

Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows

Priscilla M. Regan*

George Mason University

This article explores the issues surrounding the harmonization of privacy or data protection during the last 30 years. It begins with a history of the conflict over transborder data flows and then proceeds to analyze current national and regional policy debates about the feasibility of policy solutions to address problems that are integral to global communications and economic networks. Ongoing discussions between the European Union and the United States over Safe Harbor Principles provide data for exploring these issues. The article concludes with an analysis of whether harmonization of privacy and data protection policies is likely to evolve through existing processes and institutions.

While the Internet has popularized the notion of “beyond borders” (Kahin & Nesson, 1997), the reality is that even more items of personal data are “crossing borders.” From formal applications for visas and work permits, to business transactions, to informal voice and data communications, personal information makes its way from one country to another. Some of this data flow occurs with the knowledge and possibly the consent of individuals, but much of it is in the backdrop of administrative noise to which most people do not attend. These largely invisible flows of personal information contribute to an individual’s record of personal transactions with a range of organizations including business, health care and government, as well as becoming an item in the exchanges of record systems between organizations (Branscomb, 1994).

Since the mid-1970s, most democratic countries have passed national legislation addressing the policy concerns resulting from personal information collection and use. As will be discussed below, some countries define their legislation in

*Correspondence concerning this article should be addressed to Priscilla Regan, Department of Public and International Affairs, George Mason University, MSN 3F4, Fairfax, VA 22030; [e-mail: pregan@gmu.edu].

terms of information privacy and others in terms of data protection. The underlying concern is analogous: to give individuals some rights with respect to their personal information and to require organizations to abide by some rules with respect to the handling of that information. Differences in national laws raise a consequent issue of transborder data flows. Strong privacy protections for citizens of one country may be undermined if a citizen of that country purchases a product from another country, travels to another country, or communicates by email outside the country (Schwartz & Reidenberg, 1996). The European Data Protection Directive provides the most recent example in an ongoing process of developing transnational norms about privacy or data protection in response to the problems of transborder data flows. It also illustrates the attempts of national governments to maintain the uniqueness and effectiveness of their own privacy or data protection regimes in light of the inevitable and ubiquitous flow of personal information across borders (Regan, 1993, 1999).

This article explores the evolution of transnational norms about privacy and data protection in the context of transborder data flows. I use the framework of social constructivism to help analyze the process of defining these norms. In this framework, state and non-state actors are embedded in networks of transnational and international social relations that shape interests and behavior. Social constructivism emphasizes the investigation of philosophic principles, norms, and shared terms of discourse, as well as the analysis of the processes and institutions through which these are given meaning (Finnemore, 1996; Holden, 1996). In this case, policy debates at the national and international levels have struggled over the meaning and status of privacy, as well as over the appropriate government role for protecting privacy. Is privacy, for example, a fundamental right? What does it mean for individuals to control information about themselves? This struggle has occurred in both domestic and international institutions. As many have noted, with globalization, the process of achieving interdependence has become more complex (Keohane & Nye, 1977) and involves more policy issues and more global and regional networks of international rules and standards (Newman, 2001). Concern about the collection and use of personal information is one such new policy issue, requiring regional and international bodies to develop both appropriate roles for themselves as policymakers and also appropriate policies.

Privacy and data protection are being constructed almost simultaneously on the national and transnational levels. This case thus provides a rich opportunity to explore the interactions between international structures and national agents in development of a norm that is central both to human rights and also to global trade. The interdependence generated by global trade and the transnational convergence of values provoked by global consumerism and global concern with human rights may create incentives for the development of more collective or shared identities regarding privacy and data protection (Wendt, 1994). As will be demonstrated, the historical record is uneven, with some success and some failures in cooperation.

First, the article provides a brief review of the history of the conflict over transborder data flows. This history incorporates an analysis of the conceptual differences in countries' orientations to and definitions of the problems presented by transborder data flows (Bennett, 1992; Flaherty, 1989). Second, in the article, national and regional policy debates about what policy solutions are possible in what has become inherently global communications and economic networks are examined with particular attention to discussions between the United States (U.S.) and the European Union (EU) through the European Commission (EC), the governing body of the EU with responsibility for implementing legislation. Although privacy issues are of concern in a number of countries with global trading interests, the discussions between the United States and the European Union have spanned the longest time period and best illustrate the range of interests, principles, and institutions involved in policy formulation and adoption. Specifically, I analyze the negotiations between the Data Protection Working Party of the EC's Directorate General XV and the U.S. Department of Commerce over the American "Safe Harbor" proposal as a response to the EC's requirement that countries provide "adequate protection" for personal data moving from EC countries to non-member countries. Finally, informed by this debate between the EU and the United States, I evaluate whether harmonization of privacy and data protection policies is likely to evolve through existing processes and institutions.

