Citizen cannot seek the assistance of any Company’s “independent recourse mechanism.” Any EU Citizen’s effort to find which Company was the source of the privacy violation would likely be fruitless. In this situation, the Safe Harbor Enforcement Principle “layer” only serves to delay or prevent resolution. In contrast, EU Citizens whose identities are stolen from a United Kingdom company are under the full protection of the Data Directive that...
provides immediate assistance through the Data Directive’s Data Protection Authorities.282

b. Fixing the Enforcement Principle

The Safe Harbor Enforcement Principle should be eliminated and replaced with an enforcement mechanism similar to the Data Directive.283 Eliminating the current Safe Harbor Enforcement Principle would enable an independent government agency with meaningful investigatory powers to act *sua sponte* to police privacy violations, such as data thefts, as soon as an EU Citizen discovers them. This solution, however, would require giving additional powers to a consumer-protection agency such as the FTC. The remaining sections of Part V address how to implement a more proactive FTC, with respect to the Safe Harbor, to properly guard against privacy violations.

Some may object, arguing that there is a need for private sector recourse remains in order to resolve simple complaints. It is admittedly helpful to have resolution procedures run by non-governmental agencies, to resolve mundane complaints and dismiss unsubstantiated complaints, however, mundane and unsubstantiated complaints can be settled at the Company level. It is important to stress that having only one official enforcement “layer” in the form of a U.S. government agency does not preclude an EU Citizen from resolving issues directly with a Company. Effective privacy enforcement requires a U.S. agency be available to EU Citizens at all times. This will ensure that EU Citizens’ privacy is monitored on a macro level and that EU Citizens’ can immediately turn to a U.S. agency to address complex data privacy issues such as data breaches.

C. Government Agency Enforcement through the Federal Trade Commission

1. The Federal Trade Commission’s limited jurisdiction within the United States

FTC’s power is limited in scope by statute.284 The FTC does not have the authority to regulate banks, saving and loans, credit unions, telecommunications, interstate transportation, common carriers, or air carriers.285 As discussed earlier, the only other governmental agency that has committed to enforcing the Safe Harbor is the Department of Transportation, which regulates interstate transportation, common carriers, and air

---

282 *See infra* Part V.C.2.a. (completing the analysis of the data breach example).
283 *See supra* Part III.C.1. (discussing the Data Directive’s enforcement mechanisms).
Banking and telecommunication Companies cannot register for the Safe Harbor unless and until the respective governing bodies commit to enforcement. The Federal Communications Commission—regulating the telecommunications industry—and the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Office of the Comptroller of the Currency—regulating the banking industry—have simply refused to commit themselves to Safe Harbor enforcement. Banking and telecommunication Companies, therefore, must rely on one of the two alternative methods for complying with the Data Directive: Binding Corporate Rules or Pre-Approved contracts. Because Companies do not uniformly comply with the Data Directive under the Safe Harbor, EU Citizens may be confused as to what recourse they have for privacy concerns and violations. Further, EU Citizens may be confused which, if any, regulatory body to contact for assistance.

Additionally, the FTC does not have authority to regulate non-profit Companies. The FTC Act states that the FTC can regulate organizations “affecting commerce.” Commerce is a legal term of art that has been interpreted to mean a great number of things. American courts have given the term “commerce” a very broad definition, for the purposes of interpreting U.S. Congressional authority to regulate under the commerce clause of the U.S. Constitution’s article I, section 8. In the case of the FTC, however, U.S. courts have interpreted the term commerce narrowly, allowing the FTC to regulate only traditional businesses—purveyors of goods and services.

286 See supra Part III.C.2.b.
288 See id. See also Safe Harbor, supra note 6, annex VII.
289 See supra Part III.A.
293 See Letter from Robert Pitofsky to John Mogg, Director, DG XV, supra note 290. See also Export.gov, supra note 290.
2. The Federal Trade Commission’s limited international jurisdiction
   a. Problem
   
   Although the FTC Act allows the FTC to regulate “commerce . . . with foreign nations,” U.S. court interpretations of the FTC Act have held that the FTC does not have power to pursue “unfair deceptive acts or practices” affecting only foreigners. For example, in Nieman v. DryClean U.S.A. Franchise Company, the U.S. Eleventh Circuit Court of Appeals stated that “the FTC Act does not clearly indicate that Congress intended the [FTC] Act to apply extraterritorially.” Therefore, the FTC’s authority over foreign “unfair deceptive acts or practices” only extends when there is a domestic impact. Failure to understand that the FTC lacks jurisdiction to pursue violations affecting only foreigners was blatant oversight by the EU Data Protection Authorities that negotiated the Safe Harbor.

   b. Proposed solution
   
   The Safe Harbor perhaps could rely on individual U.S. states’ attorney generals to be a substitute for the FTC’s current inability to pursue foreign “unfair deceptive acts or practices” because, as previously discussed, U.S. states have the power to regulate some aspects of privacy law. U.S. states, however, are pre-empted from regulating issues of international scope.

