HOW SAFE IS THE SAFE HARBOR? U.S. AND E.U. DATA PRIVACY LAW AND THE ENFORCEMENT OF THE FTC'S SAFE HARBOR PROGRAM[1]

I. INTRODUCTION

Technological developments in recent years have caused rapid changes in the way business is conducted around the world. Markets are no longer tied to any particular geographic region, but rather have dramatically expanded through electronic communication technology.[2] Globalization has increased the availability of information and facilitated positive developments in numerous fields, including education, business, and economics. Specifically, the interaction between U.S. and European market players benefits greatly from the expansion of e-commerce. However, globalization has also generated concerns about protecting the privacy of personal information.

[1] First prize winner of the Andrew P. Vance Memorial Writing Competition, sponsored by the Customs and International Trade Bar Association and Brooklyn Law School.

[2] Gary Minda, *Book Review: Globalization of Culture*, 71 U. COLO. L. REV. 589, 590-1 (Summer 2000) (reviewing DANIEL YERGIN & JOSEPH STANISLAW, THE COMMANDING HEIGHTS: THE BATTLE BETWEEN GOVERNMENT AND THE MARKETPLACE THAT IS REMAKING THE MODERN WORLD (1998)).

The United States and the European Union approach data privacy differently, based on the values that underlie their respective legal and political systems, with the European Union taking a broader approach to data privacy protection than the United States. In light of such differences, E.U. policy makers are increasingly preoccupied with the potential loss of privacy protection its citizens might suffer when engaging in transatlantic e-commerce.

In the past few years, the privacy of airline passengers' data moved to the forefront of public discourse, as the new U.S. disclosure requirements conflict in many fundamental ways with the protective requirements of the European Union. News reporting brought attention to the plight of passengers seeking privacy for their personal information, and both governments acknowledged people's rights to protection in this regard.[3] However, of equal importance to this headline issue is the situation individuals face every day as consumers: What happens to personal information once it is disclosed to business entities in the course of ordinary purchases?

Jurisdiction and enforcement remain unsettled issues in the field of data privacy law. In transatlantic data transfers, it is not always clear which jurisdiction provides the governing law, and sometimes one jurisdiction must enforce the law of another. Therefore, to successfully protect an individual's right to privacy, international cooperation is needed to settle the jurisdiction question and to ensure an acceptable level of enforcement. The United States and the European Union must work together to find a mutually acceptable solution, and to ensure that the development of the new information economy does not come at too high a price to personal privacy.

The United States and the European Union have taken some significant steps in this direction, but the practical impact is yet unclear. There are now several ways for the U.S. and the E.U. to provide for consumer data privacy. Of particular importance is the Safe Harbor program, established by the U.S. Federal Trade Commission and the Commission of the European Union, to facilitate data transfer between the two countries. While the terms of the Safe Harbor reach a formally sound compromise between each country's principles, it is not obvious that the FTC's enforcement will provide an adequate remedy for individuals in case of privacy violations. Since privacy protection means very little without effective enforcement, poor enforcement of Safe Harbor provisions may also have a negative effect on the willingness of each government to work together in the future.

Surprisingly, literature on transatlantic data transfers pays little attention to the way the existing mechanisms of data protection work in prac-

---

[3] For a listing of news articles about conflicts between the U.S. and the E.U. in this area, *see EU-US Airline Passenger Data Disclosure at* http://www.epic.org/privacy/intl/passenger_data.html.

tice, and particularly to their significant shortcomings. The purpose of this paper is to analyze in detail the present mode of U.S. and E.U. intervention in data privacy protection, to illustrate the actual and potential problems raised by an insufficient level of transatlantic cooperation, and to identify remaining points of friction that demand urgent attention.

Part II looks generally at the data privacy laws in place in the United States and the European Union, and the principles that underlie each approach. Part III discusses two methods of transferring data between the United States and the European Union, specifically the European Commission's Model Contract Clauses and the U.S. FTC's Safe Harbor program. Part IV focuses on certain privacy cases recently brought to the attention of the FTC. These cases are not explicit violations of the Safe Harbor, but the FTC stated they will inform the approach to such violations when actual complaints arise. A close analysis of the settlements generated by these disputes casts serious doubts on the effectiveness of the proposed enforcement system. Part V urges further international cooperation to develop a solution to data privacy concerns that meets the requirements of both governments, while also guaranteeing the promised level of privacy protection to the citizens of the European Union.

II. Data Privacy in the European Union and the United States

For a long time, companies have been collecting and using personal demographic and contact information as a means of targeting individual consumers for marketing purposes, even selling that data to third parties to generate profit. Personal information collected by companies often includes names, e-mail addresses, postal addresses, social security numbers, and credit card numbers. This data is collected in many different ways, including credit applications, online purchases, promotional offers, free trials, and contests or sweepstakes entries. The growth of computer technology and the Internet has made it easier than ever to collect this data from consumers all over the world, and has facilitated the development of a new information economy.[4]

The exchange of personal information is an integral part of the global knowledge-based economy, especially since companies strive to sell their goods and services to consumers throughout the world, as well as develop partnerships and joint ventures with foreign companies. Much of this data exchange takes place between the United States and the European Union, as these are two of the world's leading trading blocks.[5] As a result of this increased flow of information, there is increased concern about the privacy of personal data. The wide availability of sensitive personal iden-

---

[4] Minda, supra n. 2 *at* 601-02.

[5] Thomas Heide, *Access Control and Innovation Under the Emerging EU Electronic Commerce Framework*, 15 Berkeley Tech. L. J. 993, 1000 - 1001 (Fall 2000).

tification information not only creates inconveniences for consumers, but also facilitates crimes such as identity theft.

Advances in computer and communication technology have even changed what we mean by the idea of "privacy" as applied to the collection and use of personal data. Before the technological revolution, "privacy" was effectively synonymous with "secrecy." The ability to block access to one's personal data was likened to physically protecting one's property.[6] But with rapid new technological developments, "privacy" has come more closely to mean "the power to control the facts about one's life."[7] As a result, two main approaches to data privacy protection emerged. One approach is a return to "secrecy" as a means of privacy protection, using data protection systems such as encryption.[8] While encryption systems play an important role in the development of international data privacy schemes, the details of such systems are beyond the scope of this paper.

A second, broader approach to protecting data privacy is the use of legislation, commonly referred to as "access control legislation," to control the flow of personal information.[9] However, legislative access controls are often difficult to implement because they must be developed and enforced by government agencies rather than by individuals. This is troublesome for two reasons. First, many different groups within a single country compete to establish legislation designed to meet their particular interest. For example, in the United States, individuals concerned about data privacy must battle with companies that claim a right to collect, use, and sell this data. Second, different countries have different approaches to the development of access control legislation, based on their own cultural values and governmental structure.[10]

A. *Current State of Privacy Laws: Different Approaches to the Same Problem*

Different countries employ different approaches to data privacy and access control legislation, based on their cultural, historical, and socio-economic peculiarities, and the specific features of their political systems.[11] With the globalization of business and information, the different systems of the United States and the European Union often clash over

---

[6] Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L. J. 1145, 1217 (Fall 2000).