The Problem of Transborder Data Flows

Exchanges of information, including personally identifiable information, across national borders have become a conventional component of international commerce. If an American buys a book from a bookstore in England, information on the sale and the payment for that sale crosses at least two national borders. If a Spaniard does contract work with a company in Canada, information to pay the Spaniard crosses the two national borders and is registered with the revenue agencies in both countries. These two examples are simple illustrations of the flow of information that is required for international commerce. In addition to employment and retail transactions, similar information routinely crosses borders for travel, health, and education. Any time people or their business traverse national borders, their personal information accompanies them.

Differences at the National Level

Although such exchanges of personally identifiable information have occurred since trade began, concern with individual privacy in the 1970s led most advanced industrial countries to adopt legislation to protect privacy by the late 1980s. Some countries, notably the United States and to a somewhat lesser extent Canada and France, defined their protection in terms of privacy, while other countries, including

most of the European countries, characterized theirs as data protection (Bennett, 1992; Flaherty, 1989). Additionally, some countries adopted omnibus legislation requiring public and private organizations to comply while others passed sectoral legislation establishing different standards for public and private organizations as well as within the private sector.

With the passage of national privacy or data protection legislation, national variations generated regional and international conflict. An often-quoted statement of France's Magistrate of Justice at an Organization for Economic Cooperation and Development (OECD) symposium in 1977 captures this conflict:

Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows. (as quoted in Eger, 1978, pp. 1065–1066)

This quote emphasizes the marketable, technological, and national sovereignty components of the debate about the exchanges of personally identifiable information across different national jurisdictions. But, also, other components of the problem have received attention, including the human rights concern with personal privacy and concern with the free flow of information. Each component emphasizes a distinct aspect of the problem, generates particular questions in policy deliberations, and elicits different configurations of stakeholders (Margulis, "Privacy as a Social Issue and Behavioral Concept," this issue).

Given diverse cultural traditions and varying involvements in international trade, countries define the problem of transborder data flows somewhat differently. For example, the United States generally stresses the free flow of information, often citing the First Amendment in support, and the importance of a free market. As Buss (1984) pointed out,

The very idea that a simple transfer of information between a parent company and its affiliates can be subject to restrictions seems unthinkable to U.S. executives, most of whom have grown up in a society where information has always flowed freely across thousands of miles. (p. 112)

I would argue that the American business perspective, which interprets privacy and data protection policies as non-tariff trade barriers that interfere with the free flow of information, is rooted in Americans' inherent distrust of government regulation of internal business operations, their preference for market solutions to consumer complaints, and the value of information to a market economy. In the United States, privacy issues are driven by consumerism and free trade. By contrast, in European and some other countries, privacy and data protection policies protect fundamental rights of citizens. They reflect a tradition of more government control over the economy and information flows, and the belief that governments have a duty to protect the privacy of their citizens. They emphasize not only their human

rights traditions, including privacy, but also, in light of the power of American transnational companies, national sovereignty.

National Differences in Public Attitudes

With American and European variations in national privacy or data protection laws, views about the role of government, and orientations to free trade, conflict over transborder data flows would not be surprising. These national differences appear also, to some extent, in public attitudes about privacy and information flows, especially about commercial transactions, but there are also some commonalities in national attitudes. In Spring 1999, IBM commissioned a survey in the United States, Germany, and the United Kingdom regarding consumers' attitudes about privacy and consumer marketing. Telephone interviews, averaging 20 minutes in length, were conducted with a national cross section of 1,006 adults in the United States, 1,002 in the United Kingdom, and 1,000 in Germany (IBM Global Services, 1999, p. 8). The report provides percentages but no statistical tests.

