Northwestern Journal of Technology and Intellectual Property

Volume 2
Issue 1 *Fall*

Article 5

Fall 2003

The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective

Chuan Sun

Northwestern Journal of Technology and Intellectual Property
Volume 2, Number 1 (Fall 2003)

The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective

Chuan Sun*

I. INTRODUCTION

¶1 The Internet, with the speed of its dramatic growth, is considered "an explosive economic growth opportunity that will redefine global commerce in the information age."[1] This revolutionary technology presents consumers with an "extraordinary new means to purchase both innovative and traditional goods and services, to communicate more effectively, and to tap into rich sources of information that previously were difficult to access and that now can be used to make better-informed decisions."[2] Today, millions of people access the Internet daily and many have purchased products, services, or information online.

¶2 The growth of e-commerce, however, requires consumer confidence, and privacy is a key requirement in building online consumer confidence. An increasing number of consumers are concerned with how their personal information is used in the electronic marketplace, and many consumers would rather forgo web-provided information and products than provide a website their personal information without knowing that site's information practices.[3] According to the results of a *Business Week* survey released in 1998, consumers not currently using the Internet ranked concerns about personal information and communication privacy as the foremost reason they have stayed off the Internet.[4] These findings suggest that effective and meaningful consumer privacy protections need to be implemented if the electronic marketplace is to grow significantly. Otherwise, consumers will "remain wary of engaging in electronic commerce, and this new marketplace will fail to reach its full potential."[5]

---

* J.D. candidate, Class of 2004, Northwestern University School of Law; Ph.D. candidate, Department of Communication Studies, Northwestern University.

[1] Privacy Alliance, *Before the House Subcommittee on Telecommunications, Trade and Consumer Protection of the Committee on Commerce Hearing on Online Privacy: Testimony of Ms. Christine Varney on Behalf of the Online Privacy Alliance,* 2 (Jul. 21, 1998), *available at* http://www.privacyalliance.org/resources/Varney_July_21.pdf (last visited Jan. 25, 2004).

[2] *Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web" before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce* (1998) (statement of Robert Pitofsky, Chairman, Federal Trade Commission), *available at* http://www.ftc.gov/os/1998/07/privac98.htm (last visited Jan. 25, 2004) [hereinafter *Prepared Statement of the Federal Trade Commission*].

[3] Louis Harris and Associates, Inc. and Dr. Alan F. Westin, *Commerce*, *Communications, and Privacy Online, A National Survey of Computer Users,* 20-21 (1997).

[4] *Business Week/Harris Poll: Online Insecurity*, BUSINESS WEEK, Mar. 16, 1998, at 102.

[5] *See Prepared Statement of the Federal Trade Commission*, *supra* note 2.

¶3 While the significance of privacy protection has been generally recognized, there have been broad differences among how various nations' governments formulate and implement their privacy policies and practices. Differing definitions of "privacy" have led to numerous and often inconsistent legislative schemes aiming to protect online privacy. These inconsistencies may result in conflicts among governments, and create barriers for international trade in general and e-commerce in particular.

¶4 On July 25, 1995, the European Union's Council of Ministers ("E.U. Council") formally adopted the European Union Privacy Directive ("Directive").[6] Since it became effective on October 25, 1998, the Directive has become a major concern for U.S. companies attempting to interact with existing or potential customers and employees in the European Union ("E.U."). This concern stems from the Directive's requirements that non-E.U.-based companies' privacy practices either qualify for a "Safe Harbor," or reach individual compromises with each E.U. country from which data will be extracted. These requirements have not only placed additional costs on the U.S. companies, but also placed these companies at a competitive disadvantage. The Directive also raises significant privacy policy issues for the U.S. government, whose privacy practices are more lax, resulting in rounds of negotiation between the U.S. Department of Commerce ("DOC") and the European Union in order to address these policy concerns.

¶5 This perspective focuses on the impact of this important E.U. document on U.S. commerce practices, both public and private. In particular, the perspective uses a comparative approach to study the Directive and the policy issues it imposes on the United States. In doing so, this perspective first describes the policy concerns underlying the Directive and the means by which these concerns are addressed. Next, this perspective identifies specific problems facing the United States as a result of the Directive and discusses reasons why the United States is unwilling or unable to formally adopt a privacy policy such as that reflected in the Directive. Finally, this perspective examines the Safe Harbor agreement that the U.S. government has formulated and adopted in reaction to the Directive, as well as the effectiveness of the Safe Harbor and its future in light of the recent changes in U.S. and E.U. privacy policies.

II. THE EUROPEAN APPROACH TO PRIVACY PROTECTION

¶6 When enacted in 1995, the Directive was widely considered the "most important international development in data protection in the last decade."[7] Its comprehensive public policy approach is based upon "the premise that privacy is a human right and data protection is an essential means to protect that right through a coherent and enforceable legal regime."[8] As early as 1981, the Council of Europe opened for signature and ratification a data privacy treaty intended "to secure in the territory of each Party for

---

[6] *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*, OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES OF 23 NOVEMBER 1995 NO L. 281, 31, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html (last visited Feb. 3, 2004) [hereinafter *EU Directive*].

[7] Graham Greenleaf, *The European Privacy Directive—Completed*, 2 PRIVACY L. & POLICY REP. 81 (1995), *available at* http://austlii.edu.au/~graham/PLPR_EU_1.html (last visited Jan. 25, 2004).