[7] Frederick Schauer, *Internet Privacy and the Public-Private Distinction,* 38 JURIMETRICS J. 555 (Summer 1998).

[8] Sommer, *supra* note 6, at 1218.

[9] *See, e.g.* Heide, supra note 5.

[10] V.V. Smirnov, *Law, Culture, Politics: Theoretical Aspects*, *in* COMPARATIVE LAW AND LEGAL SYSTEMS: HISTORICAL AND SOCIO-LEGAL PERSPECTIVES, 23 (W. E. Butler and V. N. Kudriavtsev, ed., 1985).

[11] *Id.*

how to handle data privacy issues. The differences between U.S. and E.U. legislative efforts are generally influenced by their differing attitudes toward the concept of data privacy and which "fundamental rights" require protection.

These clashes frequently arise as a result of the Data Directive's requirements concerning the conditions under which personal data can be transferred outside the European Union.[12] The Data Directive is the primary component of data privacy law in the European Union, and it specifically requires that a non-E.U. country must have "adequate" data privacy protections in place to receive data from the European Union.[13] Since the European Union deemed U.S. privacy protections inadequate to meet the demands of the Data Directive, data can only be transferred between the European Union and the United States by contractual arrangement or compliance with the U.S. Federal Trade Commission's Safe Harbor program.

Before looking at the Safe Harbor program and its alternatives, it is important to consider the background of E.U. and U.S. privacy law, as well as the policy behind each of these systems.

1. The European Union

The primary component to European Union data privacy law is the Data Directive, which regulates how personal information may be collected and used, inside and outside the European Union. The Data Directive was created to unify the Member States' approaches to data privacy, which until then varied considerably. The Data Directive recognizes that free transfer of information is vital to the development and success of the E.U. internal market, while also protecting an individual's right to data privacy. The Data Directive also seeks to protect the privacy of individuals' data when that information is passed from the E.U. to a non-member country.

The Data Directive does not provide specific examples of what information constitutes protected "personal data." Instead, Article 2(a) is drafted broadly, defining "personal data" as "any information relating to an identified or identifiable natural person."[14] This includes "reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity."[15] Additionally, the Data Directive defines certain types of information as belonging to a "special category" requiring extra protection. This

---

[12] Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 (hereinafter "Data Directive").

[13] Data Directive, art. 25.

[14] Data Directive, art. 2(a).

[15] Data Directive, art. 2(a).

includes data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life.[16]

The Data Directive applies to the "processing of personal data," another broadly defined concept. Article 2(b) defines data collection as "any operation or set of operations which is performed upon personal data." This includes "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[17] Article 2(b) is worded such that it covers almost any way someone's personal information could be used for a commercial purpose.

In addition to its broad definitions of personal data and data processing, the Data Directive prescribes very strict standards as to how data must be stored and protected, and under what circumstances and to whom it may be released. The individual Member States can create their own regulations for data processing,[18] but Article 7 of the Data Directive is very clear about the limited instances in which data can be processed without the individual's unambiguous consent. These include processing necessary to perform a contract, to protect the public interest, and to protect the vital interest of the individual, which often arises in the context of health or some other emergency.[19] For the special categories of data mentioned above, processing without the individual's consent is even more restricted, and adequate privacy safeguards must be in place first.[20] Member States must also guarantee every person the right to access any of their data, and the right to know exactly what information is being processed and in what fashion.[21] Individuals must also have the right to object at any time, on "compelling legitimate grounds," to the processing of their personal information.[22]

The Data Directive also requires Member States to provide a judicial remedy for any individual whose data privacy rights are violated.[23] This requirement poses a problem when the violation occurs at the hands of a company from outside the European Union, where another country must provide the remedy. In the United States, the responsibility for enforcement often falls to the Federal Trade Commission, with varying results.

In addition to regulating the flow of data between Member States, the Data Directive regulates the transfer of data to countries outside of the

---

[16] Data Directive, art. 8(1).
[17] Data Directive, art. 2(a).
[18] Data Directive, art. 5.
[19] Data Directive, art. 7(b), (e), (d).
[20] Data Directive, art. 8.
[21] Data Directive, art. 12.
[22] Data Directive, art. 13.
[23] Data Directive, art. 22.

European Union. Specifically, Article 25(1) prohibits the release of data to any country outside the European Union unless the receiving country provides "an adequate level of protection" to the privacy of the individual's data.[24] The Data Directive does not provide an exact definition for the term "adequate," but does establish several factors to consider when assessing the adequacy of privacy protection provided by the third country. These factors include the nature of the data, the purpose and duration of the proposed processing operation, the countries of origin and final destination, the general and sectoral rules of law in force in the third country, and the professional rules and security measures within that country.[25]

The Commission of the European Union has the authority to determine whether a third country meets the "adequate" standard for data protection.[26] To make this determination, the Commission may consider the domestic laws and international commitments of the third country.[27] If the Commission finds that a third country does not provide adequate protection, the E.U. Member States are empowered to take "any measures necessary" to prevent transfer of data to the third country in question.[28]

In July 2000, the European Parliament deliberated and determined that U.S. privacy protection does not meet this minimum standard.[29] The Commission followed the recommendation of Parliament and decided that, without further arrangements for collection and handling, U.S. law alone does not provide an adequate level of privacy protection.[30] The European Union therefore prohibits the release of personal data to companies in the United States unless special agreements are reached.[31] These agreements are generally either private contracts created by the companies seeking to exchange data, or participation in the FTC's Safe Harbor program, both of which are discussed in greater detail below.

The general principle governing the Data Directive is that each individual has a right to maintain the privacy of his personal information. This principle originated in Article 8 of the European Convention for the Pro-

---

[24] Data Directive, art. 25(1).

[25] Data Directive, art. 25(2).

[26] Data Directive, art. 25.

[27] Data Directive, art. 25(6).

[28] Data Directive, art. 25(4).

[29] European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, together with Committee on Legal Affairs and the Internal Market. Hearing on 22/23 February, 2000. See also Elizabeth de Bony, *E.U. Rejects U.S. Data Privacy Protection as Inadequate*, CNN ONLINE, July 7, 2000, *available at:* http://www.cnn.com/2000/TECH/computing/07/07/safe.harbor.idg.

[30] Lori Lierman, *Go Global. Get Information. Now what?* BUSINESS LAW TODAY, Jan/Feb 2003, at 57-60. *See also* Data Directive, art. 25.

[31] *Id.*

tection of Human Rights and Fundamental Freedoms,[32] and is now part of Article 8 of the Charter of Fundamental Rights of the European Union.[33] This approach assumes that individuals' data privacy is to be protected unless there is some specific, compelling interest or another legitimate basis for requiring disclosure or other forms of processing.[34]

The Data Directive incorporates these compelling interests, and grants exceptions to the privacy protection requirement in some specific instances where a competing interest outweighs the individual's right to data privacy. This includes processing operations concerning public security[35], and certain processing for historical, statistical, or scientific purposes.[36] Data processing for journalistic or artistic purposes is permitted if necessary to reconcile the right to privacy with the right to freedom of expression.[37]

The Convention and the Charter both establish a right to "freedom of expression."[38] This includes the freedom to "receive and impart information and ideas without interference by public authority and regardless of frontiers."[39] However, this right is qualified by the "duties and responsibilities" that the exercise of this freedom inherently carries with it.[40] As such, this freedom may be subject to formalities and conditions required for, among other things, the "protection of the reputation or rights of others."[41] Therefore, the right to privacy functions as a limitation on the general right to freedom of expression, and vice versa.