   The only remaining solution, therefore, is to increase the scope of the FTC’s authority to pursue foreign “unfair deceptive acts or practices.” Thankfully, the FTC can easily increase the scope of its power on its own.

298 See Branch v. FTC, 141 F.2d 31, 34–35 (7th Cir. 1944) (holding that the FTC has jurisdiction to regulate an entity’s conduct with respect to foreign customers based on the effect on domestic competition).
299 See supra Part V.B.4.a (discussing U.S. state data breach notification laws).
300 For example, Massachusetts vs. Environmental Protection Agency declared that “when a State enters the Union, it surrenders certain sovereign prerogatives . . . [States] cannot negotiate an emissions treaty with China or India, and in some circumstances the exercise of [a State’s] police powers to reduce in-state motor-vehicle emissions might well be pre-empted.” Mass. vs. EPA, 549 U.S. 497, 519 (2007). See also Crosby v. National Foreign Trade Council, 530 U.S. 363 (2000) (holding that Congress preempted a Massachusetts law that banned companies from doing business in Burma because, even though Congress was silent on preemption, the state law was an obstacle to implied objectives of federal Burma sanctions).
Under U.S. administrative law, the FTC is free to interpret its own originating statute, the FTC Act, so long as the originating statute was not already unambiguous on the matter. Although the FTC Act already, unambiguously, appears to allow the FTC to regulate “commerce . . . with foreign nations,” U.S. courts have limited this language. Nevertheless, the FTC could simply promulgate a rule interpreting its own originating statute, the FTC Act, and allow itself to pursue foreign “unfair deceptive acts or practices” despite the prior court rulings. The FTC’s new interpretation, though contrary to the previous court rulings, takes precedent.

3. The Federal Trade Commission’s limited investigatory powers

a. Problem

Under normal circumstances, the FTC Act allows the FTC to pursue outside investigation requests from five groups: (1) the U.S. Attorney General; (2) the U.S. President; (3) the U.S. Congress; (4) U.S. courts; and (5) the general public. Additionally, the FTC can initiate investigations on its own. The FTC Act appears to give the FTC broad investigatory powers; however, under the Safe Harbor, the FTC limited its own inves-

---

302 See Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984) (holding that if Congress has not directly spoken on an issue of an administrative agency’s power, then courts should defer to an agency’s construction of their own originating statute so long as such construction is reasonable).
304 See, e.g., Nieman v. DryClean U.S.A. Franchise Co., 178 F.3d 1126, 1130 (11th Cir. 1999) (stating that “the FTC Act does not clearly indicate that Congress intended the [FTC] Act to apply extraterritorially”).
305 Rulemaking is procedure under administrative law where a U.S. governmental agency creates a rule that has the force of law after a notice and comment period. See 5 U.S.C. § 553. Further discussion on the requirements of rulemaking and administrative law are beyond the scope of this Note.
306 See Nieman, 178 F.3d at 1130.
307 See National Cable & Telecommunications Association v. Brand X Internet Services, 545 U.S. 967 (2005) (holding that prior judicial construction of an agency’s originating statute is only given force if the prior decision holds that statutory construction requires a certain construction based on unambiguous terms of the statute, leaving no room for agency discretion).
309 Id.
310 Id.
311 Id.
tigatory power.\footnote{See Safe Harbor, supra note 6, annex V.} One of the Safe Harbor documents is a letter written by the FTC in response to the European Commission’s concerns about enforcement.\footnote{See Letter from Robert Pitofsky to John Mogg, Director, DG XV, supra note 290.} The FTC stated that it would “give priority to referrals of non-compliance with safe harbor principles.”\footnote{Id. (emphasis added).} “Referral” is a critical word that refers to the Safe Harbor Enforcement Principle’s guarantee to remedy requirement, which states that any “independent recourse mechanism” must notify both the DOC and the governmental body with applicable jurisdiction—usually the FTC—if a Company fails to comply with the procedures and remedies demanded by the “independent recourse mechanism.”\footnote{See Safe Harbor, supra note 6, annex II.} Therefore, under the Safe Harbor, the FTC may only receive investigation requests from “independent recourse mechanisms.” Additionally, even if the FTC receives an investigation request from an “independent recourse mechanism,” the Safe Harbor fails to require the FTC to act; instead, the Safe Harbor only states that the FTC will “give priority” to “independent recourse mechanism” investigation requests.\footnote{Id. annex V.} An EU Citizen, therefore, has no recourse if the FTC does not investigate a Company—despite an investigation request from the Company’s “independent recourse mechanism.” An EU Citizen could only submit a hard-to-locate complaint\footnote{See Communication & Information Resource Centre Administrator (CIRCA) Date Protection Panel, Standard Complaint Form, http://circa.europa.eu/Public/irc/secureida/safe harbor/library?l=/public_folder/complaint_form&vm=detailed&sbc=Title (last visited Aug. 31, 2008).} to his or her country’s Data Protection Authority and hope that the Data Protection Authority will convince the FTC to reconsider and take action on the “independent recourse mechanism” investigation request.