[8] Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L. J. 2024, 2026 (1999).

every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data."[9] This rhetoric is clearly reflected in the Directive. Article 1 of the Directive dictates that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right of privacy, with respect to the processing of personal data."[10] The Directive thus responds to the European Union's need to harmonize the previously fragmented European national data protection laws within the E.U. Internal Market, where the development of international networks brought about an enormous increase in cross-border data flows.[11]

¶7 Generally, the Directive has two overall objectives: (1) the protection of information privacy by Member States of the European Union;[12] and (2) the prevention of restrictions on the free flow of personal information among E.U. Member States, for reasons of privacy protection.[13] In other words, by establishing a clear and stable regulatory framework that requires a uniform minimum standard of privacy protection across the European Union, the Directive aims to ensure both a high level of protection for the privacy of individuals in all Member States and the free movement of personal data within the European Union.

¶8 In order to realize these two objectives, the Directive comprises a mixture of obligations for data processors who control personal data processing, together with the enforcement of individuals' rights for those who are the subject of data processing. These are reflected in a set of information privacy principles set out in Chapter II (General Rules on the Lawfulness of the Processing of Personal Data) of the Directive.

¶9 These principles cover four general areas of concern: (1) data quality, (2) legitimate processing, (3) rights of data subject and (4) security of data. The first principle, data quality, has five specific requirements:

(1) Fairness/Lawfulness: Personal data must be "processed fairly and lawfully;"[14]
(2) Purpose Limitation: Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;"[15]
(3) Relevance: Personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed;"[16]
(4) Accuracy: Personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they are

[9] *Convention for the protection of individuals with regard to automatic processing of personal data,* 20 I.L.M. 317, 317 (1981).
[10] *EU Directive*, *supra* note 6, at art. 1(1).
[11] Pearce & Platten, *supra* note 8.
[12] *EU Directive*, *supra* note 6, at art. 1(1).
[13] *Id.* at art. 1(2).
[14] *Id.* at art. 6(1)(a).
[15] *Id.* at art. 6(1)(b).
[16] *Id.* at art. 6(1)(c).

collected or for which they are further processed, are erased or rectified;"[17] and

(5) Timeliness: Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[18]

The second principle, concerning the legitimate processing of personal data, has six requirements:

(1) Consent: Personal data may be processed only if "the data subject has given his consent unambiguously;"[19]
(2) Contract: Personal data may be processed only if "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering the contract;"[20]
(3) Legal Obligation: Personal data may be processed if "processing is necessary for compliance with a legal obligation to which the controller is subject;"[21]
(4) Vital Interest: Personal data may be processed if "processing is necessary in order to protect the vital interest of the data subject;"[22]
(5) Public Interest/Official Authority: Personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in the third party to whom the data are disclosed;"[23]
(6) Legitimate Interest: Personal data may be processed if processing is "necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)."[24]

The third principle pertains to rights of the data subject, the person whose personal data is collected and transmitted. This principle secures three rights:

(1) Right of Access: Every data subject has the right to obtain from the controller "confirmation as to whether or not data relating to him are processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;"[25]
(2) Right to Correct/Block Information: Every data subject has the right to obtain from the controller "the rectification, erasure, or blocking of data, the

[17] *Id.* at art. 6(1)(d).
[18] *Id.* at art. 6(1)(e).
[19] *Id.* at art. 7(a).
[20] *Id.* at art. 7(b).
[21] *Id.* at art. 7(c).
[22] *Id.* at art. 7(d).
[23] *Id.* at art. 7(e).
[24] *Id.* at art. 7(f).
[25] *Id.* at art. 12(1).

processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;"[26]

(3) Right to Object: Every data subject has the right "to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[27]

The final principle concerns the security of the collected or transmitted personal data. The Directive requires Member States to "implement *appropriate* technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access."[28] The "appropriate" level of security is determined by balancing the nature of the data against the amount of risk involved in the processing of that data.[29]

¶10 The Directive specifies various mechanisms that aid in the implementation of these privacy principles. It requires that each Member State enact legislation to fully address and implement the Directive's four information privacy principles.[30] Further, each E.U. Member State must establish one or more public authorities to oversee and enforce privacy protections. These supervisory authorities should "act with complete independence," and must have investigative powers, "effective powers of intervention" in processing, and the power to take court action where national legislation implementing the Directive is infringed.[31]

¶11 The Directive also grants individual rights of enforcement. The Directive requires that individuals be granted the right to seek a judicial remedy for any breach of a Member State's national law regarding information privacy,[32] as well as a right to recover compensatory damages.[33] Dissuasive penalties for breach of national laws, akin to punitive damages, are also a required right for individuals, if applicable and appropriate.[34]

¶12 The Directive also encourages the formulation of codes of conduct for private self-regulation. The national supervising authorities of Member States are to issue opinions and make provisions for trade associations and other bodies as to whether they comply with national laws and the Directive.[35] In addition, the Directive establishes a supra-national administrative supervision of Member States. The supervision is distributed between three bodies: (1) the E.U. Commission; (2) a Committee of representatives of E.U. Member States (and in some circumstances, the E.U. Council itself); and (3) an advisory working party of the national data protection authorities. These supervisory bodies are responsible for monitoring Member States, recommending implementation measures, and administering opinions on the level of protection in the E.U. and in other countries.[36]

---

[26] *Id.* at art. 12(2).
[27] *Id.* at art. 14(a).
[28] *Id.* at art. 17(1) (emphasis added).
[29] *Id.*
[30] *Id.* at art. 32.
[31] *Id.* at art. 28.
[32] *Id.* at art. 22.
[33] *Id.* at art. 23.
[34] *Id.* at art. 24.
[35] *Id.* at art. 27.
[36] Greenleaf, *supra* note 7.