The Convention and the Charter both establish that everyone whose rights and freedoms are violated shall have an effective remedy before a

---

[32] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8(1) (hereinafter "Convention").

[33] Charter of Fundamental Rights of the European Union, art. 8 (hereinafter "Charter"). The Charter sets out a range of civil, political, economic and social rights of European Citizens, but is not a binding document. However, its principles are generally accepted within the European Union, and discussion is underway as to whether it should be made legally binding through incorporation into the Treaty of the European Union. *See* Charter of Fundamental Rights: Home Page *at* http://www.europarl.eu.int/charter/default_en.html.

[34] Convention, art. 8(2). Charter, art. 8.

[35] Data Directive, art. 3(2).

[36] Data Directive, art. 6(b).

[37] Data Directive, art. 9.

[38] Convention, art. 8(1); Charter, art. 11.

[39] Convention, art. 8(1); *See also* Charter, art. 11.

[40] Convention, art. 8(2). Article 8 in the Charter does not explicitly mention this qualification. However, it is likely that a similar interpretation would be read into the Charter, since it must balance other competing rights, including the right to privacy, with the right of expression.

[41] Convention, art. 8(2). Article 8 of the Charter does not mention this qualification either.

national authority.[42] Accordingly, the Data Directive includes procedures that individuals can use to control the collection and processing of their information,[43] as well as remedies for situations where these requirements are breached.[44] However, the right to an effective remedy can be difficult to enforce when the violation occurs outside of the European Union.

2. The United States

In contrast to the relevant European Union documents, the U.S. Constitution makes no explicit mention of a right to privacy.[45] The concept of a "right to privacy" was introduced in its modern form through scholarly articles,[46] and was developed by the Supreme Court through the "penumbra" doctrine.[47] However, because it is not explicitly mentioned in the Constitution, it is often seen as secondary to other rights such as freedom of expression.[48] The Legislature and the judicial system both play an important role in developing the doctrine of data privacy protection in the United States.

The U.S. government initially favored industry self-regulation over a broad legislative approach to data privacy protection.[49] U.S. companies favored this approach as well, because they believed advancements in communication technology would lead to the development of new business models, and they did not want broad data privacy laws to interfere with this advancement process.[50] This approach assumed the free market system would require companies to adapt to consumers' data privacy protection needs while simultaneously protecting the company's own economic interests, thus causing data privacy regulations to normalize to a level acceptable to both companies and consumers.

---

[42] Convention, art. 13. *See also* Charter, art. 47.

[43] Data Directive, art. 14.

[44] Data Directive, art. 22.

[45] *See* Marie Clear, *Falling into the Gap: EU Data Protection and its Impact on US Law and Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 981, 992.

[46] Louis D. Brandeis and Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[47] *See, e.g., Griswold v. Connecticut*, 381 U.S. 479 (1965). In this case, the Supreme Court invoked the Constitutional rights afforded by several other amendments, and then tied them all together with the Ninth Amendment protection of individual rights retained by the people. However, the Court stopped short of reading an actual "right to privacy" into the Constitution, and the decision in this case and other similar cases are often regarded as turning on specific facts rather than general doctrine.

[48] *See* U.S. CONST., amend. I.

[49] *The FTC's First Five Years Protecting Consumers Online at* http://www.ftc.gov/os/1999/12/fiveyearreport.pdf

[50] Shaun A. Sparks, *The Direct Marketing Model and Virtual Identity: Why the US Should Not Create Legislative Controls on the Use of Online Consumer Personal Data*, 18 DICK. J. INT'L LAW 517, 520 (Spring 2000).

To promote this goal, the FTC established five principles to govern industry self-regulation efforts, but left companies to implement and enforce them on their own.[51] These principles included: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.[52] A number of trade organizations developed voluntary compliance programs based on these principles to encourage self-regulation within their own industries, in hopes of avoiding government intervention.[53]

Within a few years, research performed by the FTC determined that self-regulation was not successful in meeting consumers' demands for data privacy. In its 1998 report to Congress, the FTC noted that many commercial Web sites provided notice of their data handling procedures and offered users some choices with respect to the handling of their personal data.[54] However, many of them failed to provide access and security for this data, or to properly enforce their privacy policies in accordance with the FTC's five principles.[55]

In 2000, the FTC mostly abandoned its position on self-regulation, and urged Congress to adopt more legislation to protect consumer privacy.[56] Since that time, the Legislature passed a number of laws designed to meet the consumers' growing demand for data privacy protection. These laws include the Children's Online Privacy Protection Act ("COPPA")[57], the Health Insurance Portability and Accountability Act ("HIPAA")[58], the Electronic Communications Privacy Act ("ECPA")[59], and the Computer Fraud and Abuse Act ("CFFA").[60]

Despite Congress's efforts to increase government regulation of data privacy, the European Union still considers U.S. privacy protections inadequate to meet the requirements of the Data Directive.[61] While Congress

---

[51] *Privacy Online: A Report to Congress*, Federal Trade Commission Report (June 1998), at 7 (hereinafter "1998 FTC Report").

[52] *Id. See also Privacy Online: Fair Information Practices in the Electronic Marketplace*, Federal Trade Commission Report (May 2000), at ii-iii (hereinafter "2000 FTC Report").

[53] *See, e.g.,* the Platform for Privacy Preferences Project ("P3P") *at* http://www.w3c.org/p3p *and* TRUSTe *at* http://www.truste.org.

[54] 1998 FTC Report, *supra* n. 51

[55] *Id. at* ii.

[56] 2000 FTC Report, *supra* n. 52, at ii-iii.

[57] Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§6502-6505 (1998).

[58] Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C.A. §210 (2003).

[59] Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§2510-2521 (2003).

[60] Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§1030 *et seq* (2002).

[61] European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, together with Committee on Legal Affairs and the Internal Market.

has admirably addressed data privacy concerns for the specific areas covered by its laws, it still has not provided for a general right of data privacy protection as contemplated by the Data Directive. Until Congress passes a broad, sweeping law granting data privacy protection to all people in all situations, it seems likely that the European Union will continue to regard the United States' protections as inadequate.

Recent U.S. actions indicate some movement toward broader legislation, as demonstrated by the changes to the Fair Credit Reporting Act ("FCRA"). In a legislative action on November 5, 2003, Congress tightened the controls on data processing with respect to credit reporting companies. These changes preempt state laws on data privacy, and establish a uniform approach to data privacy in the context of credit reporting.[62] Such broad action produces mixed results because of the wide variety of laws in place in each state. While the changes to the FCRA raise the level of privacy protection in some states, they actually decrease the level of protection available in others. On one hand, states that have strict data privacy laws hesitate to give up their citizens' protections for the sake of uniformity of law.[63] On the other hand, states that do not provide strict data privacy protection are unlikely to agree to a proposed national standard.[64] Despite the reluctance of both sides, the passage of these changes strengthening the FCRA suggest that other such compromises may be possible in the coming years, and perhaps one day data privacy law in the United States will be more uniform.