The majority of consumers in all three countries were not very interested in receiving marketing material: Consumers in the United States (48%) were more interested in receiving marketing material than consumers in Germany (32%) or the United Kingdom (29%; IBM Global Services, 1999, p. 11). Although these results reinforce the perception of a more consumer-oriented culture in the United States, they do not mean that Americans are necessarily less concerned about the privacy issues related to marketing. Indeed, virtually identical percentages of respondents in the United States and Germany believe that they have lost control over both how information is collected and how it is used by companies (United States 80% and Germany 79%) and that it is impossible to protect privacy in the computer age (United States 71% and Germany 70%). Respondents in the United Kingdom express a slightly less pessimistic attitude (IBM Global Services, 1999, Exhibit ES-3, p. 22).

A higher percentage in the United States (64%) trusts that businesses are handling personal information in a proper and confidential manner than in the United Kingdom (58%) or Germany (54%; IBM Global Services, 1999, Exhibit ES-3, p. 22). It is unclear whether these national differences stem from views about the effectiveness of laws or views about trust in business. Interestingly, the cross-national responses regarding the reasonableness of protection offered by existing laws do not parallel the responses regarding trust in business practices. More respondents in the United Kingdom (63%) find their legal and organizational practices reasonable than in the United States (59%) or Germany (55%), which reports the lowest percentage of respondents agreeing (IBM Global Services, 1999, Exhibit ES-3, p. 22).

Survey results did indicate a difference in some behaviors among respondents in the three countries. For example, Americans (78%) "refused to give information

Table 1. Cross-National Comparison of Percentage of Respondents at Four Comfort Levels With the Way Government Is Handling Protection of Consumer Privacy

	Very	Somewhat	Not Very	Not at all
United States	4	39	33	23
United Kingdom	4	46	30	11
Germany	8	48	27	8

Note. From IBM Multi-National Consumer Privacy Survey (conducted by Louis Harris & Associates) (Table 7.1a, p. 129; Table 7.1b, p. 210; Table 7.1a, p. 293), by IBM Global Services, October 1999.

to a business or company because you thought it was not really needed or was too personal” compared to the English (58%) or Germans (52%; IBM Global Services, Exhibit ES-4, p. 23). The basis for this difference is unclear. The larger percentage in the United States could be attributed to more distrust of business, but this interpretation would contradict the level of confidence in business handling of personal information. Instead, it may be accounted for by more, and possibly more intrusive, requests for information by U.S. businesses and the more developed direct marketing presence in the United States.

There were also differences in the “comfort level” that respondents in all three countries had with the “way government is handling protection of consumer privacy.” As Table 1 indicates, Americans were the least comfortable, Germans voiced the most comfort, and the English fell between, but closer to the Germans. These responses help to interpret the national variations in whether existing laws and organizational practices provide a reasonable level of consumer privacy protection. While 43% of respondents in the United States express comfort with “government handling,” 59% believe “laws and organizational practices” provide a reasonable level of privacy protection. For American respondents, the addition of organizational practices increases a general sense that privacy is being protected. This is true also in the United Kingdom, although to a lesser extent, with 50% expressing comfort with “government handling” and 63% believing “laws and organizational practices” provide reasonable protection. In Germany, responses are virtually identical for both items (IBM Global Services, Exhibit ES-4, p. 23).

Responses to the IBM survey demonstrate that there is cross-national agreement about the loss of consumer privacy. The results indicate there is room for the social construction of common governmental and organizational practices to protect consumer privacy. I would argue that businesses’ collection of personal information is a universal phenomenon and, with global trade and global companies, there will be pressures for more similarities among national business practices for the handling of personal information. Businesses, across nations, prefer fewer restrictions on the handling of personal information. By comparison, countries have adopted a range of privacy or data protection policies. Consequently, in this global environment, business shares a more common position while governments

have adopted different positions. If countries remain fragmented in their policy positions, global business needs are likely to dominate and may make it difficult to construct a more collective and comprehensive understanding of the problems and possible solutions for privacy and data protection policies.

Initial Harmonization of Policies

Recognizing the global flow of personal information and its significance in global commerce, international and regional bodies have deliberated how to address the problem of transborder data flows since the late 1960s. In 1968, the Council of Europe debated the issue and concluded that national and international law was not adequately protecting privacy (Evans, 1981). By 1974, the Council had adopted non-binding recommendations following the basic format of “fair information principles”: Information should be accurate, timely and relevant; confidentiality and security should be protected; individuals should have rights of access, notice, consent, and correction. Also, during the mid-1970s, the Council of Europe drafted an international treaty on data protection to clarify the right of privacy in the European Convention on Human Rights. This “Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data” was binding on the countries that signed it and required that national laws be consistent with it. The United States did not sign the Convention (Cooper, 1984; Patrick, 1981).