III. THE IMPACT OF THE DIRECTIVE ON THE UNITED STATES

¶13 The adoption and implementation of the E.U. Privacy Directive has brought about serious challenges for the United States. While both the United States and the European Union claim to be committed to safeguarding personal privacy, significant differences are apparent in terms of how this goal is to be achieved. This uncertainty has increased concerns among the U.S. business community about the impact of the Directive. Most of these concerns focus on Article 25 of the Directive, which prohibits data transfers to any country lacking an *adequate* level of protection, unless certain tightly defined exemptions apply.[37] This provision reflects the Directive's intention to ensure that the high level of protection within E.U. borders is not circumvented in cases where personal data originally collected or stored in one of Member States is processed or transmitted outside the European Union.

¶14 In the European Union's opinion, the United States does not meet the Directive's standards for the protection of privacy.[38] The prospect of U.S. businesses having to await the verdict of an E.U. regulatory body before being considered safe destinations for personal data transmission has led to suggestions that the European Union is attempting to enforce its model of data protection extraterritorially.[39] The U.S. business community has claimed that the Directive, if it is strictly enforced, may significantly disrupt trans-Atlantic trade and business planning, as well as impede the development of e-commerce.[40]

¶15 There are many examples of how this disruption of business may be manifested. For instance, a U.S. credit card company may be unable to process the financial profile of a German customer in its Chicago data processing facility. Alternatively, the purchase by a U.K. customer from the U.S.-based Amazon.com may not be completed because the customer's personal data may not be permitted to be transferred to the online retailer's website. Likewise, a U.S.-based firm will have problems trying to transfer the records of its French employee back to its New York headquarters. Similar complications will arise in various other sectors of industry where personal data is gathered, processed, and distributed transatlantically. This would include the press, educational institutions, telephone networks, health care, airlines, directing marketing, online retailers, and banking.[41]

IV. THE U.S. APPROACH: WHY THE DIFFERENCE?

¶16 While the European Union and the United States both claim to be committed to safeguarding personal privacy, there are fundamental differences between the two in terms of how to achieve this goal. The United States' unwillingness (or inability) to

---

[37] *EU Directive*, *supra* note 6, at art. 25 (emphasis added).

[38] Domingo Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 680 (1999).

[39] *See*, *e.g.*, Simon Davies, *Europe to U.S., No Privacy, No Trade*, WIRED 6.05, May 1998, *at* http://www.wired.com/wired/6.05/europe.html (last visited Feb. 9, 2004).

[40] *See*, *e.g.*, Declan McCullagh, *U.S. Twitchy on EU Data Privacy*, WIRED NEWS, Oct. 16, 1998, *available at* http://www.wired.com/news/business/0,1367,15671,00.html (last visited Feb. 9, 2004).

[41] *Id.*

formally adopt a privacy policy such as that reflected in the E.U. Directive can be attributed to several factors.

¶17 First, a cultural and historical difference between the United States and the European Union reveal different attitudes about the role of government regulation. In general, E.U. Member States have a much greater confidence in public institutions and dependence upon administrative law than does the United States.[42] Historically, the United States has been reluctant to regulate privacy and has no institutional mechanism solely responsible for privacy protection. Early efforts of privacy advocates in the United States were adamantly rejected by the majority of legislators. For instance, in the early 1970s, congressional sponsors of privacy legislation, led by Senator Samuel Ervin, Jr. of North Carolina, attempted to establish an oversight agency to monitor federal agencies' collection and use of personal information.[43] Opposition to these proposals came from various sources. For example, the interdisciplinary committee that reported to the Secretary of Health, Education and Welfare doubted that "the need exists or that the necessary public support could be marshaled at the present time for an agency of the scale and pervasiveness required to regulate all automated personal data systems."[44] The committee believed that privacy safeguards "require the establishment of no new mechanisms and seek to impose no new constraints on the application of electronic data processing technology beyond those necessary to assure the maintenance of reasonable standards of personal privacy in record-keeping."[45]

¶18 The United States has rejected all attempts to create a comprehensive set of privacy standards. Instead, Congress adopted a piecemeal approach, through narrow legislation, scattered in some specific target areas. Congress and some state legislatures have enacted isolated statutes such as the Fair Credit Reporting Act[46] and the Video Privacy Protection Act.[47] These legislative efforts only happened after the discovery of particularly scandalous practices (e.g., the use of private information to defame a political figure) and only cover the particular activities committed by specific actors, such as consumer credit reporting agencies or video rental service providers, respectively.

¶19 Furthermore, the courts have not broadly recognized a right to privacy in information held by third parties. In *United States v. Miller*, [48] the Supreme Court held that an individual has no Fourth Amendment interest to assert when the government demands access to the records an organization maintains about him or her (in *Miller*, bank records). An individual's expectation of privacy for records held by any third party is not legitimate, warranted or enforceable under the Constitution. *Miller* reduced (and possibly eliminated) judicial enforcement of the implementation of any privacy act.

---

[42] *See* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (Cornell University Press 1992).

[43] *Id.*; *see also* Harold C. Relyea, *The Privacy Act: Emerging Issues and Related Legislation*, CRS Report RL 30824, (Feb. 26, 2002), *available at* http://www.fas.org/irp/crs/RL30824.pdf (last visited Feb. 1, 2004).

[44] U.S. Department of Health, Education and Welfare*, Secretary's Advisory Committee on Automated Personal Data Systems*, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, 43 (1973).

[45] *Id.*

[46] 15 U.S.C.A. § 1681 (1970).

[47] 18 U.S.C.A. §§ 2710-2711 (1994).

[48] 425 U.S. 435, 437 (1976).