Administrative adjudications and judicial decisions are the second most important component to the development of data privacy law in the United States. Administrative agencies initially tried to address data privacy concerns by applying old laws to new situations. For example, the Federal Trade Commission Act ("FTC Act") allows the FTC to seek injunctive or other equitable relief for violations of the act's prohibition against "unfair methods of competition" and "unfair and deceptive acts or practices in and affecting commerce."[65] In several cases, the FTC

Hearing on 22/23 February, 2000, *at* http://www.europarl.eu.int/hearings/20000222/libe/subject/default_en.htm#3.

[62] *See, e.g.,* Michael Bazely, *Privacy Bill Undercuts State Law*, THE MERCURY NEWS, Oct. 28, 2003, *at*: http://www.bayarea.com/mld/mercurynews/business/7121447.htm.

[63] *See id.* Shortly before the proposed changes to the FCRA reached the U.S. Senate, California passed a strict and comprehensive financial-privacy law. The federal law preemption provision of the U.S. Constitution would replace California's scheme with the new, less protective federal law.

[64] *See id.*

[65] Federal Trade Commission Act, 15 U.S.C.A § 41 *et seq.*

applied the broad provisions of this act to ensure that companies upheld their privacy promises to consumers.[66]

The current state of data privacy jurisprudence in the U.S. federal courts is rather inconsistent. The Supreme Court has ruled on privacy issues in situations such as journalism, advertising, and solicitation, but has not addressed the matter of consumer data privacy per se.[67] In particular, the Supreme Court has yet to address whether the First Amendment protects a company's ability to process or sell personal data. In *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*,[68] the Supreme Court established a four-pronged test to balance the protection of commercial speech and the rights of individuals. Unfortunately, this test involves a highly fact-specific inquiry which can produce varying results in different cases. Since the Supreme Court only grants certiorari to a limited number of cases, often the matter is left to the federal Circuit Courts, which are split on whether to resolve the balance in favor of First Amendment or the right to privacy.

In *Florida Bar v. Went For It, Inc.*,[69] the Supreme Court applied the Central Hudson test and upheld the Florida Bar's mandatory 30-day waiting period before an attorney can directly solicit business from an accident victim or his family. The Court held that the Florida Bar's restriction withstood the intermediate level of constitutional scrutiny given to commercial speech, because the privacy of the victim and his family outweighed the attorneys' right to solicit business during that limited period of time.[70] However, this case did not specifically address the issue of data privacy with reference to the collection and sale of personal data.

The Tenth Circuit had the opportunity to address this issue in *U.S. West v. FCC*.[71] In this case, the U.S. West telephone company challenged a Federal Communication Commission ("FCC") regulation requiring individuals to "opt-in" to allowing U.S. West to sell their data to third parties, rather than permitting the less-restrictive "opt-out" procedure.[72] The Tenth Circuit struck down this regulation on the grounds that the FCC did not properly consider U.S. West's First Amendment rights, rendering

---

[66] *See* Federal Trade Commission Online, *at* http://www.ftc.gov; *see also In re GeoCities, Inc.*, FTC File No. 9823015 (consent agreement given final approval as of February 12, 1999); In re Toysmart.com, Inc., FTC File No. 012 3214 (2002).

[67] *See, e.g.*, Florida Bar v. Went For It, Inc., 515 U.S. 618 (1995)(solicitation); Bates v. State Bar of Arizona, 433 U.S. 350 (1977) (advertising); Virginia Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976) (advertising); NY Times v. Sullivan, 376 U.S. 254 (1964) (journalism).

[68] Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557 (1980).

[69] Florida Bar v. Went For It, Inc., 515 U.S. 618 (1995).

[70] *Id.* at 635.

[71] U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

[72] *Id.* at 1228.

this regulation a potentially improper restriction on commercial speech.[73] While the regulation was not explicitly declared "unconstitutional," this decision was nonetheless quite damaging to the notion of a right to data privacy within the Tenth Circuit. U.S. West appealed the decision, but the Supreme Court denied certiorari.[74]

The D.C. Circuit reached a somewhat different result in *Trans Union v. FTC*.[75] Trans Union challenged FTC restrictions on the sale of targeted marketing lists created from consumer credit reports, and argued that the restrictions were subject to strict scrutiny because they harmed Trans Union's right to free speech.[76] The court disagreed, holding that the marketing data lists received a reduced level of constitutional protection because they did not implicate a matter of public interest.[77] In its administrative proceedings, the FTC had found that the government had a substantial interest in protecting the privacy of individuals' credit information, and that the restrictions were narrowly tailored to meet that need.[78] The D.C. Circuit agreed with the FTC's assessment, and did not review the matter on appeal.[79]

The decisions in *U.S. West* and *Trans Union* acknowledge that the sale of marketing lists constitutes a form of commercial speech that receives a lesser level of First Amendment protection than other kinds of speech.[80] One should note that the decisions apply to very specific facts, and courts could reach different results depending on the type of data processing in each case. The inconsistency of the U.S. system contradicts the intention of the Data Directive, which seeks to create a uniform guarantee of data privacy protection for European citizens, and contributes to the E.U.'s reluctance to declare U.S. privacy protection as "acceptable."

The parallel systems of the judiciary and the legislature leave data privacy laws in the United States in a state of flux. It is not surprising, therefore, that the European Union does not hold that the United States has achieved an "adequate" level of data privacy protection. Until the

---

[73] *Id.* at 1240.

[74] Competition Policy Institute v. U.S. West, Inc., 120 S.Ct. 2215 (2000) (cert. denied).

[75] Trans Union v. FTC, 245 F.3d 809 (C.A.D.C., 2001).

[76] *Id.* at 818.

[77] *Id.* The D.C. Circuit recognized that the public has an interest in these lists, as the lists inevitably contain the personal data of members of the public. In order to apply the strict scrutiny standard of constitutional protection, however, the creation of the lists must be something that provides a benefit to the public (i.e., is "of interest" to the public.) In this case, the court noted that only private companies were "interested" in creating these lists, since they were the only ones that were going to benefit from them. This is insufficient to trigger strict scrutiny review of the measure.

[78] In re Trans Union Corp., Opinion of the Commission, No. 9255, slip op. at 37-52 (Feb. 10, 2000).

[79] Trans Union v. FTC, 245 F.3d at 813.

[80] U.S. West v. FCC, 182 F.3d at 1223; Trans Union v. FTC, 245 F.3d at 818.

Supreme Court resolves the split between the Circuit Courts by addressing the issue of whether sale and transfer of personal data is protected by the First Amendment, it is unlikely the European Union will change its position on this point.