The OECD, a group of 30 member countries committed to a market economy and pluralistic democracy that discuss and develop social and economic policy, became involved in the issue of transborder data flows in 1977 when the group convened an international conference on the subject. The 300 attendees concluded that national legislation on the privacy of personal data should be harmonized (Bigelow, 1979). The OECD established a panel of experts to develop fair information practice guidelines and, in response, the United States established a federal interagency task force to draft and propose guidelines to the OECD. In 1980, the OECD adopted non-binding guidelines that incorporated most of the “fair information principles.” Member countries were to encourage data collectors to create codes of conduct. In content, tone, and enforcement, the guidelines represented a compromise between the interests of the United States in maintaining the free flow of information and those of the European countries in achieving consistent regulations protecting personal information, with the United States achieving many concessions (Regan, 1993).

In subsequent negotiations between the United States and Europe, European submission to key U.S. demands is repeated in part as a result of the importance of the United States as a trading partner and in part because there is often some support within the European business community for the U.S. position. These bilateral negotiations highlight the two dimensions of discourse and policy that

have dominated the evolution of policy for transborder data flows. There is a cooperative dimension around trade that generates collective interests and fosters the formation of similar policies. But there is also a conflictual dimension around privacy which elicits the national interests in particular cultural norms and in views about the appropriate role for the government. On this dimension, the EU and the United States differ rather fundamentally. The question then is whether more recent processes for harmonizing privacy and data protection policies in order to foster global trade have provided an opportunity for reconstructing privacy and data protection in a more collective way. In other words, how has the interaction shaped the evolution of norms about privacy and data protection?

Global Harmonization or Continued Differentiation

During the 1990s, the locus of policy action concerning transborder data flows has been the European Union and its development of one European market by the close of 1992. The rather tortuous path to approval and implementation of the EU's "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (hereafter referred to as the Data Protection Directive; European Parliament and the Council of the European Union, 1995) took eight years and involved the approval of a number of its governance institutions including the EC, the European Parliament, and the EU Council. This attempt at harmonization of data protection policy generated debate between the European Union and the United States on three key issues: the degree of individual control over uses of personal information, the level of protection countries needed to ensure before transfers of personal information could occur, and the nature of the enforcement authority (for documents associated with this process see: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm).

The first key issue, the degree of individual control, has been couched primarily in terms of "opt-in" versus "opt-out" to uses of personal information for a purpose other than that for which it was collected. Such uses are generally referred to as secondary uses. In an opt-in system, individuals affirmatively approve any secondary uses of their personal information; in an opt-out system, the assumption is that information may be used unless the individual takes steps to veto such secondary uses. In the United States, the more passive "opt-out" possibilities have become standard fare in fine print on applications and subscriptions. American business, reflecting an emphasis on efficiency of operations and on the marketing potential provided by personal information, overwhelmingly favored "opt-out" and viewed European notions of "opt-in" as onerous and unrealistic. The European business and cultural norm entails less collection of personally identifiable information and has spawned a less developed information industry. The expectation in Europe is that personal information will not be exchanged and disclosed, while in the United States the opposite is the case.

The second key issue focused on whether the policies of other countries should be “equivalent” or “adequate” to the EU Directive before personal information could be transferred to or from an EU member state. From the U.S. business and government perspectives, the standard of “equivalent” appeared rigid because its legalistic orientation was more consistent with a civil code, statute-based system. By comparison, the “adequate” standard was more consistent with the common law, precedent-based system in the United States. Moreover, a standard based on equivalency elevated the authority of EU decision makers, while adequacy preserved more autonomy for national sovereignty of other countries.

The final key issue involved what type of government authority was necessary to enforce and oversee the implementation of data protection or privacy requirements. Most European countries had data protection or privacy commissions with either regulatory or advisory authority. For example, the German Federal Data Protection Commissioner is largely an advisory body while the Swedish Data Inspection Board is a more regulatory body with authority to license all personal information systems (Flaherty, 1989). Regardless of specific powers, these bodies provided an institutional forum with clear authority. The United States was relatively alone in not having such an agency, thus the question about which, if any, governmental institution would serve as a supervisory authority as required by the EU Directive was raised.

