Brigham Young University International Law & Management Review

Volume 1 | Issue 1 Article 6

8-16-2005

The EU Data Protection Directive: Implementing A Worldwide Data Protection Regime and How the U.S. Position has Progressed

Seth P. Hobby

THE EU DATA PROTECTION DIRECTIVE: IMPLEMENTING A WORLDWIDE DATA PROTECTION REGIME AND HOW THE U.S. POSITION HAS PROGRESSED

INTRODUCTION

In a world where e-commerce and information technology continue to increase exponentially in global pervasiveness, and are high on the agenda of every notable and self-respecting corporation—whether large and seeking to maintain market share, or small and looking for rapid expansion—the prevailing conditions naturally amplify particular challenges that are inextricably linked to the expansion of such innovative business mediums.[1] Such large and accelerated growth is almost always closely followed by regulatory intervention of some description, as governments attempt to identify an appropriate balance between the competing aims of entrepreneurial endeavor and consumer protection. In this regard, the juxtaposition of the universal commercially linked technological swell with an equally ubiquitous awareness and focus on individual privacy,[2] inherent human rights, and corporate responsibility,[3] quickly leads to a discussion of the protection of personal data. In a technology driven economy,

---

[1] While it was previously the case that the title of "multinational corporation" was reserved for only the largest organizations with vast resources, bottomless revenue sources, and employees spread copiously around the globe, the internet generation has enabled almost any company with enough technological savvy to expand its operations to a host of countries using, almost exclusively, online capabilities. *See* Joseph J. Laferrera, *Implications of the European Union Directive on Data Protection* (Mar. 17, 2005), http://www.gesmer.com/publications/international/9.php.

[2] This is particularly so in Europe. *See, e.g.*, Douglas v. Hello! Ltd., 2003 All E.R. 110 (2003), as one of many high profile examples of cases involving individual rights to privacy, even in a celebrity context.

[3] *See, e.g.*, Nike, Inc. v. Kasky, 539 U.S. 654 (2003) (dealing with the legal relationship of corporate communications under the First Amendment, but highlighting the current climate of sensitivity between corporate behavior and fundamental human rights).

where information can be rapidly aggregated, sorted, and analyzed for an array of commercial advantages, personal information may be tantamount to gold dust to companies of virtually every field.[4] Consequently, the race is on both to collect personal information and exploit it in the corporate quest to increase the ever-sacred bottom line. Concurrently, the focus on protecting such information, for so long a peripheral aim in many countries, has been inevitably heightened; which in turn has led to the adoption of vast investigation and subsequent regulation in many countries.

If it can be argued that the United States has been at the cutting edge of technological expansion in the commercial realm, the European Union ("EU") is undoubtedly advancing the cause of data protection through regulation; the perception of the efficacy and necessity of that regulation, however, can be debated. In October 1995, the European Community adopted "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (the "Directive"),[5] laying out a comprehensive harmonizing data privacy regime to be implemented by the EU's member states within three years.[6] Although the primary goal of the Directive was to inculcate unity of data protection regulation among the states of

[4] *See* James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU–U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145 (2001) (discussing the growth of internet commerce and the background leading to the inception of the EU–U.S. Safe Harbor Agreement).

[5] Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Directive].

[6] *Id.* art. 32. Article 249 of the E.C. Treaty dictates that a Directive emanating from the European Council "shall be binding, as to the result to be achieved, upon each Member State, to which it is addressed, but shall leave to the national authorities the choice of forms and methods." EC TREATY art. 249 (ex. 189). Thus, although the principal aim of the Data Protection Directive was harmonization of the laws among member states relating to the protection of personal data, in reality, the Directive simply sets minimum standards that must be met by the states in their national implementation. As will be discussed, this in itself has caused some concern regarding the efficacy of the harmonization process. *See* EUROPEAN COMMISSION, REPORT FROM THE

the Union (then numbering fifteen),[7] certain provisions contained within the Directive dealing with data transfers to countries outside of the EU have an absolute impact on the data protection policies of every nation that trades with an EU member.[8] In essence, the Directive prohibits transfers of personal data[9] from an EU member state to any non-member nation that does not engender an "adequate level of protection."[10] Consequently, given that at the inception of the Directive no single nation in the world had a data protection framework even remotely close to that required by EU's mandate, such a requirement automatically injected the international community with a dose of insecurity over its future trade potential with the EU.

When considered in a broad global context, it is hard to avoid the feeling that the EU's implementation of such a wide sweeping regulatory exercise in the realm of fundamental human rights[11] goes too far by effectively creating a worldwide data privacy regime utilizing the proverbial back door. Particularly in nations such as the United States, which have historically taken a fundamentally

---

COMMISSION, COM(03)265 final at 11–12 [hereinafter FIRST REPORT]. Nevertheless, even where a member state fails to adopt appropriate national legislation within the time limit specified by a directive, the provisions of the directive, insofar as reasonably possible, will under certain circumstances have direct effect (as distinct from direct applicability) on individuals wishing to use the provisions of the directive in an action against the state. Furthermore, citizens that have suffered loss as a result of the member state's failure to implement a directive may have a right of action for damages against the state. For a general discussion of the direct effect of directives on member states and their citizens, see A.M. ARNULL ET AL., WYATT & DASHWOOD'S EUROPEAN UNION LAW 89–104 (4th ed. 2000) [hereinafter ARNULL].

[7] And potentially the three European Economic Area member countries: Norway, Lichtenstein, and Iceland.

[8] *See* Directive, *supra* note 5, arts. 25–26.

[9] *See id.* art. 2(a) (defining "personal data" as "any information relating to an identified or identifiable natural person").

[10] *Id.* art. 25. For a discussion of the parameters required by the Directive to meet the adequate protection threshold, see *infra* Part III.A.

[11] *See id.* art. 1(1).

different approach on privacy regulation,[12] the EU's approach may have been hard to swallow. Knowing that no country, even the commercial powerhouse that is the United States, can afford to abrogate international trade with a commercial block as large (both geographically and economically) and potentially valuable as the EU,[13] there is, in practical terms, very little choice other than to find a way to comply with the European regime.[14] Consequently, there is a generic feeling among those entities who collect and transfer data and those who necessarily keep a watchful eye on trade regulation, that the EU has instituted an unadulterated global policy for data protection, spreading its tentacles far beyond its own borders, and taking a sizeable bite out of the national sovereignty of every nation that wishes to deal with the EU.

At least on their face, the EU's motivations for including the international transfer restrictions seem legitimate.[15] The EU has alluded to the need for international compliance with equivalent protectionist policies for data protection, in order that the "high standards of data protection established by the Directive [not be] undermined, given the ease with which data can be moved

---

[12] U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR WORKBOOK, *available at* http://www.export.gov/safeharbor/sh_workbook.html (last visited Apr. 6, 2005) (discussing the sector-driven ad hoc approach to privacy regulation) [hereinafter SAFE HARBOR WORKBOOK].

[13] In 2002, the United States had approximately $379 billion of trade with the EU, including a significant portion of electronic commerce, which substantially drives cross-border flows of information regulated by the Directive's provisions. *See id.*

[14] Several countries have already embarked on a complete overhaul of their respective privacy regulations, including Australia, Argentina, and Canada. *See* James A. Harvey & Kimberley A. Verska, *What the European Data Privacy Obligations Mean for U.S. Businesses*, http://www.gigalaw.com/articles/2001-all/harvey-2001-02-all.html (last visited Apr. 6, 2005). As will be discussed, however, even such directive measures have not been entirely successful in placating the European regulatory juggernaut. *See infra* notes 78–81 and accompanying text.