Some Companies have stated that they have chosen not to join the Safe Harbor because of the very real possibility that, even if a matter were referred to the FTC by an “independent recourse mechanism,” the FTC could take no action. British Petroleum’s group privacy and data protection manager state that British Petroleum did not join the Safe Harbor because it “lacked the desired teeth to physically bind BP’s affiliates to the Safe Harbor principles.”\footnote{Pedersen, supra note 9, at 3.} Even if the FTC were to follow up on an investigation request from an “independent recourse mechanism,” both the EU Citizen whose privacy is at issue and any concerned third party, such as the Article
29 Working Party, would have no standing on any investigation that the FTC conducts.\footnote{236}

In summation, EU Citizens that ordinarily rely on EU member state Data Protection Authorities to protect their privacy rights\footnote{291} are forced to become their own police agents and report unresolved violations on their own.\footnote{323} Continuing with the data breach example,\footnote{324} EU Citizens seem particularly ill suited to detect data breaches occurring in the U.S., save for well-reported data thefts. The majority of data privacy concerns stem from one of two circumstances. The first situation is when there is a private sale of personal information—for example, to a marketing company willing to pay for personal home addresses—where both parties to the transaction would rarely be open about their actions. The second scenario is when a Company is “hacked” and personal information is stolen from it. Some Companies may want to keep quiet about the breach of security. In both of these scenarios, the FTC’s self-limitation on enforcing the Safe Harbor means that there is no centralized regulatory body that can remedy the data breach privacy violations in a uniform manner.

b. Proposed Solution

The DOC and the Data Protection Authorities should amend the Safe Harbor to compel FTC oversight and allow for investigation requests directly from EU Citizens and third-party organizations. A 2004 EU commission on the Safe Harbor similarly urged the FTC to “undertake \textit{sua sponte} investigations where questions exist regarding Safe Harbour compliance.”\footnote{325} The FTC already has procedures in place for accepting public complaints.\footnote{326} Additionally, many third-party non-governmental organizations would voluntarily help the FTC enforce the Safe Harbor, such as the Electronic Privacy Information Center\footnote{327} and the Electronic Frontier Foundation.\footnote{328} Finally, each EU member state’s Data Protection Authority has its


\footnote{291} \textit{See supra} Part III.C.1.

\footnote{323} \textit{See supra} Part V.B.4.a (discussing how an EU Citizen would be unlikely to pinpoint the source of a stolen identity).

\footnote{324} \textit{Id}.

\footnote{325} EU Safe Harbor Criticism, \textit{supra} note 8, at 10.


own research abilities.\textsuperscript{329} The Data Protection Authorities would undoubtedly be willing to research potential violations of privacy on behalf of EU citizens and forward the information to the FTC.

It would take a large bureaucracy to oversee hundreds of Company’s privacy protection initiatives, and the FTC may not have the resources to devote to many investigations given the scope of data exchange between the EU and U.S.\textsuperscript{330} Additionally, the FTC Bureau of Consumer Protection’s Division of Enforcement and Privacy are probably more motivated to use their limited resources\textsuperscript{331} to enforce laws that have a direct impact on Americans. The FTC, however, would not have to use many resources, if it received assistance from non-governmental organization and Data Protection Authority investigations and complaints.

If the Safe Harbor were amended to force FTC oversight and allow for investigation requests directly from EU Citizens and non-governmental organizations, then the Enforcement Principle would need to be completely rewritten. The new Enforcement Principle should be flexible enough to take a common law approach similar to the Data Directive, but should also codify ongoing interpretations of the Safe Harbor. This would give Companies more concrete notice of actions that violate the Safe Harbor.