The history, debates, lobbying, and resolutions of these issues in the final EU Data Protection Directive are examined in detail in several studies (Cate, 1997; Regan, 1999; Reidenberg, 1999; Schwartz & Reidenberg, 1996; Swire & Litan, 1998). In general, the final directive represents a compromise on each of these issues. It is commonly accepted that “informed consent” will mean some form of notice. The choice to “opt-out” will be accepted for most instances of secondary use; the exception is that if personal information is regarded as “sensitive,” then “opt-in” would be required. The “equivalent” standard was rather quickly dropped in favor of the more flexible “adequate” standard. The requirement for a “supervisory authority” was retained but would be interpreted loosely and in light of the regulatory frameworks in different countries.

Although the previous discussion is framed in terms of differences between the United States and the EU, it is important to note that differences among European countries also impacted the bargaining and negotiating on the Directive’s principles. Germany (in particular) and France advocated strong privacy or data protections that would be consistent with the protections in their own national laws. Some European countries favored weaker protections, again consistent with their own laws, and some had not yet passed privacy legislation. The members of the EU did not share a common perspective on the specifics of the Directive, but they did share a common perspective on the need to harmonize, for purposes of free trade within the EU, the regulations governing transborder data flows. As Shaffer (2000, p. 12) similarly points out:

It was the convergence of interests of powerful states, backed by large markets, to both facilitate free information flows and retain stringent data privacy controls that permitted the EU Directive to go forward. It was France and Germany's political exploitation of market power that enabled protection to be traded up in the European Union.

Once the EU's final Data Protection Directive was approved and European countries drafted national legislation in conformity with that Directive, debate continued about how to deal with the apparent discrepancies between U.S. and EU policy without curtailing information exchanges, especially those essential to global commerce. Three methods were possible. The first was to provide evidence that U.S. policies were indeed adequate to those of the EU. To this end, the EC commissioned two American law professors to analyze the extent to which the American practice of sector by sector, rather than comprehensive, privacy protections met the "adequacy" standard of the EU Directive. As Simitis states in the foreword to the study by these two professors, their analysis "precludes simplistic judgments" and does not lead to a "clear cut verdict on the United States" (Schwartz & Reidenberg, 1996, p. x).

The second method for dealing with discrepancies between the EU Directive and U.S. protections was to negotiate individual contracts for information exchanges. Article 25 of the EU Directive requires that "adequacy" be evaluated in light of "all circumstances surrounding a data transfer operation." Schwartz (1995) points out that this "specifically permits contracts that add to the level of data protection available in a given country" (p. 485). However, because contractual arrangements do not have the force of law and are not entered into by two sovereign nations, some EC officials do not find such arrangements acceptable. For example, a contract between German Railway and Citibank was approved by the German Data Protection Authority, but a German data protection official argued that a contractual solution was not an appropriate "model," but could only "complement and support but never replace national legislation" (Dix, 1996).

As it became obvious to American businesses that it was highly unlikely either that the EU would issue a general ruling that U.S. policy was adequate to that of the EU Directive or that contractual arrangements would be easily negotiated, a third option became attractive. This was to negotiate an arrangement between the EU and the United States that would enable personal information to flow with some level of assurance that it would not be misused. Trying to preserve a self-regulatory, sectoral framework for information privacy protection, American business prevailed upon officials in the International Trade Administration (ITA) of the U.S. Department of Commerce to develop a "Safe Harbor" arrangement with officials from the EC's Directorate General (DG) XV, the Internal Market DG with political and operational responsibility for media, commercial communications, and information society services. Through a "Safe Harbor," American businesses that agreed to the arrangement would be viewed as being in compliance with the adequacy requirement of the EU Directive and would ensure that

their flows of personal information were not interrupted. The development process for a Safe Harbor provided yet another opportunity for the evolution of norms and policies that would be based more on collective notions of privacy. The next section analyzes in some details the process of negotiating a Safe Harbor to determine whether learning and change occurred between the United States and EU or whether traditional interests and ways of interacting continued.