[15] *See* DATA PROTECTION IN THE EUROPEAN UNION 12, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/guide/guide-ukingdom_en.pdf (last visited Apr. 6, 2005) [hereinafter DATA PROTECTION].

around international networks."[16] While this assertion is hard to dispute from a realistic standpoint—particularly considering the widely known difficulties of enforcing international "law" in any arena—it is equally difficult to submit to the concept that the regulation of personal data processing needs to be so broad and regimented in the first place. This is particularly evident when one considers that most countries appear to have been generally satisfied with their current regimes, whether regulatory or industry-based. As such, one is tempted to suggest that if the EU cannot effectively restrict the extraneous impact of its regulatory endeavors, perhaps it needs to avoid such complex and far-reaching regimes. As the EU should well understand in light of its own ongoing internal member state wrangling over issues of sovereignty,[17] no country likes to feel the downward pressure of being dictated to concerning issues that may have significance in terms of a nation's ability to regulate its own affairs, ergo national sovereignty, simply by virtue of economic leverage.

Despite the wide ranging enforcement capabilities that the Directive provides to the EU and its member states, there are concerns that such measures may be unnecessarily attempting to hold back a tank with a pellet gun. The result of the EU's legislative exploits, in this complicated and extremely broad area, may be nothing more than increased compliance costs and additional red tape for corporations earnestly engaged in business on an international scale, while those

[16] *Id.*

[17] For a general discussion of the conflict between EU law supremacy and the conservation of national sovereignty, see ARNULL, *supra* note 6, at 151–68.

at whom the Directive is really aimed get lost among the tide of attempted enforcement.

This paper looks at the background to the formation of the European data protection regime, its ostensibly limitless application, and the extent to which its ramifications indirectly regulate international trade and international data privacy policy, with a particular emphasis on the dealings between the United States and the EU. The United States as a whole has not been designated as a country providing blanket "adequate protection" through an existing or subsequently implemented privacy regime. On the other hand, there are only a few nations that have been afforded such status. However, the United States is the only nation to date to effectively conduct negotiations with the EU and reach a satisfactory compromise regarding alternative methods of meeting, or at least circumventing, the strict requirements of article 25 governing third party cross-border information flows. For its trouble, the United States has been placed under the microscope of European Commission scrutiny in its fulfillment of the agreed obligations, perhaps, partially at least, in recognition of the common perception that bringing the United States on board fully will eventually lead to closer compliance with the EU regime by other countries.

BACKGROUND AND IMPLEMENTATION

The EU has developed an almost sinister reputation for entering into regulatory pursuits that, despite generally genuine concerns underlying the conception of the endeavors,[18] often leave outsiders perplexed as to the EU's

[18] Often regulations are motivated by countries lobbying to protect what they see as something economically beneficial to them that may be diluted without the imposition of formal regulations. Such was the

justifications for its actions, causing speculation as to what the EU could possibly be dreaming about regulating next. Often, the EU is perceived, even by the citizens of its own member states, as a faceless bureaucratic institution that concerns itself with such matters such as how straight a banana should really be to be considered marketable, and whether chocolate of a certain constitution can really be called chocolate.[19] Such measures, although generally engendering legitimate concerns despite their facially absurd nature, have certainly not always been received with open arms as individual nations have struggled to maintain the balance of European solidarity with the often citizen-driven need to preserve at least some semblance of national sovereignty and independence.

Moreover, such matters have at times thrown the EU into trade disputes with individual nations, including the United States. In addition, broad-sweeping EU-wide measures have at times violated or placed the EU in danger of violating[20] its obligations under agreements with such international bodies as the WTO.[21] The impetus for the imposition of the EU's data protection regime, however, was in keeping with two of the quintessential goals of the community:

---

case with chocolate, with countries such as Belgium seeking to preserve the "purity" of the chocolate designation. *See* John T. Rourke & Mark A. Boyer, *When is a Banana a Banana?*, http://highered.mcgraw-hill.com/sites/007248179x/student_view0/chapter7/a_further_note_2.html (last visited Apr. 6, 2005).

[19] *See* Council Directive 2000/36, 2000 O.J. (L 197) 19–25; *see also* Rourke & Boyer, *supra* note 18.

[20] Press Release, Directorate General Trade of the European Commission, EU Welcomes Suspension of US Sanctions Following Resolution of WTO Banana Dispute (July 1, 2001), *available at* http://europa.eu.int/comm/trade/miti/dispute/bana.html.

[21] *See* Eric Shapiro, Note, *All Is Not Fair in the Privacy Trade: The Safe Harbor Agreement and the World Trade Organization*, 71 FORDHAM L. REV. 2781 (2003); *see also, e.g.*, World Trade Organization, *EC, United States Accept Ruggiero Compromise on Banana Dispute* (Jan. 29, 1999), *at* http://www.wto.org/english/news_e/news99_e/dsweb.html; Press Release, European Union, European Commission Takes Steps to Adapt Banana Import Regime to Enlargement (Mar. 5, 2004), *at* http://www.eurunion.org/news/press/2004/20040039.html; Aaron Lukas, *Yes, We Sell No Bananas*, *at* http://www.freetrade.org/pubs/articles/al-12-2-98.html (last visited Mar. 16, 2005).

(1) to promote an internal market consisting of absolute free trade between the members of the Community; and (2) to protect fundamental human rights on a variety of levels, particularly the right to individual privacy.[22]

The Need for Data Protection Regulation Harmonization in the EU

Protection of personal data is nothing new in the European context. In 1970, beginning with the German state of Hesse, European nations began to be cognizant of the potential for abuse of information privacy, particularly as technology continued to evolve. Consequently, many nations gained data protection momentum and began enacting regulations to combat what was perceived as a serious threat to individual liberties. This has consistently been one of the keystones of the European Community foundation, and was equally present in many individual nations.[23] Not surprisingly, as new and innovative protectionist methods were adopted in the EU's various member states, significant differences inevitably ensued. Implementation of these ad hoc national measures commonly included provisions regulating, or even prohibiting, transnational data flows, where adequate protection of personal data was not existing or forthcoming. The disparity among nation states provided a conduit for high level discussion that eventually led to the drafting of the Directive and the

[22] *See* Directive, *supra* note 5, art. 1; *see also* FIRST REPORT, *supra* note 6, at 3 ("Directive 95/46 enshrines two of the oldest ambitions of the European integration project: the achievement of an Internal Market . . . and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important.").

[23] *See generally* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997) (highlighting that between 1970 and 1997 most European nations, including those not associated directly with the Community, had enacted some type of data protection policy or specific statutes); *see also* Patrick J. Murray, Comment, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932, 933 (1998) (citing COLIN J. BENNETT, REGULATING PRIVACY 16 (1992)).

implementation of an overall policy aimed at stabilizing the threat to the internal market of the Community. As one Commission report, studying the potential impact of the separate regimes, suggested:

> [t]he diversity of national approaches and the lack of a system of protection at the Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross border flow of data might be impeded . . . .[24]

If the perception that led to the initial focus on data protection rights was accurate, namely a growth in technological sophistication providing simpler and more efficient methods of data collection, processing, and diverse usage, there seems little question that even the 1995 introduction of the Directive was before its time. Since the drafting of the Directive, there has been a veritable boom of technological expansion, with ever increasing numbers of consumers and businesses utilizing the internet as a primary source of operations, both retail and commercial.[25] With the understanding that the internet was designed, and is commonly referred to, as the "information superhighway," it has also emerged as the ultimate source for the effortless collection of personal data, something that has been a boon to businesses, a legitimate but often misunderstood fear of consumers, and a political nightmare for regulators. Indeed, any regular internet user will attest to the plethora of solicitations for personal information arising

---

[24] FIRST REPORT, *supra* note 6, at 3 (quoting COM(90)314 final, at 4).