III. Methods for Transferring Data From the E.U. to the U.S.

Despite these differences, the global nature of business involves frequent data transfers between the European Union and the United States. These transfers occur in corporate settings, such as when a single company maintains offices in both locations, or in consumer situations, such as making purchases over the Internet. However, Article 25 of the Data Directive states that data cannot leave the European Union and pass to a third country that does not provide adequate data privacy protection. Since the European Union declared U.S. data privacy protections inadequate, U.S. companies must provide such protections contractually in order to receive data from the European Union. The Data Directive leaves it up to the Member States to approve or disapprove of the data transfer.[81] Currently there are two preferred methods for creating the conditions necessary to transfer data between the United States and the European Union: Individually negotiated contracts and the FTC's Safe Harbor program.

If the data transfer takes place through an individually negotiated contract, the Member State can require the companies to deposit a copy of the contract prior to the transfer, and has the final approval regarding whether or not the transfer may take place.[82] However, incorporation of the Commission's model contract clauses ensures that the contract meets the European Union's standards of data privacy protection, and prevents the Member State from stopping the transfer.[83]

A second common approach to data transfer between the European Union and the United States is through the FTC's Safe Harbor program. If the data transfer is to a U.S. company that participates in the Safe Harbor program, it is presumed that the level of data protection provided is adequate, and the transfer does not need the Member State's approval to take place.[84]

---

[81] Data Directive, art. 26(2).

[82] *Id.*

[83] Data Directive, art. 5.

[84] *See generally* FTC Safe Harbor Online, *at* http://www.export.gov/safeharbor/sh_verview.html

A. *Individually Negotiated Contracts and the Commission's Model Contract Clauses*

Private contracts provide the first common method for transferring data between the European Union and a country with inadequate data protection. Data Directive Article 26(2) permits such transfers if each individual transaction provides its own adequate safeguards, which can be accomplished by appropriate contractual clauses.[85] These clauses must include the protections required by the Data Directive, including the individual's right to access their data, to know exactly what information is being processed and in what fashion, to object at any time on "compelling legitimate grounds" to the processing of their data, and to have a judicial remedy available if these rights are violated.[86]

To help companies in third countries comply with the Data Directive's requirements, the European Commission produced several model contract clauses, approved on June 15, 2001,[87] and revised on December 27, 2001.[88] The Commission continues to review its own model clauses, as well as those proposed by countries outside the European Union.[89] These clauses are not mandatory in data transfer contracts between the European Union and the United States, but are available to simplify compliance with the Data Directive.[90] If these model clauses are present in a contract, the Member State cannot refuse the data transfer, although they still retain the authority to require the depositing of the contract prior to the transfer.[91]

The model clauses enforce the requirements of the Data Directive in several ways. First, they incorporate the definitions of "personal data" and "data processing" as defined in the Data Directive, to establish a uniform basis for transaction.[92] Second, they permit data subjects to enforce their contractual rights against data exporters as third-party beneficiaries, and against data importers if the exporters are unavailable.[93] The data subject retains the right to choose whether they wish to enforce

---

[85] Data Directive, art. 26(2).

[86] *See, e.g.,* Data Directive, arts. 8 and 12.

[87] Commission Decision 2001/497/EC of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under the Directive 95/46/EC, 2001 O.J. (L 181) 19.

[88] Commission Decision 2002/16/EC of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC, annex (hereinafter "Model Clauses").

[89] *See* Information on Model Contract Clauses Online, *at* http://europa.eu.int/comm/internal_market/privacy/modelcontracts/new-develop_en.htm.

[90] *See* Model Contract Clauses Frequently Asked Questions Online, *at* http://europa.eu.int/comm/internal_market/privacy/modelcontracts/clausesfaq_en.htm.

[91] *Id.*

[92] Model Clauses, clause 1.

[93] Model Clauses, clauses 3, 6.

their rights through mediation or the court system.[94] If the enforcement action is pursued in court, it takes place in the Member State where the data exporter is located.[95]

The U.S. Departments of Commerce and the Treasury initially resisted these model clauses because of a concern that the clauses imposed unnecessarily burdensome requirements on U.S. companies, possibly in excess of the requirements contemplated by the Data Directive.[96] The United States hoped to establish safe harbor arrangements for sectors outside the jurisdiction of the FTC, and feared the model clauses would set the bar unnecessarily high and impede negotiation on such a program.[97] The United States also disfavored the automatic grant of jurisdiction over disputes to the exporting Member State, where U.S. companies would be subject to stricter laws than under U.S. jurisdiction.[98] This is of particular concern because of the provision that permits the data importer (the U.S. company) and exporter (the E.U. company) to be held jointly and severally liable for damages caused to the data subject.[99]

The Commission disagreed with the complaints presented by the U.S. government, and approved the model clauses anyway.[100] In particular, the Commission denied a connection between the creation of model clauses and the future negotiation of a safe harbor program for financial institutions.[101] In reality, however, these model clauses will likely set the bar for future negotiations, as it is doubtful the European Union will settle for a safe harbor program that provides less data privacy protection than the model clauses.

Looking past the power struggle between the United States and the European Union, the model clauses have many virtues for consumers. The clauses specifically set out the required data privacy protections, and contain provisions to ensure that individuals have recourse if their data privacy rights are violated. Without the stipulations concerning jurisdiction and liability, individuals could find themselves unable to enforce their rights in a court of law due to technicalities. This is problematic from the personal perspective of the consumer, and also because the

---

[94] Model Clauses, clause 7.

[95] *Id.*

[96] *See* Letter to the Commission from the U.S. Department of Treasury, *at* http://europa.eu.int/comm/internal_market/privacy/docs/clausexchange/letterustreasury_en.pdf.

[97] *Id.*

[98] Commission Decision 2001/497/EC of 15 June 2001, *supra* n. 87, recital 17.

[99] *Id.* at recital 18.

[100] *See* Letter from the Commission to the U.S. Departments of Treasury, *at* http://europa.eu.int/comm/internal_market/privacy/docs/clausexchange/replyustreasury_en.pdf.

[101] *Id.*

Data Directive requires that individuals must have a right of action against a company that violates their data privacy rights.[102]

Individually negotiated contracts are not an ideal solution for smaller companies, who may lack the resources for complex, international contract negotiation. While the model clauses aid compliance with the Data Directive, they do not address the myriad of other business issues present in such a contract. In response to this problem, the U.S. Federal Trade Commission ("FTC") developed the Safe Harbor program discussed below. The Safe Harbor, however, is not a complete replacement for these individually negotiated contracts. A number of important business sectors fall outside the jurisdiction of the FTC, including telecommunications and finance, and as such, companies in these excluded sectors cannot participate in the Safe Harbor program.

B. *The FTC's Safe Harbor Program*

Rather than forcing companies to contract for each separate data transaction, the European Commission and the U.S. Federal Trade Commission jointly established a Safe Harbor program.[103] This program is designed to safeguard individual data privacy and allow for the efficient yet secure transfer of data between the European Union and the United States. Compliance with the Safe Harbor is accepted as the equivalent of compliance with the Data Directive.