Safe Harbor Negotiations

These negotiations began several months before the October 25, 1998, effective date for the EU Directive. Detailed documentation of these negotiations can be found on the Web site of the Department of Commerce's International Trade Administration (ITA; <http://www.export.gov/safeharbor>) and provide the basis for the following summary of events. On November 4, 1998, Ambassador David Aaron of the ITA wrote a letter to U.S. industry representatives seeking input on "Draft International Safe Harbor Principles." The seven draft principles were, in effect, a restatement of the fundamental fair information practices and included requirements that organizations would provide "clear and conspicuous" notice regarding the collection and use of personal information, would offer individuals the choice of opting out of secondary uses and disclosures to third parties, and would give individuals the ability to access personal information. An onward transfer principle required organizations to ensure that third parties to which they disclosed information provided the same privacy protection. Finally, organizations were obligated to guarantee security, data integrity, and mechanisms for enforcement.

Ambassador Aaron's letter signaled that the EU had agreed tentatively to the broad arrangements that U.S. businesses sought by allowing voluntary action and self-certification and emphasizing commerce rather than privacy. In particular, companies would "choose voluntarily" to adhere to privacy principles; organizations could come within the Safe Harbor "by self certifying" that they would adhere to these privacy principles; the principles were designed "to enhance commerce between the U.S. and the European Community"; and, the principles were not intended to "govern or affect U.S. privacy regimes." The tentative agreement on the Safe Harbor concept addressed U.S. business concerns that they not be obligated to comply with privacy principles that would negatively affect commerce, would change the self-regulatory approach to privacy protection in the United States, and would entail outside monitoring of their information practices. Ambassador Aaron emphasized that the primary benefit of the Safe Harbor was that all 15 Member States would be bound by the EC's recognition of these principles as adequate, thus eliminating the need to negotiate with individual countries.

The Draft Safe Harbor Principles began a two year process of comment and revision involving four iterations of the principles with a period of comment for each iteration. The number of specific organizations or individuals submitting

comments decreased over the four comment periods with 75 comments on the first draft, 59 on the second, 42 on the third, and 28 on the fourth. The overwhelming majority were from business-related organizations. Fourteen organizations submitted comments on all three drafts; the list reads as a “who’s who” in the high-tech, global, information and services sector and includes the Associated Credit Bureaus, Bell Atlantic, Lexis Nexis, McGraw-Hill Companies, Time Warner, Inc., and Visa. Four organizations submitted comments on all four drafts: American Insurance Association, Direct Marketing Association, Information Technology Industry Council, and, United States Council for International Business. Initially, public interest groups, such as the ACLU, criticized the industry-centered process and suggested that a period of broader public comment was necessary. The process remained a specialized one that was largely removed from easy public participation. It was not until the third draft that nine consumer and privacy advocacy groups submitted comments. The TransAtlantic Consumer Dialogue, a coalition group including the Consumer Federation of America, the Center for Media Education, and the Electronic Privacy Information Center, submitted comments on both the third and fourth drafts.

The industry comments provided no surprises, reflecting overwhelming support for a voluntary, self-certified Safe Harbor that would ensure the continuation of transborder data flows. There were suggestions for weakening specific draft privacy principles, especially the requirements for: organizations to give “clear and conspicuous” notice and choice; organizations to require third parties to provide the same level of privacy (onward transfer); individuals to have “reasonable access” to information about them and the ability to correct or amend inaccurate information; and organizations to provide enforcement mechanisms including recourse, verification, and sanctions. Although the seven principles were retained as principles, the substance of each was weakened somewhat in response to industry comments.

Harmonization Through Safe Harbor?

On June 9, 2000, the Draft Safe Harbor Principles were transmitted from the U.S. Department of Commerce to the EC, and the final EC decision approving the “Safe Harbor Privacy Principles” was released on July 27, 2000. However, there are several reasons to suspect that the “Safe Harbor” may not be the vehicle through which harmonization is successfully achieved. First, the long-standing differences in the orientations of the EU and United States to the issue of privacy or data protection persist. The EU stresses the use of government power to control organizations and protect citizens’ rights while the United States reveals its reluctance to use government power and accentuates the benefits businesses will gain from the Safe Harbor arrangement. This is well illustrated by language in the documents of each. Article 1 of the EC’s Commission Decision emphasizes that transfers of data to an organization shall occur when two conditions are met:

(a) the organization's unambiguous and public disclosure of its commitment to comply with the Safe Harbor Principles; and (b) the organization's being "subject to the statutory powers of a government body. . .empowered to investigate complaints and obtain relief" (Commission of the European Communities, 2000). The EC decision highlights explicitness, openness, binding rules, and enforcement. In contrast, the Department of Commerce's "Safe Harbor Overview" emphasizes "predictability and continuity," elimination of "the need for prior approval," and "simpler and cheaper means of complying with the adequacy requirements of the Directive" (U.S. Department of Commerce, 2000).