[25] *See id.* at 4; *see also* FEDERAL COMMUNICATION COMMISSION, AVAILABILITY OF ADVANCED TELECOMMUNICATIONS CAPABILITY IN THE UNITED STATES, Fourth Report to Congress, *available at* http://www.ccp.ucla.edu/pages/internet-report.asp (last visited Apr. 6, 2005) (stating that forty-eight million adults in the United States use high-speed internet access in the home).

there. It appears that such rapid technological advances highlight the need for protection from the violation of an individual's informational privacy.

However, even heightened cognizance of the data protection challenges associated with the technological explosion does not automatically lead to easily managed solutions. Traditional means of legislating and regulating commercial behavior often seem ill equipped in the internet age, leading to attenuated applications of existing laws[26] and forcing lawmakers to stretch their imaginations to mold statutory constructions to fit a seemingly ethereal global community, embracing often ephemeral technologies and methods. Perhaps this was part of the impetus for the broad ranging agenda intended for implementation via the Directive.[27] Several years after the promulgation of the Directive, the European Commission admitted that

> "data explosion" inevitably raises the question of whether legislation can fully cope with some of those challenges, especially traditional legislation, which has a limited geographical field of application, with physical frontiers, which the internet is rapidly rendering increasingly irrelevant.[28]

The Commission itself is certainly aware of the difficult yet necessary task of identifying an appropriate balance between regulatory idealism and reality, and indeed is concerned about its own reputation, and the reputation of the

---

[26] *See, e.g.*, Nike v. Kasky, 539 U.S. 654 (2003) (forcing the courts to apply traditional unfair business practice laws to communications widely proliferated through internet and other technological means for which the laws were never intended).

[27] European Union materials suggest that although the Directive is "technologically neutral," the internet has specifically been considered as an important means of data transfer, particularly in relation to countries that do not meet the criteria for providing adequate protection. DATA PROTECTION, supra note 15, at 8. Thus, the tracking of internet users' personal information through the use of cookies will come under the Directive, although if information is collected in a more visible way, the user may arguably have given consent to the collection of their information. *Id.*; *see also infra* text accompanying note 45.

[28] FIRST REPORT, *supra* note 6, at 4.

Community as a whole, as it attempts to stabilize the efficacy of the Directive.[29]

With all of this as a backdrop, on October 24, 1995 the European Parliament and Council enacted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[30] In addition to a lengthy preamble, the Directive listed as its primary objective the protection "of the fundamental rights and freedoms of natural persons . . . with respect to the processing of personal data,"[31] and, secondarily, "the free flow of personal data between Member States . . . ."[32]

Enactment and Basic Provisions of the Directive

Member States were required to implement the terms of the Directive into their respective national laws within three years of the date of the enactment.[33] Significantly, despite pre-existing data protection laws in almost every nation of the Union,[34] five members failed to implement appropriate measures by the 1998 cut off date, and in late 1999, the European Commission instituted actions in the European Court of Justice (ECJ) against France,

---

[29] *See infra* text accompanying note 74.

[30] Directive, *supra* note 5. The Directive was later extended to bind the three additional members of the European Economic Area . *See* Decision 38/1999 of 25 June 1999, 1999 O.J. (L 296) 41.

[31] *Id.* art. 1(1).

[32] *Id.* art. 1(2).

[33] *Id.* art. 32.

[34] By 1995, only EU member states Italy and Greece did not have any data protection legislation in place, and this situation was the catalyst for the most difficulty in transferring data within the internal market. Since Italy and Greece were among the first to implement the Directive into national law, the free flow of information difficulties among member states were quickly vitiated, and there has apparently been no case to date of blocking data transfers between member states, something the Commission touts as a success regarding the imperatives of the Directive. FIRST REPORT, *supra* note 6, at 10. It will be interesting to note whether this successful run continues in the post-accession era of ten new nations joining the EU earlier this year.

Germany, Ireland, Luxembourg, and the Netherlands.[35] To date, however, all member states have at least some statutory based regime in place, although some states are still working on upgrading or fleshing out some of the intricacies.[36]

1. Basic provisions of the Directive.

The Directive broadly covers all processing of personal data[37] by controllers[38] or processors,[39] and anticipates the formulation of precise definitions of the conditions under which data can be processed by the member states in their national promulgation.[40] Use of data regulated under the Directive includes both private and public sector controllers, and requires them to abide by certain rules in the use of that data.[41] The general rules allowing the processing

---

[35] Press Release, European Union, Data Protection: Commission Takes Five Member States to Court (Jan. 11, 2000), *at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/00/10&format=HTML&aged=1&language=EN&guiLanguage=en; *see also* FIRST REPORT, *supra* note 6, at 3 n.1. Commencement of the actions resulted in fairly swift, but not immediate, resolution of the matters. Germany and France reported their enactments, but with an ongoing plan to upgrade their existing data protection laws, and each of these cases was closed by the Commission. Ireland gave notice of a partial compliance, but has yet to reach full concurrence. The action against Luxembourg went through the ECJ, and led to a condemnation of Luxembourg for failure to fulfill its EU obligations. *See* ARTICLE 29 WORKING PARTY, SIXTH ANNUAL DATA PROTECTION REPORT, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/2003-6th-annualreport_en.pdf (last visited Mar. 16, 2005) [hereinafter SIXTH ANNUAL REPORT]. A complete status of the implementation of the Directive is available at http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm (last visited Apr. 6, 2005). *See also* ARNULL, *supra* note 6 and accompanying text (discussing the potential direct effect of European directives).

[36] *See* STATUS OF IMPLEMENTATION OF DIRECTIVE 95/46 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm (last visited Apr. 6, 2005). In addition, the ten countries that have recently acceded to the Union, as part of their "Copenhagen criteria" all enacted data protection legislation prior to the date of accession. FIRST REPORT, *supra* note 6, at 13.

[37] Directive, *supra* note 5, art. 2(b) (This provision in particular highlights the comprehensive, all-encompassing, and potentially limitless nature of the Directive's scope, defining the "processing of personal data" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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").

[38] *Id.* art. 2(c).

[39] *Id.* art. 2(d).

[40] *Id.* art. 5.

[41] *Id.* arts. 2(d), 6.

of data require controller or processor to: (a) process such data fairly and accurately; (b) collect data only for explicit and legitimate purposes and use it accordingly; (c) collect data accurately and keep it up to date where necessary; (d) provide reasonable measures for data subjects to rectify, erase, or block inaccurate data stored about them; and (e) not keep data about any subject longer than is necessary.[42] In addition, the Directive requires member states to organize a supervisory authority, which, inter alia, must maintain a register of companies and individuals controlling data of specified types, and receive notifications from controllers enumerating its purposes and descriptions of proposed data processing.[43]

The Directive also regulates when data can be collected and used.[44] Such occasions include when: (a) the data subject has provided unambiguous consent;[45] (b) the processing is necessary to the performance of a contract involving the data subject; (c) the processing is required by a legal obligation; (d) the processing is necessary to protect an interest that is essential to the data subject's life; or (e) the data controller has a legitimate interest in doing so.[46] The

---

[42] *Id.* art. 6(a) (d).