The Safe Harbor is a voluntary program that establishes requirements for U.S. companies handling personal data. Specifically, the Safe Harbor requires adherence to seven principles: (1) Notice to individuals about an organization's data collection practices; (2) The ability for individuals to "opt-out" of such collection practices, and to "opt-in" in the case of "sensitive information;" (3) Certain responsibilities of data-collecting organizations regarding the onward transfer of such data to third parties; (4) Obligations regarding the security and integrity of data collected; (5) The ability of individuals to access information collected about themselves; (6) The relevance of the personal information collected to the purpose for which it is used; and (7) Enforcement procedures.[104]

A company must follow two steps to join the Safe Harbor: First, the company must publicly certify its adherence to the Safe Harbor. Second, it must establish a three-step compliance program, which can either be a general private-sector program or the company's own individual program. The company enacts its own Safe Harbor compliance, and the FTC monitors the company's adherence. Currently, only companies that fall under the FTC's jurisdiction can participate in the program, thereby

---

[102] Data Directive, art. 22.

[103] *See generally* FTC Safe Harbor Online, *at* http://www.export.gov/safeharbor.

[104] *See generally* FTC's Safe Harbor Web site *at* http://www.export.gov/safeharbor/sh_overview.html.

excluding important business sectors such as financial services and telecommunications.

Participation in the Safe Harbor also guarantees U.S. jurisdiction over any dispute arising from the data handling practices. This component of the Safe Harbor is attractive to U.S. companies, particularly since much of the U.S./E.U. data transfer takes place on the Internet, where the issue of jurisdiction has not yet been resolved.[105] The FTC maintains a Web site for the Safe Harbor, which contains the names of each company that has achieved Safe Harbor certification. Thttp://www.export.gov/safeharbor.he FTC views each company's presence on this list as an affirmative obligation to meet Safe Harbor requirements, which is actionable if violated.[106]

Participation in the Safe Harbor also guarantees that disputes will be resolved by the FTC.[107] The FTC has authority to sue a company that misrepresents its data-handling practices to the public, but whether it has an affirmative obligation to do so is unclear.[108] Commissioner Thompson of the FTC stated that this statutory jurisdiction would provide the basis for government action against any U.S. company that held Safe Harbor certification but failed to abide by the requirements.[109]

IV. Enforcement of the Safe Harbor

As of this writing, there have not been any official complaints from the European Union about Safe Harbor violations by U.S. companies. However, the Safe Harbor relies on a complicated set of rules, and violations could be difficult for the average consumer to identify. Enforcement will likely be left up to independent investigations conducted by the FTC. Such investigations have increased in number in the past few years, although it is not always clear how the FTC detects these violations. In some instances, data privacy advocacy organizations such as the Electronic Privacy Information Center (EPIC) monitor various data privacy practices on their own, and report possible violations to the FTC.[110]

Despite the lack of official Safe Harbor complaints, FTC Commissioner Thompson identified several cases that will guide the FTC in han-

---

[105] *See, e.g.,* Cherie Dawson, *Creating Borders on the Internet: Free Speech, The United States, and International Jurisdiction*, 44 Virginia J. Int'l L. 637 (Winter 2004).

[106] *See US/EU Safe Harbor Agreement: What it is and What it Says About the Future of Cross Border Data Protection* (hereinafter "Thompson paper"), at fn. 7.

[107] Thompson paper at 4. *See also Deception Policy Statement, Cliffdale Associates, Inc.,* 103 F.T.C. 110, 176 (1984).

[108] Thompson paper at 4. *See also In re Toysmart.com*, Civil Action No. 00-11341 (D.M.A. July 21, 2000); *In re GeoCities, Inc.*, Docket No. C-3849 (Final Order February 12, 1999).

[109] Thompson paper at 4.

[110] *See, e.g,* EPIC Online, *at* http://www.epic.org.

dling those cases when they arise.[111] Two cases in particular, In the Matter of Microsoft Corporation and In the Matter of Eli Lilly and Company, are likely to shape the FTC's approach to privacy violation investigations.[112] Recently, the FTC investigated another case, In the Matter of Guess?, Inc. and Guess.com, Inc., which is considered to be the third in this series.[113]

In each of the following cases, the FTC chose to undertake an independent investigation of the alleged to data privacy violations. The complaints in all three cases alleged that the companies made misleading representations in their privacy statements about the kind of personal data collected, and how that data was used and stored.[114] The FTC asserted that these statements were "false and misleading," and therefore a violation of FTCA §5.[115]

In his Privacy Policy statement, Commissioner Thompson stated that the basis for an investigation of a Safe Harbor complaint would be the same as the basis for the investigation in these cases.[116] Specifically, a company that held itself out as compliant with the Safe Harbor, when it was in fact not in compliance, would be making a "false or misleading statement" in violation of FTCA §5.[117]

The FTC settled each of these three cases, but the question remains whether the terms of the settlements provide satisfactory protection to individual privacy from the viewpoint of the European Union.[118] It is especially important to determine if the settlements provide sufficient deterrence from future violations, as well as adequate remedies for violations of an individual's rights as required by the Data Directive.

---

[111] *Id.* at 7.

[112] *Id.* at 7-8.

[113] *See Guess Settles FTC Security Charges: Third FTC Case Targets False Claims about Information Security*, *at* http://www.ftc.gov/opa/2003/06/guess.htm.

[114] *In the Matter of Eli Lilly and Company*, FTC File No. 0123260, Complaint, *at* http://www.ftc.gov/os/2002/01/lillycmp.pdf (hereinafter "Eli Lilly Complaint"); *In the Matter of Guess, Inc. and Guess.com, Inc.,* FTC File No. 0223260, Complaint, *at* http://www.ftc.gov/os/2003/06/guesscmp.htm (hereinafter "Guess Complaint"); *In the Matter of Microsoft Corporation*, FTC File No. 0123240, Complaint, *at* http://www.ftc.gov/os/2002/08/microsoftcmp.pdf (hereinafter "Microsoft Complaint").

[115] *Id.*

[116] Thompson paper, at 7.

[117] *Id.*

[118] *In the Matter of Eli Lilly and Company*, FTC File No. 0123260, Agreement, *at* http://www.ftc.gov/os/2002/01/lillyagree.pdf (hereinafter "Eli Lilly Agreement"); *In the Matter of Guess, Inc. and Guess.com, Inc.*, FTC File No. 0223260, Agreement, *at* http://www.ftc.gov/os/2003/06/guessagree.htm (hereinafter "Guess Agreement"); *In the Matter of Microsoft Corporation*, FTC File No. 0123240, Agreement, *at* http://www.ftc.gov/os/2002/08/microsoftagree.pdf (hereinafter "Microsoft Agreement").

A. *In the Matter of Microsoft, Inc.*

In 2002, the Federal Trade Commission investigated Microsoft, Inc. for privacy policy violations in their online "Passport" and "Passport Wallet" services.[119] These violations were brought to the FTC's attention by a coalition of consumer groups led by the Electronic Privacy Information Center (EPIC).[120] In the complaint, the FTC alleged that in the "Microsoft .NET Passport Q&A" section of its Web site, Microsoft made false representations about the privacy provided to individuals' collected personal data.[121]

Specifically, Microsoft represented that the personally identifiable information collected through the Passport service was limited to e-mail, name, telephone number, credit card information, and billing and shipping addresses. The FTC alleged that Microsoft falsely represented this as the only personally identifiable information collected. In fact, Microsoft also collected a personally identifiable record of sites to which the Passport user logged in, dates and times of the sign-ins, and which customer service representative linked to a user's name in order to respond to a user's request for service. The FTC alleged this was a violation of FTCA §5(a) because the privacy statements made in the "Microsoft .NET Passport Q&A" section were misleading with respect to the type of personally identifiable information collected.