The second reason that Safe Harbor may not be successful is that the EU has consistently preferred to deal with governments of states while the United States has been reluctant to adopt an official government role. Although the U.S. Department of Commerce negotiated the agreement, it has limited its future involvement as is quite clearly stated on the instructions for signing up on the "Safe Harbor List":

In maintaining the list, the Department of Commerce does not assess and makes no representation as to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list. (emphasis in original; U.S. Department of Commerce, n.d.)

The Department of Commerce unambiguously signals that it will adopt a passive role. This may well mean that European countries that have questions or problems with transfers of information will deal directly with the U.S. enforcement agencies recognized by the EC. In the Safe Harbor Overview, the Department of Commerce explains the enforcement of the Safe Harbor as being "carried out primarily by the private sector" with back-up "as needed by government enforcement of the federal and state unfair and deceptive statutes. Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or the states provide overarching government enforcement of the Safe Harbor principles" (U.S. Department of Commerce, 2000).

The patchwork of sectoral regulation that has long confused the Europeans is continued under the thin veil of the Safe Harbor principles behind which there is no one government entity but fragmented state and local agencies with sometimes unclear jurisdictions. In the Commission Decision, the EU agrees to recognize and deal with an approved list of U.S. enforcement agencies, but Article 3 of the Decision notes that if any of them is found "not effectively fulfilling its role, the Commission shall inform the U.S. Department of Commerce" (Commission of the European Communities, 2000). It would appear that the United States expects its Department of Commerce to adopt a passive, non-interventionist role while the EU expects to be able to work more directly with the Department of Commerce.

A third reason to doubt the success of Safe Harbor in achieving harmonization is that there are critics of the Safe Harbor principles in both the United States and EU. The EU approval was not without internal opposition. On July 5, 2000, the European Parliament registered its view that the remedies for individuals in the proposed Safe Harbor did not provide adequate protection. Nevertheless, the EC decided to proceed with the agreement but informed the Department of Commerce that it would monitor this part of the agreement and would evaluate its Safe Harbor decision in 2003.

In the United States, there are two sources of criticism. One is from the National Business Coalition on E-Commerce and Privacy, whose members include General Electric, Home Depot, and Visa USA. In an April 5, 2000, letter commenting on the March 15, 2000, draft principles and Frequently Asked Questions (FAQs), the Coalition raised a number of concerns including: (a) that the principles “far exceed any privacy requirements that have ever before been imposed in the United States, thus raising a very real question of national sovereignty”; (b) that the agreement should state that existing federal statutes addressing financial privacy and consumer credit information fulfill the adequacy provisions; (c) that U.S. organizations should not have to agree to principles that are not applied to similar organizations in other countries; (d) that the United States should have considered options other than the Safe Harbor agreement; (e) that there needs to be more industry consultation and a serious study of cost and technological feasibility; and (f) that Congress should have the opportunity to review the agreement (National Business Coalition, 2000). Other industry comments reflected similar concerns. It is safe to conclude that there is not universal business agreement about the Safe Harbor Principles, although there might well be the sense that the Safe Harbor represented the best that was possible and that it was important for all to conclude some agreement.

The second source of criticism comes from privacy advocates and consumer groups, such as the TransAtlantic Consumer Dialogue (TACD), which represents over 60 European and American consumer protection groups including the European Consumer Association, Consumer Federation of America, Center for Media Education, Consumer Project on Technology, Electronic Privacy Information Center, National Consumers League, and U.S. Public Interest Research Group (U.S. PIRG). The primary criticism of this group was that the Safe Harbor agreement would not provide adequate protection to European citizens because of its reliance on a self-regulatory system that has been unsuccessful in the United States. As they point out,

Ultimately, companies can do what they like with personal data provided they can be said to have the consumers' consent. The real danger here is that consent clauses can be cleverly drafted to give companies almost a free hand to process data as they wish. In practice, consumers are forced to accept the companies' terms or otherwise lose the opportunity to do business with the company (or any other company) at all. (TransAtlantic Consumer Dialogue, 2000)

The ACLU, as well as other American privacy and consumer groups, expressed concern that “the adoption of a Safe Harbor proposal will provide European Union citizens greater protection than Americans against privacy violations committed by U.S. firms” (American Civil Liberties Union, 1998).