[43] *See id.* arts. 18 21.

[44] *Id.* art. 7.

[45] Note that although this requires that the data subject agree "freely and specifically after being adequately informed" this does not necessarily mean more than acquiescence after having received such notice, as can be implied from the use of differing language in the provision relating to sensitive data. *See* DATA PROTECTION, *supra* note 15, at 7; *Cf.* Directive, *supra* note 5, art. 8(2)(a) (requiring "explicit consent" as opposed to "unambiguous consent").

[46] Directive, *supra* note 5, art. 7(a) (f). The final provision, although seemingly providing a catch-all that in practice may be manipulated by unscrupulous data controllers is vitiated by the caveat that it must be in keeping with the fundamental freedoms alluded to in article 1(1). What this means in real terms is that data controllers are responsible to validate with the supervisory processing of data that approaches grey areas, even though the ultimate arbiter of such rights, and the legitimacy of processing operations, will if necessary be determined by the courts.

Directive mandates even more stringent requirements to allow the processing of data considered "sensitive," that is, data dealing with racial or ethnic origin, political opinions, religious or philosophical beliefs, and data concerning health or sex life.[47]

In keeping with the explicit purpose of upholding and advancing fundamental human rights, data subjects are afforded specific remedial opportunities in case of grievances, subject to some necessary qualifications. For example, data subjects have the right to be informed when personal data is collected about them,[48] the right to access personal data held about them,[49] the right to object to inaccurate data held about the subject, the right to object to certain uses of the subject's personal data,[50] and the right to access information concerning automated decisions made in relation to personal data.[51] Violations and complaints regarding the processing of an individual's data can be lodged with the national supervisory authority, which has a responsibility to investigate and effect remedial measures where necessary in response to such complaints. If no satisfactory result is achieved, an individual has recourse to the courts; or if the complaint is against the member state itself, complaints can be made directly to the Commission, which must take appropriate steps to settle the matter, including taking action in the European Court of Justice if necessary.[52]

---

[47] *Id.* art. 8.

[48] *Id.* arts. 10–11.

[49] *Id.* art. 12. *But see id.* art. 13 (listing exemptions and restrictions on such rights involving such elements as national security, defense, public security, criminal investigations, and other such considerations).

[50] *Id.* art. 14.

[51] *Id.* art. 15.

[52] DATA PROTECTION, *supra* note 15, at 10–11.

Even by looking at this cursory overview of the essential elements of the regime, it can quickly be adduced that the boundaries of the Directive's application, far from being clearly defined, are potentially limitless in scope. As a consequence, there is little question that not only does the Directive burden almost anyone having any relation to business and commerce with the label of a "controller," by holding them responsible for abiding by the Directive's provisions; it is equally clear that there is virtually no chance that the European Commission or the national supervisory authorities, created by the Directive, have any viable chance of keeping up with the mandated enforcement.[53] Therefore, the Commission and the national supervisory authorities must pick their battles accordingly.[54]

---

[53] *See, e.g.*, FIRST REPORT, *supra* note 6, at 12–13. The Commission admitted that the "ubiquitous" nature of personal data makes it difficult to obtain accurate information about compliance with the law. *Id.* at 12. It did, however, submit that the evidence collated pointed to three specific underlying issues regarding compliance and enforcement: (a) supervisory authorities are under-resourced and have such an array of responsibilities as to shift enforcement procedures down the priority chain; (b) "patchy compliance" by data controllers that are unwilling to amend their existing method of operations to incorporate rules that are "complex and burdensome" when the risk of being caught is so low; and (c) a low level of knowledge among data subjects, which may be part of the catalyst for part (b). *Id.*

[54] One example that gives some insight into this observation is the direct selling industry. Companies that have operations in multi-level marketing, party-plan or other such methods of direct sales are essentially driven by hundreds of thousands of independent distributors, each of whom store information relating to his or her customers, and other related distributors (referred to as "downline" or "network"). Under the remit of the Directive, each of these distributors must annually register with the national supervisory authority by paying the standard fee, and must meet all the other obligations under the provisions of their national laws, including notifying customers and other distributors that they are storing their personal information, and providing information about the individual's rights pertaining to such information. Generally speaking, it can be presumed that few such entrepreneurs will ever expend the time, effort, and resources to comply with the provisions, and it is even more unlikely that they will ever be challenged on such non-compliance. Other commentators have noted that the logical extensions of the Directive's requirements, if taken literally, can impose "extraordinary" obligations. *See, e.g.*, Laferrera, *supra* note 1. Laferrera provides the example of an employer who keeps a list of its employee's names and telephone extensions, noting that technically it is processing data within the meaning of the Directive and therefore must obtain consent of the employee, or notify the employee any time the information is provided to a third party. *Id.* There is some evidence to demonstrate that employers are not frantically contacting their lawyers to audit every facet of their companies' data processing, an apathy that may lead to more egregious examples of data protection violations; but part of this general lethargy for businesses meeting their data protection obligations may have been spurred by the extraordinary reach of the Directive, and the tacit understanding that there is virtually no chance that national supervisory authorities could, even if they had the motivation, police or enforce the terms of the Directive to any substantial extent.

With this in mind, the results of research conducted by the Commission shed some light on some of the more interesting considerations that help to gauge public perception, and the efficacy of the Directive in making an impact on the personal data markets. For example, the Commission found that despite the Directive's requirement of apparently high standards of data privacy, 44% of survey respondents considered the standards as a minimum protection of their personal data rights.[55] Somewhat paradoxically, 81% of respondents also considered the level of awareness of individuals regarding data protection rights to be insufficient, bad, or very bad.[56] The same investigation also revealed that although there was a general acceptance among businesses of the need for data protection rights,[57] there seemed to be a general apathy towards fulfilling the obligations towards individuals when such data protection rights were exercised.[58]

2. Transfers of personal information to "third countries"—article 25 basics

Undoubtedly, the most publicized, contentious, and onerous (at least from a non-EU nation perspective) provisions contained in the Directive are those that relate to the transfer of personal data to so-called "third countries." [59] In essence, the Directive blocks all international transfers of data to countries

[55] FIRST REPORT, *supra* note 6, at 9. It is worth noting that the Commission is not to be considered as reliable as a scientifically selected survey, but it reported the public forum feedback for what it is worth, and it is committed to conducting additional research into such responses in the future. *Id.*

[56] *Id.*

[57] *Id.* (showing that almost 70% of businesses that participated in the survey concurred that data protection regulation was necessary to society).

[58] *Id.* (highlighting that more than 60% of businesses did not consider it an important function within their business to respond to requests for access to an individual's personal information. One suspects that this may be only part of the story).

[59] *See* Directive, *supra* note 5, arts. 25–26, 29.

outside of the EU, where the "third country does not ensure an 'adequate level of protection'."[60] Findings of adequacy are made by the Commission, in consultation with the Working Party established under article 29 of the Directive. Member States have an obligation to inform the Commission of countries that do not enshrine such adequate protection (although this seems redundant since transfers are not authorized on a blanket basis without the express approval of the Commission).[61] At first blush, such a rule, particularly given the scope of the data encompassed by the Directive, would seem to invite the wheels of commerce to come to a screeching halt. But as with any good rule, there are exceptions, and article 26 of the Directive contains several.