¶20 Second, the lack of external institutional control on privacy issues reflects the central U.S. model for fair information policy implementation: voluntary compliance and self-help. This model is built upon "the philosophy that self-regulation will accomplish the most meaningful protection of privacy without government interference, and with the greatest flexibility for dynamically developing technologies."[49] The theory holds that the "marketplace will protect privacy because the fair treatment of personal information is valuable to consumers; in other words, industry will seek to protect personal information in order to gain consumer confidence and maximize profits."[50] In *The Framework for Global Electronic Commerce* (known as the "Magaziner Report"), the White House stated that "the administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes."[51] It also states that "we believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation."[52] The Federal Trade Commission ("FTC") acknowledged the same concern in its privacy report to Congress in 1998. The FTC reported that "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[53]

¶21 Finally, the American approach to privacy protection is driven by business interests, as compared to the E.U.'s rights-based approach. One commentator noted that "in effect, the Magaziner Report catered to the industry of personal data rather than enshrining the participation of citizens' participation in decision about their personal data."[54] Indeed, the marketplace of personal information is big business in the United States. For example, going back to 1998, the gross annual revenue of companies selling personal information and profiles, largely without the knowledge or consent of the individuals concerned, was reported US$1.5 billion.[55]

¶22 The United States' unwillingness or inability to adopt a formal, comprehensive privacy policy akin to the Directive reflects significant cultural, historical, legislative and regulatory differences between the U.S. and the E.U. How to find compromise and formulate a mutually beneficial privacy policy remains a significant challenge to U.S. regulators, businesses and policy-makers. These efforts have already begun, as evidenced by the creation of the Safe Harbor.

V. THE UNITED STATES REACTS: THE SAFE HARBOR

¶23 Since the adoption of the Directive in 1998, the U.S. government has engaged in intense negotiations with the European Union in order to resolve their privacy policy

---

[49] Joel Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 774 (1999).

[50] *Id.*

[51] The White House, *A Framework for Global Electronic Commerce* (Jul. 1, 1997), *at* http://www.technology.gov/digeconomy/framewrk.htm (last visited Jan. 25, 2004).

[52] *Id.*

[53] Federal Trade Commission, *Privacy Online: A Report to Congress* (Jun. 1998), *available at* http://www.ftc.gov/reports/privacy3/toc.htm (last visited Jan. 25, 2004).

[54] Reidenberg, *supra* note 49, at 775.

[55] *Id.*

discrepancies. On November 1, 2000, the fruits of these negotiations, a Safe Harbor agreement, went into effect.[56]

¶24 Under the Safe Harbor agreement, a U.S. company soliciting personal data from the European Union must abide by the following seven criteria in order to receive the E.U. data: Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement.[57] These criteria are based largely upon the Fair Information Practices principles developed by the Federal Trade Commission over the past three decades.[58] Details of these criteria are as follows:

(1) Notice: Organizations must notify individuals about the purposes for which they collect and use their personal information. Organizations must provide information on how individuals may contact the organization with inquiries or complaints, the types of third parties to which it discloses the personal information and the choices and means the organization offers for limiting the use and disclosure of the information.[59]
(2) Choice: Organizations must give individuals the opportunity to "opt out"—to choose whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by that individual. For sensitive information, an affirmative or explicit "opt in" choice must be given to the individual if their information is to be disclosed to a third party or used for a purpose other than its original or authorized purpose.[60]
(3) Onward Transfer (Transfers to Third Parties): In order to disclose information to a third party, organizations must apply the Notice and Choice principles (above). Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it knows that the third party subscribes to the Safe Harbor principles or is subject to the Directive or other 'adequacy' finding. As an alternative, the organization may enter into a

---

[56] U.S. Department of Commerce, *Safe Harbor*, *at* http://www.export.gov/safeharbor (last visited Jan. 25, 2004).

[57] *Id.*

[58] Angela Vitale, *The EU Privacy Directive and the Regulating Safe Harbor: the Negative Effects on U.S. Legislation concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT'L L. 321, 338 (2002).

[59] *Safe Harbor*, *supra* note 56.

[60] The Department of Commerce does not define what "sensitive information" is, and an organization does not always have to provide opt in choice with respect to sensitive data. According to the DOC, such choice is not required where the processing is:

1) In the vital interests of the data subject or another person;
2) Necessary for the establishment of legal claims or defenses;
3) Required to provide medical care or diagnosis;
4) Carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
5) Necessary to carry out the organization's obligations in the field of employment law; or
6) Related to data that are manifestly made public by the individual.

Department of Commerce, *FAQ 1: Sensitive Data, at* http://www.export.gov/safeharbor/FAQ1sensitivedataFINAL.htm (last visited Jan. 25, 2004).

written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.[61]

(4) Access: Individuals must have access to personal information about them that an organization holds and must be able to correct, amend, or delete that information where it is inaccurate—except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of other persons would be violated.[62]

(5) Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.[63]

(6) Data Integrity: Personal information stored or transmitted must be relevant to the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current.[64]

(7) Enforcement: In order to ensure compliance with the Safe Harbor principles, organizations must have:

(a) readily available and affordable independent recourse mechanisms so that individuals' complaints and disputes can be investigated and resolved and damages awarded under applicable law or private sector initiatives;
(b) procedures for verifying that the commitments companies make to individuals adhere to the Safe Harbor principles; and
(c) obligations to remedy problems arising out of a failure to comply with the Safe Harbor principles.