As previously discussed, the Data Directive employs a common law adjudication approach to enforcement.\textsuperscript{332} A common law approach is useful for dealing with new situations and to adjudicating by analogy; however, the new Enforcement Principle should also inform Companies of the current state of the law. To accomplish this, the FTC should use its power to promulgate rules.\textsuperscript{333} Since 1962, the FTC has promulgated rules that define specific acts as unfair or deceptive.\textsuperscript{334} After the FTC promulgates a rule under §57a(a)(1)(B), any violation of that rule is considered a \textit{per se} unfair or deceptive act or practice under the FTC Act.\textsuperscript{335} Therefore, as the FTC adjudicates new privacy cases, the FTC may promulgate new rules to reflect the


\textsuperscript{330} In 2004, the U.S. and its six largest European trade partners shared approximately $400 billion in trade. U.S.-EU Safe Harbor Framework PowerPoint, supra note 59, at slide 3.

\textsuperscript{331} See \textsc{WARD}, supra note 321, at 2–3 (“As federal bureaucracies go, the Federal Trade Commission is small. Its annual budget is approximately $156 million and it has a total staff of approximately 1000.”).

\textsuperscript{332} See supra Part III.C.1 (“Data Protection Authorities give prior privacy adjudications a \textit{res judicata} effect when litigating new cases.”).

\textsuperscript{333} See 15 U.S.C. § 57a(a) (2006). For a brief discussion of these rules and rulemaking, see supra note 305.

\textsuperscript{334} The FTC’s rulemaking authority was later upheld as constitutional. See Nat’l Petroleum Refiners Ass’n v. FTC, 482 F.2d 672 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974).

\textsuperscript{335} 15 U.S.C. § 57a(d)(3).
new adjudications. Additionally, the FTC could pass annual or bi-annual rulemakings that implement new understandings of the Data Directive, as interpreted by the Article 29 Working Party resolutions and the Data Protection Authorities. The FTC rulemakings would save the FTC time and resources in adjudicating new cases.

Peter Fleischer, Google’s Chief Privacy Counsel, has complained that it is difficult to keep track of different countries’ privacy laws.\(^336\) Mr. Fleischer stated that “[t]o be effective, privacy laws need to go global. . . . [Privacy] standards must be strong and credible but above all, they must be clear and they must be workable.”\(^337\) FTC rulemakings would be a good step towards quelling Mr. Fleischer’s concerns by harmonizing EU and U.S. data protection law.

4. The Federal Trade Commission enforcement is prepared to regulate privacy violations

The FTC has the experience necessary to regulate Companies that transfer EU Citizen data. The FTC could protect EU Citizens better in two circumstances. The DOC and the Data Protection Authorities could agree to amend the Safe Harbor to compel FTC oversight and allow for investigation requests directly from EU Citizens and non-governmental organizations.\(^338\) Alternatively, even if the Safe Harbor agreement is not amended, the FTC could increase investigations and enforcement under U.S. law against Companies that are members of the Safe Harbor. Companies that violate U.S. privacy law are likely the same Companies, which would also be abusing the Safe Harbor principles.

In the past, the FTC has vacillated on its role to regulate consumer privacy violations. In 1999, the FTC officially supported Company self-regulation for issues of privacy.\(^339\) In 2000, however, after completing a survey on website privacy policies, the FTC recommended legislation to protect privacy.\(^340\) Despite the FTC’s change of heart, when George W.

---


Bush appointed a new head FTC commissioner, the FTC’s policy reverted to privacy self-regulation. Today, the FTC polices online privacy in four areas: (1) U.S. consumer access to their own information; (2) U.S. consumer choice about use of their information; (3) U.S. consumer opportunity to correct errors in collected information; and (4) security of information from unauthorized use.

The FTC’s earliest effort of applying the FTC Act to online privacy was a 1999 prosecution of GeoCities, a website hosting service. GeoCities offered free and fee-based web hosting services after consumers filled out an online form that included some questions that were mandatory and other questions that were optional. The form also asked if applicants wished to receive offers from advertisers. The FTC alleged that the GeoCities website misled customers to believe that advertisers would only receive the information consumers provided in the mandatory sections, including name and address. Instead, GeoCities also shared the information that consumers provided in the optional form sections, including education level, income, marital status, occupation, and interests. The FTC settled with GeoCities in return for GeoCities’ agreement to post a privacy policy that informed consumers what information was being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information.