The FTC and Microsoft reached a settlement in this case, so it never proceeded to adjudication.[122] The settlement requires that Microsoft not misrepresent the following information in the future: The nature of all "personally identifiable information" that Passport collects from consumers; the extent to which Passport maintains, protects, or enhances the privacy, confidentiality, or security of any personally identifiable information; the treatment of previously collected personal information in the event of changes in the privacy policy terms; and any other matter regarding the collection, use, or disclosure of personally identifiable information.[123]

The settlement defines "personally identifiable information" as including, but not limited to, the following: First and last name; home or other physical address, including street name and name of city or town; e-mail address or other online contact information such as instant messaging identifier or a screen name that reveals an individual's e-mail address; telephone number; social security number; persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is

---

[119] Microsoft Complaint.

[120] *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises*, August 8, 2002, *at* http://www.ftc.gov/opa/2002/08/microsoft.htms.

[121] *In the Matter of Microsoft Corporation*, FTC File No. 0123240, Exhibit A, *at* http://www.ftc.gov/os/2002/08/mscmpexhibts.pdf.

[122] Microsoft Agreement.

[123] *Id.* at 3.

combined with other available data that identifies the individual; or any information in combination with any of the above.[124]

Microsoft must also establish and maintain, in writing, an extensive information security program. The agreement describes the factors Microsoft must consider when creating this program, and states some specific requirements the program must incorporate. The program must be monitored on a regular basis by an independent third party reviewer selected by the Associate Director for Enforcement of the FTC.[125]

Conspicuously absent from the settlement is a remedy for the individual whose privacy was violated. The agreement provides for possible civil penalties for continued or future violations,[126] but it is questionable whether these provide a legitimate deterrent. It is also unclear whether a harmed individual can bring another suit against Microsoft for the same violations, or whether the FTC's action and subsequent settlement precludes that possibility.

B. *In the Matter of Eli Lilly and Company*

The FTC also investigated the data privacy practices of Eli Lilly.[127] Eli Lilly operated several different Web sites, including EliLilly.com and Prozac.com. Eli Lilly offered a Web-based e-mail reminder service called "Medi-Messenger" for patients taking Prozac, which it operated from March 2000 to June 2001. This service collected from the user an e-mail address, a password, the text of the message they wanted to be sent, and the schedule on which they wanted the reminder sent.[128] Eli Lilly published on its Web site a detailed privacy policy addressed to users of this service, representing that the information collected from the user is protected in a highly secure fashion.[129]

On June 27, 2001, an Eli Lilly employee sent an e-mail to all recipients announcing the end of the service. The employee failed to "hide" the e-mail addresses in the message, and inadvertently disclosed the e-mail addresses of fellow subscribers to all 669 recipients.[130] This inadvertent disclosure led to a FTC investigation of Eli Lilly's data privacy practices.

The FTC alleged that, through its privacy policy, Eli Lilly represented that it took security measures appropriate for the sensitivity of the data it was storing. The e-mail address disclosure demonstrated a failure on the part of the company to properly implement security precautions for sensitive information, by failing to provide appropriate training to employees

---

[124] *Id.*

[125] *Id.* at 4-5.

[126] *Id.* at 2.

[127] Eli Lilly Complaint

[128] *Id.*

[129] *Id.*

[130] Eli Lilly Complaint, at ¶6.

and to implementing adequate checks and controls on the system.[131] Finally, the FTC alleged that Eli Lilly's failure to provide that protection rendered the statements in the privacy policy "false and misleading" and therefore in violation of FTCA §5(a).[132]

The FTC also settled with Eli Lilly, incorporating the same definition of "personally identifiable information" established in Microsoft, adjusted to exclude data of physicians, nurses, and other health care professionals that is collected in connection with that person's performance of their duties.[133] As part of their settlement, the FTC required Eli Lilly to establish and implement a similar security and privacy program to that required of Microsoft, with added precautions regarding employee training because of the error in this particular case.[134]

The other terms of the settlement agreement parallel the agreement reached with Microsoft. Although the agreement provides for possible civil penalties, it lacks explicit provisions addressing continued violations. Once again, the settlement fails to adequately provide a remedy for the violation of the individual's right to privacy as promised by the Data Directive, and it is unclear if the settlement precludes later action by harmed individuals.

C. *In the Matter of Guess?, Inc. and Guess.com, Inc.*

The most recent case that fits the pattern of a Safe Harbor violation is In the Matter of Guess?, Inc. and Guess.com, Inc.[135] Guess? Inc. ("Guess") is a fashion company that sells clothing through many avenues, including its Web site, Guess.com. To facilitate clothing purchases, the Guess site collects information from its consumers, including their names, addresses, credit or debit card numbers, and card expiration dates.[136] This collected information, along with information on the available products, is stored in tables of a database, which is in turn stored on a server. The site is designed such that consumers use a Web browser to retrieve both product information and their own personal information from the database.

Guess posted its privacy policy online, which stated that the collected data was secure and protected by an encryption system.[137] The FTC alleged that Guess failed to implement the security measures as explained in the privacy policy, specifically by failing to encrypt the data and ensure

---

131 Eli Lilly Complaint, at ¶7.

132 *Id.*

133 Eli Lilly Agreement at 3.

134 *Id.* at 4.

135 *See Guess Settles FTC Security Charges: Third FTC Case Targets False Claims about Information Security*, *at* http://www.ftc.gov/opa/2003/06/guess.htm.

136 Guess Complaint.

137 In the Matter of Guess, Inc. and Guess.com, Inc., FTC File No. 0223260, Exhibit A, *at* http://www.ftc.gov/os/2003/06/guesscmp.htm.

that it could not be improperly obtained from the outside.[138] This failure left the data open to attacks using database technology known as Structured Query Language ("SQL").[139]

In February 2002, an individual used an SQL "injection attack"[140] to obtain clear text containing the personal information stored in the tables, including customer names, credit card numbers, and addresses.[141] The FTC said this attack demonstrated the inadequacy of Guess's privacy measures and instituted an investigation of their privacy practices and representations, alleging that the information was not encrypted.[142] Additionally, the "injection attack" used to obtain the credit card numbers was a commonly known type of attack, and the database should have been designed to prevent this. The FTC alleged that, because of these violations, the privacy policy statements made on Guess.com were "false and misleading" in violation of FTCA §5(a).[143]

Just as in the Microsoft and Eli Lilly cases, the FTC and Guess reached a settlement.[144] This settlement incorporates the same definition of "personal information" as the previous two cases and similarly provides for the possibility of civil penalties for future violations, but once again fails to provide a remedy to harmed individuals.