Furthermore, sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations failing to provide annual self-certification letters will no longer appear in the participants list and will no longer be assured Safe Harbor benefits.[65]

The Safe Harbor agreement is followed by entities on a voluntary basis.[66] A company may implement all the restrictions of the Safe Harbor, notify the U.S. Department of Commerce that the company intends to comply with the Safe Harbor, and publicly

---

[61] *Safe Harbor*, *supra* note 56.
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] The private sector is still reluctant to implement the "Safe Harbor" principles. According to an FTC survey, only twenty percent of websites in the Random Sample that collect personal identifying information implement, at least in part, all fair information practice principles. *See* Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on "Privacy Online: Fair Information Practices In the Electronic Marketplace" before the Committee on Commerce, Science, and Transportation of the United States Senate* (May 25, 2000) (statement of Robert Pitofsky, Chairman, Federal Trade Commission), *available at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm (last visited Jan. 25, 2004).

declare compliance on its website. Alternatively, a company may develop its own self-regulatory policies, notify the DOC and publicly declare its compliance.[67] Finally, voluntary compliance may be achieved through complying with a "safety seal" program that notifies the DOC of the company's participation and ensures compliance.[68]

VI. The Effectiveness of the Safe Harbor and Its Future

¶25 At the time of this writing, the Safe Harbor has been in effect for over three years. How effectively have the Safe Harbor principles been implemented and enforced? In the aftermath of the September 11, 2001 terrorist attacks, the United States has implemented anti-terrorism measures that enable the federal government to access its citizens' data with fewer restrictions. Meanwhile, the European Union has continued tightening up its privacy regulations, as evidenced by the recent implementation of an "anti-spam" law requiring companies to get individuals' consent before sending e-mail, tracking personal data on websites, or pinpointing callers' locations via satellite-linked mobile phones.[69] How do these policy changes affect the Safe Harbor? This section addresses the effectiveness of the Safe Harbor implementation and enforcement, and its future in light of these recent U.S. and E.U. privacy policy developments.

¶26 Whether the Safe Harbor principles[70] may be effectively implemented and enforced has been a concern for both the E.U. and U.S. governments during and after the Safe Harbor negotiation process. The U.S. DOC recognizes three general limitations on the application of these principles in the Safe Harbor Preamble. First, adherence to the Safe Harbor principles may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements.[71] Second, the Safe Harbor principles may not apply when U.S. law and government regulations create conflicting obligations or explicit authorizations.[72] Third, application of the Safe Harbor principles may be limited when exceptions are permitted by the Directive or by a Member State's national law, such as where the transfer of personal data is necessary to satisfy a contractual obligation owed by the transferor to an individual.[73] Some entities were either cynical about the Safe Harbor [74] or doubted whether enough U.S. companies would voluntarily comply with it to make it effective.[75]

---

[67] Vitale, *supra* note 58, at 339.

[68] *Id.*

[69] Associated Press, *Anti-Spam Law Goes into Force in Europe* (Oct. 31, 2003), *available at* http://www.eweek.com/article2/0,4149,1369409,00.asp (last visited Jan. 25, 2004).

[70] *See infra* Section V.

[71] *Safe Harbor*, *supra* note 56.

[72] *Id.*

[73] *Id.*; *see also* Covington & Burling, *Privacy: The U.S. "Safe Harbors" to the European Union's Directive on Data Protection*, *available at* http://www.cov.com/publications/download/oid6151/211.pdf (last visited Jan. 25, 2004).

[74] For instance, Evan Hendricks, editor of *Privacy Times* and a defender of the Directive, thought that the Safe Harbor was "more political than substantial," and that the only real solution is to "have adequate privacy legislation" in the U.S, *cited in* Declan McCullagh, *Safe Harbor is a Lonely Harbor*, Wired News, Jan. 5, 2001, *available at* http://www.wired.com/news/politics/0,1283,41004,00.html (last visited Jan. 25, 2004). The law firm Covington & Burling also expressed its concern that the Safe Harbor may result in separate rules for EU citizens and the U.S. citizens, respectively. *See Safe Harbor*, *supra* note 56.

[75] For instance, Andrew Shen, an analyst at the Electronic Privacy Information Center, said, "What surprised me the most was that the companies, or associations that Commerce had there to talk up safe

¶27 One indicator of the status of the Safe Harbor implementation is the number of companies that have voluntarily complied with the Safe Harbor. From its very beginning, U.S. companies have been reluctant to volunteer. On February 1, 2001, three months into the program, only twenty companies signed up.[76] By May 1, 2001, six months into the program, the number of companies increased to thirty-nine.[77] By October 31, 2001, at the completion of one full year of the program, the certified total was 124.[78] The number grew to 225 by August 16, 2002,[79] and as of November 22, 2003, the number of overall companies signed up for the Safe Harbor only stood at 412.[80] Although the number itself does not necessarily tell the effectiveness of the Safe Harbor,[81] it is evident that the Safe Harbor implementation is at least not as effective in scope as it was expected to be after three years of implementation. Some U.S. officials had expressed hope that one hundred companies would sign up in the first month, and one thousand within the first year.[82] The current number (412 after three years) is far below that expectation, and therefore disappointing.

¶28 In February 2002, the E.U. Commission of the European Communities ("Commission") issued a staff working paper ("working paper"), which assessed the effectiveness of the implementation and enforcement of the Safe Harbor principles.[83] The Commission found that as of December 1, 2001, all of the Safe Harbor agreement's elements were in place,[84] and that it is "expected that Safe Harbor membership will continue to grow steadily."[85] The Commission also found that "individuals are able to lodge complaints if they believe their rights are being denied, but few have done so [and] no complaint so far remains unresolved."[86]

---

harbor were so reluctant to endorse it . . . but it's very obvious that the U.S. is going to have a hard time getting companies to sign up for it," *cited in* McCullagh, *supra* note 74.

[76] The U.S. Department of Commerce maintains a list of companies certified under the Safe Harbor and their dates of certification: U.S. Department of Commerce, *Web Page for Safe Harbor List, at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Jan. 25, 2004) [hereinafter *Safe Harbor List*]. The historical data used here was quoted from David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 IND. INT'L & COMP. L. REV. 265, 281 (2002).