The first set of "derogations" virtually mirror those provided for the collection of data generally, but of course these same parameters must be consistent with the international level at which such transfers will operate. So, for example, a transfer to a third country may take place on condition of unambiguous consent of the data subject, but the consent must no longer be just for the collection of the processing of the personal data, but for the specific transfer to a third country that may not provide parallel treatment of personal data.[62] Other standard derogations include those for the necessary performance of a contract involving the data subject, transfers required by law, and transfers necessary to protect the interests of the data subject.[63]

---

[60] *Id.* art. 25(1).

[61] *See id.* art. 25(2) (6).

[62] *Id.* art. 26(1)(a).

[63] *Id.* art. 26.

Other than these relatively straight-forward derogations, there is a "cover the bases type exception" that basically provides for transfers to be made to third countries not supplying nationally incorporated data protection where "adequate safeguards can be adduced 'with respect to the protection of the privacy and fundamental rights and freedoms of individuals . . . .'"[64] As will be discussed, this opens up several doors of opportunity for countries that have historically taken a more "sectoral" or self-regulating approach regarding data protection, allowing such countries to obviate the need for a complete legislative overhaul in the field of data privacy. It is under this derogation that the United States managed to carve out its own unique solution for the continuance of free data sharing from EU entities to certain qualifying entities in the United States.[65] It is also the derogation provision that incited the Commission, with appropriate consultation, to craft and adopt standard contractual clauses that can be utilized by entities wishing to transfer data internationally in order to fulfill the adequate safeguards required by the derogation.[66]

III. INTERNATIONAL TRANSFERS—REGULATION, ENFORCEMENT, AND CIRCUMVENTION

The General Adequacy Requirement for Third Country Transfers

Pursuant to article 25 of the Directive, member states must ensure that transfers of personal data must take place only after a determination has been

[64] *Id.* art. 26(2).

[65] *See infra* text accompanying section C.

[66] Commission Decision 2001/497, 2001 O.J. (L 181) 19.

made that the intended nation of the recipient provides "adequate protection."[67] However, the Directive (or, for that matter, other prior or subsequent Community documents) does not provide much guidance on how adequacy is to be defined or determined, other than to state that it should be "assessed in the light of all the circumstances surrounding the data transfer" on a case-by-case basis.[68] Of course, one significant departure from this is enshrined in article 26(2), and allows member states to authorize a transfer or set of transfers to a third country not engendering adequate protection across the board where the controller "adduces adequate safeguards" with respect to the fundamental aims of the Directive.[69] This trickle-down right and responsibility of the member states would seem to provide the necessary flexibility to avoid over-encumbrance of international transactions in respect of data privacy requirements where the third country as a whole lacks adequate protection, particularly given the minute number of nations adjudged to meet the national requirement. However, the Commission has highlighted concerns over the divergence in member state implementation,[70] and the threat this poses to the aims of the Directive.[71]

---

[67] Directive, *supra* note 5, art. 25(1). A finding of adequacy may be determined based on the domestic law of the country seeking to gain such a designation or on international commitments entered into with the Commission, such as is the case with the Safe Harbor Agreement between the EU and U.S. *See infra* Section C.

[68] For a comprehensive overview and discussion of the operations and ramifications of the adequacy requirement, see Murray, *supra* note 23.

[69] Directive, *supra* note 5, art. 26(2); *see also id.* art. 1(1).

[70] *See* FIRST REPORT, *supra* note 6, at 18.

[71] *See* DATA PROTECTION, *supra* note 15, at 12 (articulating the primary fear of the Commission that without consistent application in international transfers of the high standards of data protection adopted in the Directive, the purpose of those standards would be quickly undermined given the pace at which data transfers can pervade international networks).

The Commission noted, for example, that some member states filtered the adequacy determination down to the controllers themselves with very limited control or input from the supervisory authority. This naturally has the effect of diluting the standard of the adequacy determinations and falling short of the article 25 obligations, even if controllers act in a purely legitimate or innocuous fashion.[72] On the other hand, some member states have taken the micro-management approach of requiring *all* data transfers to third countries to pass an administrative approval process, including transfers to countries and controllers already determined by the Commission to meet blanket adequacy protection.[73] The Commission has found this approach to be both onerous and unnecessary in its logistical application and equally inconsistent with the Directive's mandate to protect flows of data without unnecessary burdens.[74]

1. Findings of national adequacy to date

Under the Directive, the Commission was imbued with the power to determine, in accordance with article 25(5), that a country possesses a regime of data privacy that ensures adequate protection regardless of the identity of the controller.[75] The consequence of such a decision is that data transfers can occur between any one of the twenty-five member states and the three European

[72] FIRST REPORT, *supra* note 6, at 18.

[73] *Id.*

[74] *Id.* (stating that "[a]n overly lax attitude in some Member States – in addition to being in contravention of the Directive – risks weakening protection in the EU as a whole, because with the free movement guaranteed by the Directive, data flows are likely to switch to the 'least burdensome' point of export. An overly strict approach, on the other hand, would fail to respect the legitimate needs of international trade and the reality of global telecommunications networks . . . which is damaging for the credibility of the Directive and for Community law in general.").

[75] COMMISSION DECISIONS ON THE ADEQUACY OF THE PROTECTION OF PERSONAL DATA IN THIRD COUNTRIES, http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm (last visited Mar. 20, 2005) [hereinafter DECISIONS ON ADEQUACY].

Economic Area members, without any necessity for additional safeguards. In the post-Directive era, several countries have completed radical overhauls of their data privacy policies, some for the direct purpose of falling into line with the Directive's adequacy requirements. However, it remains that very few countries have so far qualified for an adequacy finding by the Commission.[76] To date, the Commission has issued decisions verifying the adequacy of protection in only Switzerland (in 2000), Canada (in 2001), Guernsey (in 2003), Argentina (also in 2003), and the Isle of Man (in 2004).[77]

Other countries have tried and failed to satisfy the requirements that the EU is apparently looking for before assigning an adequacy label. For example, Australia implemented its Privacy Amendment (Private Sector) Act in 2000, at least partially in response to the Directive, to bring Australia's data protection regime into line with the requirements[78] and simplify the transfer process between Australian companies and their European trading partners.[79] The EU Commission rejected the comprehensive privacy law as inadequate, much to the chagrin of Australia's Attorney-General, who vehemently disagreed and lambasted the European Union for not getting its own house in order and not recognizing or understanding the extent or efficacy of the privacy regime.[80] The

---

[76] *See id.*

[77] *Id.*

[78] *See* Harvey & Verska, *supra* note 14.

[79] *See* Attorney-General Daryl Williams, *European Data Protection Commissioner's Opinion of Australia's Privacy Law*, http://www.ag.gov.au/www/attorneygeneralHome.nsf/0/8C9464056CE8169CCA256B5A001318DF?OpenDocument (last visited Apr. 6, 2005).

[80] *See id.*; *see also* SIXTH ANNUAL REPORT, *supra* note 35, at 22 (discussing the reasons advised by the Article 29 Working Party, adhered to by the Commission, for a negative adequacy finding against Australia).

Attorney-General lauded Australia's legislation, remarking that although the Australian government would continue to work with EC officials to resolve the issue, it would not impose restrictions and requirements that unnecessarily burden businesses.[81]

It is not unreasonable to extrapolate from the current position regarding adequacy findings by the Commission that the EU may have set the bar too high, and as a consequence nations are finding it difficult to install a framework that fits their own legislative policies and theories while meeting the EU's projected requirements. Of course, one additional explanation, and one that is not without merit, is that many nations and entities within those nations simply do not understand what the EU is requiring them to do.[82] Either way, it is quite possible that what the EU is looking for is not in fact adequacy of national privacy laws, but is instead *equivalence* of national privacy laws. In that respect, given that no independent country can realistically afford to entirely forego international trade with the EU and its members, it is feasible to suggest that the EU's Directive goes beyond the regulation of its own borders and is in reality tantamount to introducing a worldwide privacy regime through the backdoor.