D. *FTC Case Review Summary*

Absent from all of the settlements analyzed above are remedies for the harmed individuals. Because the FTC specifically flagged these cases as informing the approach to future Safe Harbor violations, the lack of a remedy hardly reassures the European Union that enforcement will comply with the Data Directive requirements. The actions of the FTC successfully ended these particular violations, but the settlement agreements did not explicitly address whether a harmed individual can bring a future action for personal damages. This is an important issue because, when there is an actual Safe Harbor violation, it will dictate whether individual

---

[138] Guess Complaint.

[139] Structured Query Language, or SQL, is a computer language commonly used to program and retrieve information from databases.

[140] The complaint did not provide a detailed description of the "injection attack" used to obtain the information from the database. However, it is likely the attacker logged into the database through a Web browser, just as a consumer would do to make a purchase, and then directly input SQL commands to query the portions of the database containing the unencrypted credit card information. Standard practice in the industry is to program the database such that outside users can make only limited queries (such as their own personal information or merchandise availability), for the exact purpose of preventing this type of attack.

[141] Guess Complaint.

[142] *Id.; see also* In the Matter of Guess, Inc. and Guess.com, Inc., FTC File No. 0223260, Exhibit A, *at* http://www.ftc.gov/os/2003/06/guesscmp.htm.

[143] Guess Complaint.

[144] Guess Agreement.

remedies are part of the settlement agreement, or whether individuals will be left on their own to pursue remedies after a settlement is reached.

One of the problems with providing individual remedies is the difficulty in quantifying the harm suffered. In the Microsoft case, it appears that the Electronic Privacy Information Center (EPIC) discovered the violation and brought it to the attention of the FTC before any serious harm could occur to the individuals. The FTC conducted the investigation and created a settlement designed to prevent future harm, so the lack of an individual remedy in the settlement is not entirely unexpected. If the Data Directive's remedy requirement is interpreted to mean only that individuals must be free to pursue their own remedies, then these agreements pass muster, provided that they do not preempt future action by individuals. If the Data Directive requires the settlements to explicitly provide a remedy, or if the agreements do in fact preempt future individual actions, then these standard-form settlement agreements will have to be revised by the FTC before they can apply to Safe Harbor cases.

In the Guess case, a hacker retrieved individual unencrypted credit card numbers as a result of Guess's security failure. It is not clear whether these numbers were used to make unauthorized purchases, but it is possible that consumers discovered the breach when they noticed unauthorized purchases on their cards. If this is the case, the financial harm suffered is easily quantified and remedied by providing compensation for charges that resulted from the violation. If not, or if purely financial compensation is not sufficient to satisfy the Data Directive, then the total harm actually suffered by the individuals must be determined before the FTC can provide a remedy.

Individuals suffered a very real harm as a result of Eli Lilly's disclosure of Prozac users' names, but the type of harm suffered is much more difficult to quantify. As a result, it would be hard for the FTC to make adequate provisions for those individuals in the settlement agreement. Financial compensation might be welcomed by the individuals, but is unlikely to remedy the harm to reputation or self-esteem, which is much harder to quantify than a financial loss. Additionally, since the harm suffered would vary for each individual, the FTC could not negotiate one remedy that would fully satisfy everyone. Thus, it makes sense that a remedy was not incorporated into the settlement agreement, but to satisfy the Safe Harbor, the individuals must have an opportunity to pursue a remedy on their own.

Granting individuals a right to redress is an important issue that needs to be resolved before an actual Safe Harbor violation case comes to the FTC, as it determines whether the Safe Harbor complies with the Data Directive's requirement of individual remedies. The Safe Harbor grants the FTC jurisdiction over any enforcement actions, so it seems unlikely that the individual could sue in courts to enforce their rights if the settlement fails to do so adequately. Even if it is possible, the Safe Harbor provides for U.S. jurisdiction over any disputes, so a European individual

bringing an action must face the difficulty and inconvenience of seeking a remedy in a U.S. court. Additionally, forcing individuals from the E.U. to come to the U.S. to litigate violates the terms of the Data Directive. One possible solution might be to ensure that any settlement reached in the Safe Harbor provides a remedy for individuals, but it is not clear whether this is an explicit requirement of the Safe Harbor program, or whether such an approach will be used in Safe Harbor settlements as opposed to domestic settlements.

V. Conclusion

The United States' approach to data privacy conflicts with the European Union's approach in very fundamental ways. With the creation of the Data Directive, the European Union demonstrated its clear preference for a comprehensive regime of data privacy laws, and held this to be the way to provide adequate protection for the data privacy of its citizens.

Unfortunately, U.S. efforts to create a comprehensive data privacy regime have met with minimal success so far. The U.S. Legislature is trying to establish more uniform data privacy laws on a federal level, but states generally resist these efforts. The federal courts are split on the constitutional issues surrounding data privacy protection, and this split will not be resolved until the U.S. Supreme Court gives more direction on the issue by granting certiorari to more cases. Until these points are addressed, the European Union will likely continue to regard United States privacy protection as inadequate to meet the requirements of the Data Directive.

The two common approaches to data transfer represent an interesting sort of compromise between the positions of the European Union and the United States. On one hand, in individually negotiated contracts, the Commission retained much control over the creation of the model contract clauses to be included in private contracts for data transfer. These clauses clearly address concerns such as jurisdiction and liability, and generally resolve them in favor of the European Union's approach to data privacy.

On the other hand, the United States had a heavy hand in the establishment of the FTC's Safe Harbor program. The Safe Harbor does not strictly comply with the requirements of the Data Directive, and while its terms address the same concerns of jurisdiction and liability, it resolves these concerns in favor of the United States. It also remains to be seen whether the Safe Harbor will be enforced by the FTC in a way that complies with the Data Directive.

In many ways, it seems that the compromises reached thus far have been out of necessity rather than a true desire to foster international cooperation. The large flow of data between the European Union and the United States made it necessary for the governments to cooperate and establish model contracts and safe harbors. The practical result of

strict enforcement of the Data Directive could bring many businesses to a stand-still if the flow of information across international borders were to be cut off. Regardless of which side "comes out ahead" in these arrangements, the benefit is the simplification of data transfer between the European Union and the United States.

The most important goal of all of the negotiating that takes place between the European Union and the United States, however, is to protect the rights of individual citizens. The European Union created the Data Directive to establish a uniformly high level of data privacy protection for its citizens, and as such, it very clearly defines the rights of individuals and requires a method of recourse if those rights are violated. While each government naturally wants to look out for its own best interest, decisions must be made to ensure that individuals are protected as the flow of information increases and the "world economy" develops. Jurisdiction over judicial remedies must be settled in order to protect individuals from missing the opportunity to enforce their rights due to procedural hurdles.

While the model contract clauses and the FTC Safe Harbor program differ in their details, they both substantially comply with the basic requirements set out by the Data Directive. There have not yet been any complaints about data handling, but European Union contract law and the U.S. Federal Trade Commission are poised to address enforcement issues when they arise. The enforcement of the model contract clauses and the Safe Harbor will be the true test of how well the Data Directive protects the privacy of individuals in the face of cross-border data transfers.

The European Union and the United States will continue to look out for their own best interests during future negotiations on this issue, but hopefully when the time comes to reach important compromises, they can put their differences aside and work together to ensure that companies are fulfilling their responsibilities and promises to the public.

TRACEY DILASCIO