[77] *Safe Harbor List*, *supra* note 76.

[78] *Id.*

[79] *See* E-mail from Michelle O'Neill, Deputy Assistant Secretary for Information Technology Industries, to Stefano Rodota, Chairman of the EU Data Protection Working Party, and Susan Binns, Director of the European Commission DG Internal Market Data Protection Unit (Aug. 16, 2002), *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/usg_en.pdf (last visited Jan. 25, 2004).

[80] *See Safe Harbor List*, *supra* note 76.

[81] This is because companies that choose not to join may provide adequate safeguards in other ways, for instance, through contracts or an industry Code of Conduct.

[82] *See* Castor, *supra* note 76, at n.107.

[83] *The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce*, Commission of the European Communities Staff Working Paper, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf (last visited Jan. 25, 2004) [hereinafter *EU Commission Working Paper*].

[84] *Id.*

[85] *Id.*

[86] *Id.*

¶29 However, the Commission found that a substantial number of organizations that have claimed to adhere to the Safe Harbor do not seem to be observing "the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policy."[87] In particular, the Commission found problems with respect to transparency in three aspects.

¶30 First, voluntary statements of adherence to Safe Harbor principles and/or relevant privacy policies were not systematically visible.[88] Companies must register with the Commerce Department and publicly declare their adherence to the Safe Harbor principles in order to enjoy the benefits of Safe Harbor.[89] For many organizations, no public statement of adherence to the Safe Harbor principles can be found. For a small number, even the privacy policy mentioned in the organization's self-certification could not be accessed.[90] The Commission therefore concluded that these omissions indicate that "Safe Harbor participants are in some cases falling short of what the texts require, with a resulting loss of transparency and clarity, in particular vis-à-vis the public in general."[91]

¶31 Second, it appears that privacy policies adopted by self-certified organizations do not systematically reflect Safe Harbor principles. The Commission found that "less than half of organizations post privacy policies that reflect all seven Safe Harbor Principles."[92] This fact alone was "a cause for some concern" by the Commission, as the European Union's reading of the Safe Harbor reflects that self-regulating participants must have a visible privacy policy in conformity with the Safe Harbor principles.[93] Failing to incorporate all seven principles into a privacy policy is an indication that the organization concerned "may not have understood and may not therefore be meeting the full range of their Safe Harbor obligations."[94]

¶32 Third, the Commission found that in many cases there was a lack of "clarity for individuals who might wish to exercise their rights vis-à-vis data about them held by an organization in the Safe Harbor."[95] Some organizations chose dispute resolution bodies, but did not reveal the contact information of these bodies to individuals, while others failed to inform individuals of the procedure of making complaints. Other organizations have multiple privacy policies but do not give clear guidance to individuals on which polices would apply to them. In short, there is a possibility that individuals "may not know what rules apply to the processing of their data, or how they can exercise their legitimate rights."[96]

¶33 The Commission also found problems with respect to the enforcement of the Safe Harbor provisions. The Commission acknowledged that there are a wide variety of

---

[87] *Id.*

[88] *Id.* The relevant privacy policy refers to the Commerce Department's Frequently Asked Questions (FAQs) on the Safe Harbor. *See FAQ 1: Sensitive Data*, *supra* note 60.

[89] *See EU Commission Working Paper*, *supra* note 83. Also, FAQ 6 states, "[a]ll organizations that self-certify for the Safe Harbor must . . . state in their relevant published privacy policy statements that they adhere to the Safe Harbor principles," *at* http://www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm (last visited Jan. 25, 2004).

[90] *See EU Commission Working Paper*, *supra* note 83.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

sanctions available to enforce Safe Harbor rules under dispute resolution mechanisms. However, it noticed that "not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbor rules and not all have in place privacy practices applicable to themselves that are in conformity with the Principles, as required by Safe Harbor rules."[97] This type of practice is inconsistent with the requirements of the DOC's "Frequently Asked Question number 11," which explains that Safe Harbor participants are required to choose dispute resolution bodies that provide individuals with full and readily available information about how the dispute resolution procedure works when individuals file a complaint, and that the dispute resolution mechanism's privacy practices conform to Safe Harbor principles. In other words, although enforcement is a key element in the Safe Harbor framework, if the enforcement bodies themselves do not conform to the Safe Harbor rules, it is hard (and hypocritical) to enforce the same rules for others. [98]

¶34 The E.U. working paper provides a comprehensive review of the Safe Harbor's effectiveness. Particularly, it identifies problems with regard to transparency and enforcement, two vital elements in the Safe Harbor's self-regulatory framework. In light of the E.U. assessment's findings, there are some doubts regarding the level of the effectiveness of the Safe Harbor's implementation.[99]

¶35 Policy developments on both sides of the Atlantic in the past three years also have had impacts on the Safe Harbor's effectiveness. On the E.U. side, the European Parliament and European Council continue to enhance privacy protections. In the United States, Congress adopted anti-terrorism measures after the September 11, 2001 terrorist attacks that created holes in individuals' control over their personal data and their right to protect their data's privacy. These policy developments raise important questions as to whether the Safe Harbor will continue to be effective and whether the Safe Harbor principles need to exist at all.

¶36 The E.U. Parliament and the Council of the European Union passed a new Directive on privacy and electronic communications on July 12, 2002 ("New Directive"), which went into effect on October 31, 2003.[100] This New Directive seeks to ensure an equivalent level of protection of privacy rights among Member States with respect to personal data processing in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the E.U. Community.[101] The New Directive has stringent requirements with respect to personal data processing in electronic communications that go beyond the scope of the Safe Harbor principles.