The FTC has also successfully pursued several other corporations for online privacy violations. In 2000, the FTC prosecuted ReverseAuction.com for harvesting consumers’ personal information from a competitor’s site and then sending deceptive spam to the consumers to solicit their business. In 2000, the FTC prosecuted Toysmart.com for selling...
idential, personal customer information collected on the Toysmart.com website, despite Toysmart.com’s privacy policy to the contrary. In 2001, the FTC prosecuted Microsoft for falsely representing that its “Passport Wallet” service, which stored customer credit card numbers and billing information, was safer or more secure than purchases made at other websites without the “Passport Wallet” service. In 2002, the FTC prosecuted the pharmaceutical company Eli Lilly for unintentionally disclosing the entire recipient list of a Prozac refill-reminder service to every subscriber of the service. In 2002, the FTC prosecuted Guess.com—a website that sells Guess jeans—for failing to take reasonable measures to prevent consumer information, including credit card numbers, from being accessed by hackers. In 2004, the FTC prosecuted Tower Direct—the company that owns Tower Records and runs the Tower Records website—for a security flaw in the Tower Records website that exposed customers’ personal information to other customers, in violation of Tower Direct’s privacy policy representations. Finally, in 2005, the FTC prosecuted Vision Properties—a company that provided virtual “shopping cart” services to thousands of online merchants—for collecting and renting customer personal information sourced from the online merchants that employed Vision Properties. Neither the


customers nor the online merchants that employed Vision Properties consented to collecting and renting the customer information.\footnote{See Press Release, Fed. Trade Comm’n, Internet Service Provider Settles FTC Privacy Charges (Mar. 10, 2005), http://www.ftc.gov/opa/2005/03/cartmanager.shtml.}

Finally, the FTC has recently taken several proactive steps to address online privacy. It has created an online tutorial to educate businesses and other organizations about practical and low-cost data security methods.\footnote{See Fed. Trade Comm’n, Protecting Personal Information: A Guide for Business, http://www.ftc.gov/infosecurity/.} Additionally, it addressed the behavioral advertising issues raised by online advertising and the merger of Google and DoubleClick.\footnote{See supra Part IV (discussing the privacy implications of the Google-DoubleClick merger).} In November 2007, the FTC held a conference on behavioral advertising.\footnote{See Press Release, Fed. Trade Comm’n, FTC to Host Town Hall to Examine Privacy Issues and Online Behavioral Advertising (Aug. 6, 2007), http://www.ftc.gov/opa/2007/08/ehavioral.shtml. See also Fed. Trade Comm’n, Behavioral Advertising: Tracking, Targeting, and Technology, http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.} In response to input received at the conference, the FTC commissioner voted unanimously to approve the release of new behavioral advertising privacy principles.\footnote{See Fed. Trade Comm’n, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), http://www.ftc.gov/opa/2007/12/principles.shtml.} The FTC proposed that behavioral advertisers should: (1) clearly state that consumer data is being collected; (2) allow consumers to easily opt-out of data collection; (3) secure the customer data collected; (4) retain customer data only “as long as is necessary to fulfill a legitimate business or law enforcement need;” (5) obtain a customer’s “affirmative express consent” if a behavioral advertiser wishes to use a customer’s data for a “materially different purpose than was disclosed when the data was collected;” and (6) obtain a customer’s “affirmative express consent” before collecting “sensitive” consumer data—such as data on health and sexual orientation.\footnote{See Fed. Trade Comm’n, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, available at http://www.ftc.gov/os/2007/12/P859900stmt.pdf.} The FTC’s proposed behavior advertising principles are extremely similar to the Safe Harbor’s general requirements on data collection.\footnote{See supra Part III.B.2 (discussing the Safe Harbor’s Notice, Choice, Onward Transfer, Security, Data Integration, and Access Principles).} The FTC’s recent proactive approach to privacy regulation shows that it is prepared to undertake a larger role regulating privacy under a revised Safe Harbor.
VI. CONCLUSION

Although the EU may have initially believed that the Safe Harbor Enforcement Principle’s “independent recourse mechanisms” could effectively enforce the Safe Harbor, it remains highly questionable whether the current enforcement mechanisms are sufficient. The enforcement mechanisms in place appear ineffective and, therefore, are likely unable to deter violators. Ineffective enforcement, in turn, creates deteriorating trust and possibly reduced trade. The EU and the U.S. should renegotiate the Safe Harbor’s Enforcement Principle and replace its ineffective “independent recourse mechanisms” with FTC oversight. Broad FTC oversight would be an effective Safe Harbor enforcement mechanism that would reconcile the difference between EU and U.S. privacy laws.