Nevertheless, there are available arrangements other than simply finding a way to weave national legislative policies into the EU's adequacy standard. Most notable among those, and one of the most widely discussed and monitored

---

[81] Williams, *supra* note 79.

[82] *Australian Companies Largely Ignorant of EU Data Protection Laws*, PRIVACYEXCHANGE.ORG, Mar. 22, 2001, *at* http://www.privacyexchange.org/news/archives/gpd/globdev0106.html; *see also* Murray, *supra* note 23 (describing in detail the difficulties and intricacies associated with the EU's adequacy standard, including a misunderstanding of the requirements by third countries and differing opinions within the EU).

results of the Directive to date, is the U.S. Safe Harbor Agreement,[83] which has the general purpose of allowing U.S. companies to self-certify to specific privacy policies, thus obviating the need for an adequacy determination (for which the United States certainly does not qualify), but fulfilling the identical purpose for those companies that register for the program.[84]

Standard Contractual Clauses—an Additional Option for Compliance

In addition to the two categories of general provisions allowing continuity of international transfers, the EU has also created a non-exclusive set of standard contractual clauses that can be negotiated in individual contracts for transactions that involve personal data transfers.[85] The standard clauses are simply intended to be one additional option for controllers to qualify for transfers of personal data to third countries under the Directive and ostensibly have no impact on the adequacy decisions of the Commission. Entities wishing to transfer such data can still rely on contracts already drafted and approved by national supervisory authorities, but only under rare and specified circumstances will a

---

[83] *See* DECISIONS ON ADEQUACY, *supra* note 75 (providing Safe Harbor Agreement decisions, overviews, and documents); *see also* U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR, http://www.export.gov/safeharbor/ (last visited Apr. 6, 2005).

[84] *Id.* Also worthy of note, but not discussed in detail within the scope of this paper is the agreement between the European Community and the United States, pursuant to a Commission adequacy finding, on the processing and transfer of air passenger name records (PNR), which generally makes it allowable for airlines operating out of the EU to transfer passenger data to the U.S. Department of Homeland Security to support national security measures in the wake of the 9/11 disaster. *See id.*; Press Release, European Commission, International Agreement on Passenger Name Records (PNR) Enters Into Force (May 28, 2004), *at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/694&format=HTML&aged=0&language=en&guiLanguage=en; *see also* Press Release, U.S. Department of State, U.S., EU Agree On Air Passenger Data Transfer (Dec. 16, 2003), *at* http://www.useu.be/Terrorism/USResponse/Dec1603PNRAgreement.html.

[85] *See generally* EUROPEAN COMMISSION, MODEL CONTRACTS FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES, *at* http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm (last visited Apr. 6, 2005) (providing documents dealing with the drafting, discussion, adoption, notification, and frequently asked questions regarding the Commission's standard contractual clauses for the transfer of personal data to third countries).

supervisory authority have the capacity to block transfers that seek to make use of the Commission's clauses.[86]

Notwithstanding the additional options for flexibility and compliance that the standard clauses provide, particularly for a business that does not wish to undergo a full scale investigation and revamp of its privacy policy, the plan has met with mixed reactions by commentators and practitioners.[87] Some have applauded the policy for handing businesses an option allowing them to stay out of official programs such as the Safe Harbor.[88] Meanwhile, others have cautioned against the inextricable, onerous, and perhaps unacceptable business implications that come with use of the standard clauses, such as the inclusion of data subjects as third party beneficiaries of contracts (which has varying ramifications according to local contractual principles),[89] which makes data importers subject to audit by a supervisory authority and possible restriction in the choice of applicable law and court jurisdiction.[90]

This brief overview of the basic parameters and alternatives for continued transfers under the Directive of personal data to third countries naturally leads to the issue of the U.S. response, particularly in light of the immense scale of trade between the United States and the EU.[91]

---

[86] *See id.* (discussing allowable blockages of transfers using the standard contractual clauses under circumstances such as where the clauses are not respected by the importing controller or processor, or constitute a grave risk of harm to data subjects).

[87] *See* Alexander Zinser, *The European Commission Decision on Standard Clauses for the Transfer of Personal Data to Third Countries: An Effective Solution?*, 3 J. INTELL. PROP. 24 (2003).

[88] *See generally infra* notes 92–111 and accompanying text.

[89] Zinser, *supra* note 87, at 32–33.

[90] *See id.*; *see also* Stephen H. LaCount et al., *European Union Data Protection Directive and U.S. Safe Harbor: An Employer Update* (Sept. 7, 2004), *at* http://www.nixonpeabody.com/linked_media/publications/PrveyAlert_09072004.pdf.

[91] *See supra* note 13 and accompanying text.

The EU—U.S. Safe Harbor Agreement, its Implementation, Efficacy, and Progression

1. Background to U.S. data privacy

While the European perspective on personal data has been geared towards comprehensive public intervention, with priority exclusively preserved for individual rights, the U.S. has consistently preferred a market-based or self-regulatory approach that has developed into what the Department of Commerce has described as "sectoral," with legislative solutions forthcoming to govern more sensitive areas of personal data transactions.[92] There are certainly plenty of pros and cons associated with the differing theories. From the perspective of advocates of the European doctrine, the U.S. approach leaves too much to chance in the realm of fundamental human rights, leaving individuals uninformed and overexposed to the insidious acts of more sophisticated parties.[93] From the U.S. standpoint, the sectoral approach may allow for a higher level of information flow, based firmly on First Amendment grounds, thus imbuing citizens with "significant economic and social benefits," in addition to reinforcing a "healthy distrust for governmental solutions, preferring instead reliance upon entrepreneurial and market based protections."[94] There is little doubt that such founda-

[92] *See* SAFE HARBOR WORKBOOK, *supra* note 12; *see also* Assey & Eleftheriou, *supra* note 4, at 149–50 (discussing the U.S. approach that predominantly incorporates industry norms, codes of conduct, and the consumer marketplace, and focuses only secondarily on legislative measures targeted towards specific sectors of the economy); *see also* Issuance of Safe Harbor Principles and Transmissions to European Commission, 65 Fed. Reg. 45666, 45666–67 (July 24, 2000) (stating that, "[w]hile the United States and European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation.") [hereinafter SAFE HARBOR PRINCIPLES].

[93] Assey & Eleftheriou, *supra* note 4, at 149–50.

[94] *Id.* at 150.

tional philosophical differences, at least in part, are sufficient to prevent any type of general adequacy finding by the Commission regarding the United States as a nation.

Notwithstanding these obvious differences, both the EU and the United States were highly cognizant of the significant amount of commerce between the two trading blocks that could potentially be affected by the provisions of the Directive and the interests of both parties that were at stake. Consequently, the EU and the U.S. Department of Commerce entered into negotiations to lay out a framework that would provide the requisite "adequacy" under the Directive on an individual-company or public-entity level, without the need for wholesale changes to current U.S. data privacy laws.