---

[97] *Id.*

[98] The Commission identified six U.S. private sector organizations that have been chosen by organizations in the Safe Harbor to operate as their dispute resolution bodies. These six organizations are: the American Arbitration Association, BBBOnline, the Direct Marketing Safe Harbor Program, Entertainment Software Rating Board Privacy Online EU Safe Harbor Programme, Judicial Arbitration and Mediation Services and TRUSTe. *See id.*

[99] *See EU Commission Working Paper*, *supra* note 83.

[100] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Eur. Consult. Assoc., *available at* http://europa.eu.int/comm/internal_market/privacy/law_en.htm (last visited Jan. 25, 2004).

[101] *Id*. at art. 1(1).

¶37 For example, the "anti-spam" provision of the New Directive requires that unsolicited communications (including communications originative from automatic calling machines, fax machines, and e-mail) for direct marketing purposes may only be made to subscribers who have given prior consent—an "opt-in" requirement.[102] If this opt-in requirement is enforced against U.S.-based direct marketing companies, adherence to Safe Harbor principles will not help these U.S. companies. The Safe Harbor "Choice" principle allows for both opt-in and opt-out approaches, but if U.S. companies choose the opt-out approach (a common practice of direct marketing businesses), they are in violation of the New Directive and subject to E.U. sanctions and/or penalties.

¶38 The impact of these new requirements on the Safe Harbor's effectiveness is significant, as the scope of the Safe Harbor framework may be expanded beyond what was intended by the European Union and the United States in their original negotiations. A potential consequence would be that an additional burden is imposed on U.S. companies involved in trans-Atlantic business transactions, forcing them to assume additional and more stringent requirements. The Safe Harbor framework never intended such a consequence, but rather was developed to address the "adequacy" requirements of the 1995 Directive.[103] If the European Union continues to pass new and stricter privacy protection rules that are to be strictly enforced against the U.S. companies, the purpose of the Safe Harbor will be defeated, and the Safe Harbor framework may be rendered moot. Already, some U.S. companies have chosen to bypass the Safe Harbor and instead have adopted E.U.-style policies and practices.[104]

¶39 On the other hand, the September 11, 2001 terrorist attacks on the United States profoundly changed the way the U.S. government handles data protection. Today, Washington is less willing to protect data than it used to be. During the Clinton administration (1992-2000), a Chief Counselor for Privacy position was housed within the United States Office of Management and Budget.[105] President George W. Bush dissolved the post upon taking office.[106] Now, the United States' top privacy officer is affiliated with the Department of Homeland Security.[107] Through the enactments of new laws and new offices, the government now has more unfettered access to a citizens' data than ever before. It is therefore not surprising that the American anti-terrorism measures clash dramatically with European privacy laws.

¶40 A key area where such a clash occurs is related to airline Passenger Name Record ("PNR") data. The U.S. Bureau of Customs and Border Protection ("CBP," formerly the U.S. Customs Service) and the Transportation Security Administration ("TSA"), pursuant to relevant federal statutes, require that foreign airlines flying into U.S. territory transfer to the U.S. administration personal data relating to the passengers and crew members

---

[102] *Id.* at art. 13(1).

[103] *See* Michelle O'Neil's email to Rodota and Binns, *supra* note 79.

[104] For example, DuPont and Proctor & Gamble have announced privacy policies that are based on EU's model. *See* David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL ST. J., Oct. 10, 2003, at A1.

[105] This position was served by Peter Swire, who is now a professor at Ohio State University Moritz College of Law.

[106] Scheer, *supra* note 104.

[107] *Id.*

flying to or from the United States.[108] Such personal data clearly falls within the protection of the 1995 Directive. Hence, any transfer of this type of data has to be made in the presence of adequate safeguards afforded by the U.S. authorities.[109] The United States tries to address concerns regarding PNR protection and its policy framework in *Undertakings of the United States Bureau of the Customs and Border Protection and the United States Transportation Security Administration* ("*Undertakings*").[110] Specifically, *Undertakings* addresses issues such as the use, treatment, and protection of PNR data by the CBP and the TSA, the treatment of sensitive data, the storage and the methods of accessing PNR data, the CBP and TSA computer system security, compliance, and the transfer of PNR data to other government authorities.[111] The United States hopes that the *Undertakings* will satisfy the requirements of the Directive or the Safe Harbor principles.

¶41 However, in a recent speech to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Frits Bolkestein, E.U. Commission member in charge of the Internal Market and Taxation, pointed out that the requisite safeguards for PNR data are not present, and that the current level of privacy protection over PNR data by U.S. authorities is not adequate.[112] Bolkestein identifies four shortcomings of the current U.S. policy regarding the PNR data. First, the Directive's "purpose limitation" is violated because the U.S. government does not want to limit its use of PNR to the fight against terrorism, but wants to extend its use to "other serious criminal offenses" and is not prepared to narrow this use further. Second, the "scope of data required" is not sufficiently narrow: the U.S. government requires thirty-nine different PNR elements, which is not proportionate to its purpose. Third, the U.S. government's data storage periods for PNR are very long (six to seven years) without adequate reason. Finally, the U.S. government's undertakings are insufficiently legally binding to satisfy the Safe Harbor or Directive principles.[113]

¶42 It is interesting to observe that while the Safe Harbor framework is readily available and has been a partially effective instrument to facilitate the data flow between

---

[108] CBP's legal authority comes from 49 U.S.C. § 44909(c)(3) (1994) and its implementing (interim) regulations, 19 C.F.R. § 122.49b, which require that each air carrier operating passenger flights in foreign air transportation to or from the United States must provide CBP with electronic access to PNR data, to the extent it is collected and contained in the air carrier's automated reservation/departure control systems. TSA's legal authority comes from the Aviation and Transportation Security Act of 2001 (ATSA) 49 U.S.C. § 44901 (2001). TSA is required to evaluate all passengers before they board an aircraft using a computer assisted passenger prescreening system. 49 U.S.C. § 44903(j)(2)(A) (1994).

[109] Press Release, European Union, Opinion of the European Data Protection Authorities on the Transfer of Passengers' Data to the United States (Jun. 17, 2003), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/2003-06-23-prn-apis_en.pdf (last visited Jan. 25, 2004).

[110] *See* U.S. Bureau of Customs and Border Protection & U.S. Transportation Security Administration, *Undertakings of the United States Bureau of the Customs and Border Protection and the United States Transportation Security Administration* (May 22, 2003) (laying out the U.S. approach on the protection of the transferred PNR data), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf (last visited Jan. 25, 2004) [hereinafter *Undertakings*].

[111] *Id.*

[112] Frits Bolkestein, EU/US Talks on Transfers of Airline Passengers' Personal Data, Address to European Parliament Committee on Citizen' Freedoms and Rights, Justice and Home Affairs, Brussels, Sept. 9, 2003, SPEECH/03/396, *available at* http://europa.eu.int (last visited Jan. 25, 2004) (on file with the Northwestern Journal of Technology and Intellectual Property).

[113] *Id.*

E.U. countries and U.S. entities, the CBP and TSA did not choose to entirely adhere to it in their *Undertakings*. Although some elements of the Safe Harbor framework were addressed in *Undertakings* (e.g., Notice, Access and Security requirements),[114] the Choice and Enforcement principles are absent from *Undertakings*. There are two potential explanations for this policy discrepancy: (1) a lack of collaboration between different U.S. government agencies (in this case, CBP/TSA and the DOC); and (2) national security needs simply trump the need for data protection, and the Safe Harbor's framework may limit the ability of CBP and TSA to effectively perform their protective duties.

¶43 The clash between U.S. Homeland Security interests and international privacy concerns implies that if the United States continues to adopt anti-terrorism measures that clash with E.U. privacy law, the effectiveness of the Safe Harbor rules may continue to deteriorate—first by the limited number of signatories and the implementation problems, then by the limited areas to which the Safe Harbor principles apply. Once again, the United States and the European Union are currently engaging in negotiation again in order to come up with a policy framework that compromises the differences of the two sides. It will be interesting to see whether the missing Safe Harbor principles will be added to the revised Undertakings.

VII. CONCLUSION

¶44 The Safe Harbor agreement between the United States and the European Union has been adopted for over three years at the time of this publication, and it has had dramatic impacts on privacy policy debate in the United States. There is evidence that U.S. lawmakers have begun to copy the essence of the Safe Harbor agreement in bills they propose. For instance, language in proposed legislation[115] reflects the objectives of the Safe Harbor and the Directive.[116] In addition, the FTC has begun to change its role in privacy protection from advocating industry self-regulation to promoting increased federal regulation. If Safe Harbor principles were mimicked in legislation, the FTC would have a heightened role in the enforcement of any new legislation because of its reliance on Section 5 of the Federal Trade Commission Act, which declares "unfair or deceptive acts or practices in or affecting commerce" to be illegal.[117]

¶45 However, the effectiveness of the Safe Harbor has been limited by both the number of companies electing to join and implementation problems relating to transparency and enforcement. The Safe Harbor as an international compromise has been further

---

[114] *See Undertakings, supra* note 110.

[115] *See*, *e.g.*, S. 2928 (the Consumer Internet Privacy Enhancement Act), 106th Cong. (2000), *available at* http://thomas.loc.gov/cgi-bin/query/C?c106:./temp/~c106reuWuM (last visited Feb. 9, 2004); H.R. 89 (the Online Privacy Protection Act of 2001), 107th Cong. (2001), *available at* http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107EZw9Ew (last visited Feb. 9, 2004); and S. 2606 (the Consumer Privacy Protection Act), 106th Cong. (2000), *available at* http://thomas.loc.gov/cgi-bin/query/C?c106:./temp/~c106VZsrtB (last visited Feb. 9, 2004).

[116] The Consumer Internet Privacy Enhancement Act, for example, makes it unlawful for a commercial website operator to collect personally identifiable information unless certain conditions are satisfied. The website must provide the user with notice that includes identification of the website operator, a list of the type of information that might be collected, etc. These requirements are strikingly similar to those requirements in the Safe Harbor agreement. *See* S. 2928, 106th Cong. §§ 2(a), 2(b) (2000), *supra* note 115.

[117] 15 U.S.C. § 45(a)(1) (2001).

weakened by the European Union's passage of a more stringent Directive on data protection in electronic communication as well as the anti-terrorism measures taken by the U.S. government after September 11, 2001. In addition, recent research has revealed that the Safe Harbor agreement has had some unanticipated negative effects on the U.S. privacy policy.[118]

¶46 There is no doubt that the E.U. privacy model has had profound impacts on the U.S. privacy policy formulation. From a civil rights perspective, it is good news that the U.S. at least is undergoing some pro-E.U. changes in its privacy protection policy. However, the privacy policy conflicts between the United States and the European Union will not likely go away. The European Union's continuing efforts to "beef up" privacy protection will inevitably clash with the United States' interests in national security and protecting its free market. What this will do to the development of e-commerce remains an issue that only can be resolved in the marketplace. One thing is for certain, however—a compromising policy framework that addresses the needs of both the European Union and United States will require innovative ideas and painstaking efforts by both sides of the Atlantic.

[118] A detailed discussion of these negative impacts of the Safe Harbor agreement is beyond the scope of this perspective. For more information with respect to this argument, *see* Vitale, *supra* note 58, at 341.