2. The Safe Harbor Agreement framework—basic principles

Following intense and protracted negotiations between the EU and the United States,[95] on July 24, 2000, the Department of Commerce finally issued[96]—and the EU promptly accepted[97]—the principles of the so-called Safe Harbor Agreement, heralding the beginning of a new era in U.S. personal data protection. The basic thrust of the Safe Harbor Agreement (SHA) and its principles is to provide U.S. organizations with an effective and straightforward means of transposing the Directive's data protection requirements into their

---

[95] *See* David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of the Safe Harbor's First Year*, 12 IND. INT'L & COMP. L. REV. 265, 275–76 (2002) (highlighting the fundamental disagreement between the parties regarding the best way to proceed, the request of the EU that the U.S. implement federal legislation governing the use of personal data by commercial entities, and the EU's rejection of five separate proposals by the U.S. before reaching an agreement).

[96] SAFE HARBOR PRINCIPLES, *supra* note 92.

[97] Commission Decision 2000/520, 2000 O.J. (L 21) 5, 7.

operations, thereby avoiding any concerns for both them and their EU data exporters that they will be found in violation by the EU and consequently be subject to enforcement under the Directive.[98] There are of course some important limitations in the fields of national security, public interest, conflicts with existing U.S. law, and other similarly bona fide departures.[99] The SHA is a purely voluntary scheme, but those organizations that decide to take advantage of its provisions are encouraged to "implement the principles fully and transparently," and apply the principles to all data processing and transfers following registration in the scheme.[100]

The substance of the SHA is embodied in the seven basic principles which Safe Harbor registered organizations must entrench into their policies and procedures. The principles are: notice, choice, onward transfer, security, data integrity, access, and enforcement. Furthermore, organizations must self-certify annually to qualify for the ongoing benefits of the program.[101]

Notice. The notice requirement requires organizations to inform individuals about the purposes for which information is being collected, provide contact details for the organization to facilitate complaints by data subjects, inform subjects of any third party use of the data, and make available the means to communicate to the organization choices regarding the use of the data. Notice must be clear and conspicuous, and must be provided on the front end of any data

98 SAFE HARBOR PRINCIPLES, *supra* note 92, at 45666–67.

99 *Id.* at 45666.

100 *Id.*

101 For a list of the registration requirements, see U.S. DEPARTMENT OF COMMERCE, INFORMATION REQUIRED FOR SAFE HARBOR CERTIFICATION, *at* http://www.export.gov/safeharbor/sh_registration.html (last visited Mar. 20, 2005).

transaction where reasonably practicable. Failing that, it must be provided as soon as possible thereafter.[102]

Choice. Under the choice principle, organizations must provide individuals with an opportunity to "opt out" from disclosure of their information to third parties or other data uses that are incompatible with the original purposes for which the data is collected. To facilitate this option, organizations must provide to individuals clear and readily available information and mechanisms. More stringent requirements apply to the processing of "sensitive data" as defined by the Directive, requiring a conscious "opt in" facility.[103]

Onward transfer. Onward transfer of data may only occur where the notice and choice provisions are adhered to. Most importantly, however, for the successful operation of the SHA, such transfers may only be made where that party is also registered under the SHA or is otherwise in compliance with a commensurate level of data protection, such as a written agreement binding the party to the SHA principles for that specific transaction.[104]

Security. Processors of personal data under the SHA must take reasonable steps to prevent personal data collected and used from "loss, misuse, and unauthorized access, disclosure, alteration, and destruction."[105]

Data integrity. In accordance with the Directive, the SHA requires that personal data should be relevant for the purposes for which it is collected, must

---

[102] SAFE HARBOR PRINCIPLES, *supra* note 92, at 45667.

[103] *Id.* at 45667–68.

[104] *Id.* at 45668.

[105] *Id.*

be used in accordance with the purposes for which it was collected, and should be initially authorized by the individual. Consistent with this, SHA organizations are required to ensure that the information is reliable, accurate, complete, and current insofar as necessary for the purposes of its intended use.[106]

Access. The access requirement is closely linked to the data integrity requirement. Pursuant to the requirement, individuals must be granted access to the information that an organization holds about them, and must be endowed with the ability to delete, correct, or amend such data, provided that the expense of maintaining such an operation is not unreasonably disproportionate to the rights of the individual and does not affect the rights of persons other than the individual.[107]

Enforcement. Enforcement contemplates the use of mechanisms, both public and private, to ensure compliance by those participating in the SHA. Not only must organizations annually certify, but the SHA anticipates use of federal and state law to enforce obligations, as well as the availability, designated by the organization, of an independent resolution body to handle disputes that are unresolved between the organization and the individual.[108]

Clearly, even these basic principles raise many questions regarding procedure, policy, and to what extent U.S. organizations will actually benefit by

---

[106] *Id.*

[107] *Id.*

[108] *Id.* The Federal Register entry enumerating these principles also provides a useful FAQ section, commentary, and assessments, which provide a more detailed analysis of the principles, their anticipated promulgation, derogations, concerns, and benefits. *See id.* at 45668 85. One additional point that should be made is that organizations may cordon off sectors of their data privacy operations to meet the SHA, for example in the context of human resources records, which may be far more manageable in the SHA context than a complete organization-wide overhaul.

signing up to a scheme that incorporates principles unfamiliar to many organizations and forces them to make significant changes in their information systems, the education of their workforce, and perhaps even their technological capabilities.[109] Not surprisingly then, the SHA has had, and continues to have, its critics. Some argue that compliance with its principles is too costly, unfair, and unmanageable, an argument concurrent with finger-pointing at alleged EU hypocrisy by not putting its own house in order before seeking to expand its jurisdictional power in the data privacy field far beyond its own borders.[110] With that said, the SHA has been gaining momentum as organizations have learned of its benefits, recognizing it as simply one means of ensuring unfettered continuation of personal data transfers from EU-based entities to their U.S. counterparts—certainly not the most appropriate approach for everyone, and certainly not without its flaws in conception or implementation.[111]

3. Implementation and progress of the SHA—an ongoing and imperfect tenure

Given the SHA's unique status among the responses to the EU's Directive, and no doubt due to the size and economic power of the U.S., the EU has been dedicated to ongoing scrutiny of the SHA's implementation and efficacy. Combining this paradigm with the EU's apparent paranoia[112] about its

---

[109] For a general discussion of the benefits and costs of signing onto the scheme, see Assey & Eleftheriou, *supra* note 4, at 156. The article also contains a useful discussion of what an organization should consider when deciding whether to enroll in the program, and if so, what steps must be taken at a foundational level to commence the transition to compliance with the principles. *Id.* at 156–58; *see also* Castor, *supra* note 95, at 279–86 (analyzing costs and benefits of the SHA, both actual and contemplated).

[110] Assey & Eleftheriou, *supra* note 4, at 158.

[111] *See generally* EUROPEAN COMMISSION, COMMISSION STAFF WORKING DOCUMENT, SEC (2004) 1323, [hereinafter STAFF WORKING DOCUMENT]; *see also* JAN DHONT ET AL., SAFE HARBOR DECISION IMPLEMENTATION STUDY (2004) [hereinafter IMPLEMENTATION STUDY].

[112] *See supra* note 74 and accompanying text.

reputation resulting from its indirect attempt to take the Directive around the world, it is easy to understand why the EU is so adamant that the program be carefully monitored, and that improvement and support in and from the U.S. is forthcoming. Earlier this year, as part of its ongoing investigation of the implementation of the SHA, the Commission requested a joint study be made involving the knowledge and experience of scholars from the EU, European Economic Area, and the United States.[113] This study was followed by the recent release of the Commission's second report pertaining to the "implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce."[114]

The attraction of organizations to the SHA has been far from numerically impressive in its initial years.[115] A number of reasons have been cited for this, including for instance: companies are reticent to make legal commitments that may lead to liability in the United States for the purpose of satisfying contemptuously perceived European rights problems; organizations lack understanding of the SHA, its requirements, and purposes; and, given the apparent lack of the wide-scale enforcement organizations and measures, they choose to "lay low" until such time as they *really* have to take steps to come above board.[116]

---

[113] IMPLEMENTATION STUDY, *supra* note 111.

[114] STAFF WORKING DOCUMENT, *supra* note 111.

[115] *See* Castor, *supra* note 95, at 280 (pointing out that only 124 U.S. companies had signed up for the scheme by the end of the first year, many of them small and medium-sized businesses); STAFF WORKING DOCUMENT, *supra* note 111, at 5 (discussing the continued growth of SHA registration each year and the increased protection ensuing from these registrations, but expressing disappointment at the overall number, which is less than initially anticipated, and hoping that the recommendations of the report will lead to greater pervasiveness of certifications in the future).

[116] *See* Laferrera, *supra* note 1; Assey & Eleftheriou, *supra* note 4, at 156–58; *see also* Harvey & Verska, *supra* note 14.

Furthermore, other organizations may have avoided embarking on broad upgrades to their technology and human resources facilities to meet an under-enforced standard that they know they may not be able to adequately uphold, at least in the short term.[117] Even though there are about 600 currently-registered participants of the Safe Harbor program, this number no doubt only represents a tiny fraction of the U.S. entities that process data from EU organizations. Naturally, therefore, it can be safely assumed that even though there are several alternative measures available to legitimize transfers of personal data from the EU, there are probably a vast number of U.S. companies that are choosing, at least for now, to comply only with their U.S. obligations and will deal with the EU ramifications if and when they arise. At this juncture, where enforcement mechanisms are at a minimum and a company can seemingly fly under the radar, incentives to join the Safe Harbor agreement are, temporarily it would seem, at a minimum—absent an officious EU-based entity requiring strict adherence by a U.S. transferee. However, even this seems unlikely in the face of a low percentage of enforcement among the EU member states.

Even those companies that have certified under the SHA have apparently struggled to meet even the bare minimum commitments that they have made.[118] Both the Commission Report and the implementation study noted serious deficiencies in almost every aspect of the basic principles of the SHA, with virtually no certified organizations possessing privacy policies that reflect all

[117] Harvey & Verska, *supra* note 14.

[118] STAFF WORKING DOCUMENT, *supra* note 111, at 6–8; IMPLEMENTATION STUDY, *supra* note 111, at 105–07.

seven of the SHA principles.[119] The Commission recommended several courses of action to bring organizations into compliance with the principles, including its own involvement in some of the proposed processes.[120] These included, for example: more rigorous respect for the SHA principles, with greater commitment and compliance generally by SHA companies; a more proactive stance on the part of the Department of Commerce with respect to ensuring viability of public privacy policies upon certification; more proactive monitoring by the Federal Trade Commission (FTC) in line with the "assiduousness" it had applied to spam-related matters; and increased use of power by data protection authorities (DPAs) to suspend data transfers, even to Safe Harbor-certified organizations, when there is a "substantial likelihood" of noncompliance.[121]

In addition, the Commission Report also independently examined the role of all relevant participants from the U.S. side of the SHA, including the Department of Commerce, the FTC, independent resolution bodies, and the EU DPA's, and found need for improvement in each area.[122] The Commission was at least magnanimous enough to provide suggestions for remedial action to correct those deficiencies.[123] In conclusion, the Report expressed a mix of encouragement and frustration, but the Commission was sufficiently satisfied to allow

---

119 STAFF WORKING DOCUMENT, *supra* note 111, at 8.

120 *Id.*

121 *Id.*

122 *Id.* at 9-13; *see also* IMPLEMENTATION STUDY, *supra* note 111, at 105-11 (analyzing the deficiencies the study identified in the various areas of the SHA implementation, and suggesting mechanisms for improvement and notably including clearer guidance and policing on the part of the Department of Commerce).

123 *Id.* at 13-14.

operations to continue without radical changes, simply suggesting improvement across the board.[124]

Despite the positive indications expressed by the Commission, it is difficult not to infer from the report some sense of exasperation, not necessarily directed towards the United States, but perhaps because it has become a victim of its own broad policies. Understanding that the United States is simply one jurisdiction to which the Commission inevitably must extend its data protection activities—albeit a very important one from a trade perspective, and as an exemplary nation for data protection standards—one perception is that the Commission may have stretched itself beyond capacity from a global-regulatory, or at least an enforcement, perspective. Though it is difficult to sympathize with the EU's plight, let alone empathize with it, one gets the sense that the EU desperately wants to elicit the U.S.'s full cooperation as it attempts to enforce its legislative policies outside of the traditional boundaries. Looking at that position from an objective standpoint, aside from the potential economic meltdown that may occur as a result of failure to at least facially cooperate, the proclivities associated with the need for national autonomy seem to militate against the U.S. offering its very best efforts to get the EU out of its self-imposed jam.

IV. CONCLUSION

Perceived from U.S. eyes, concerns have been expressed in a general vein regarding the desirability of allowing the EU to dictate the parameters of personal data protection regulations in a U.S. context.[125] First and foremost, it has

[124] *Id.*

[125] *See, e.g.*, Assey & Eleftheriou, *supra* note 4.

been assessed that the need for U.S. entity compliance with the Directive's principles, whether through the SHA or one of the alternatives, could leave U.S. citizens feeling like "second class citizens within their own country."[126] Furthermore, and perhaps most difficult to rebut, is the argument that by compromising sufficiently to negotiate the SHA, the United States ultimately capitulated by giving up some small part of its sovereignty to the EU.[127]

Accusations of usurping sovereign powers beyond acceptable levels is nothing new to the European Union; it is the very fight it has had with many of the individual states in its own Community.[128] The key distinction, of course, is that those nations explicitly agreed to limit their sovereignty to some extent, even if the boundaries of that relinquishment are undefined and are perhaps dynamic. But such allegations have rarely been discussed in terms of nations not within the European Community, where the institutions of the Community, at least ostensibly, have no real authority to mandate any form of regulatory regime.

Even though international law is a somewhat ethereal concept and flows to and fro with the tides of the seas that separate the nations, one general principle that stands out is that national autonomy should rarely be encroached upon by over-reaching international neighbors. One practical protection against over-reaching is that if nations do not buy into the proposed restrictions on more than a cursory level, proposed restrictions simply will not be consistently applied or enforced, despite the best efforts or intentions of the promulgator. Such is the

126 *Id.*

127 *Id.*

128 See ARNULL, supra note 6 and accompanying text.

case with the EU's data protection directive. Taken to their logical extension, the terms of the Directive span every nation, every privacy regime, and every entity within those nations. Naturally, enforcement of such broad and large-scale concepts is difficult to police to any great extent. Furthermore, with the EU evidencing scant and insufficient ability to accomplish effective regulation, even within its own jurisdiction, it seems that at least for the foreseeable future the EU has an uphill battle in taking its interventionist approach to fundamental freedoms and individual privacy around the globe. Consequently, of all the dynamics relating to the Directive that will inevitably play out in the future, consistent interpretation and enforcement of the EU's data protection regime undoubtedly remain at the heart of its potential success.

Seth P. Hobby