Events since July 2000 support this argument regarding the unlikelihood that the Safe Harbor agreement will be successful in achieving harmonization. American businesses have been slow to sign the agreement. Only 198 U.S. companies have signed the Safe Harbor agreement through June 2002. These are mostly small to mid-size firms with the exceptions of Hewlett-Packard, Dun & Bradstreet, and Microsoft. This unenthusiastic response reflects continued concerns about whether companies can actually comply with the requirements in a manner that will satisfy the EU and that does not leave them open to more active oversight by the Federal Trade Commission (Assey & Eleftherious, 2001). In response to business reluctance and some political opposition, the EC revisited the question of whether contractual arrangements could satisfy the EU directive. In January 2001 the EC released a draft of model contract provisions. Although some companies may find contracts a preferable method as they avoid the public list on the Department of Commerce Web site of those who have signed the Safe Harbor agreement (Harvey & Verska, 2001), U.S. businesses, through the Departments of Treasury and Commerce, registered opposition to the standard contract clauses which they believe “impose unduly burdensome requirements that are incompatible with real world operations” (Mosquera, 2001). After modifying the draft model contract somewhat in response to American business concerns, the EC adopted in June 2001 a decision setting out standard contractual clauses for transfers of personal data. Also, the EC issued, in February 2001, a progress report evaluating the operation of the Safe Harbor agreement. The EC noted the lower than expected response and criticized the avoidance of transparent policies and lack of clarity about dispute resolution mechanisms.

Is Harmonization Possible?

Throughout the 30 years of debates about transborder data flows, I argue that there has been a conflict between two enduring concerns: privacy or data protection, and market power. Governments in the United States have been stronger supporters of market power than have those in Europe. Governments in Europe have been stronger proponents of privacy or data protection than have those in the United States. These orientations are unlikely to change given differences in cultural norms, legal systems, philosophies of government, and commitments to free markets. Despite these stable forces, the globalization of both information/communication systems and also the economic system will continue to promote changes at the global, rather than national, level. Globalization has been driving the interest in harmonization and all indications are that the globalizing

logic of both communications systems and economic systems will be even more influential in the on-line world where the flow of information is ubiquitous, and where it is harder to discern national borders.

As a result of the globalization of information and economic systems, I believe it is likely that discussions about transborder data flows will move from national or regional forums to international forums. Standard-setting bodies for the design of architectures and protocols for communications systems will be increasingly important in setting the defaults for and possibilities of privacy in the on-line world (Lessig, 1999). Such standard setting is occurring in discussions of the World Wide Web Consortium (W3C), created in 1994 to facilitate the development of common protocols to ensure the interoperability of the Web, and the Internet Corporation for Assigned Names and Numbers (ICANN), established in 1998 to assume responsibility for Internet management functions previously performed under contract for the U.S. government, as well as a number of traditional standard-setting bodies, including the International Standards Organization. W3C and ICANN are global organizations whose memberships are largely dominated by private sector corporations, including technology vendors and corporate users, with other members including academic and government users. Both operate primarily by consensus but, with private sector dominance, decisions are likely to mirror private sector interests unless consumer groups play an active role in monitoring their activities and educating the general public. (For additional information about W3C and ICANN, go to <http://www.w3.org> and to <http://www.icann.org>, respectively.)

At the same time that the globalization of the communication infrastructure increases the role and importance of standards-setting bodies, I believe that the globalization of the economic system augments the role of international trade organizations, such as the World Trade Organization, and treaty agreements, such as the General Agreement on Tariffs and Trade or General Agreement on Trade and Services. If privacy or data protection requirements affect trade, then these organizations would have a legitimate interest in trying to influence policy. However, trade organizations already have full, complex and controversial agendas and are unlikely to become major players in the near future.

Transborder data flows always have been both a trade issue and a rights issue. Harmonization is, by definition, a trade issue because the purpose of harmonization is to provide a more predictable framework for trade. Based on my understanding of the literature, the rights perspective on transborder data flows is raised primarily at the national level and competes for recognition in efforts where harmonization is the goal. If the transborder data flow issue is defined as one of communication network architecture and standards, what might that mean for privacy and data protection? The obvious answer would appear to be that global corporate interests, reflecting technology vendors and corporate users, would dominate discussions that would be held largely in technical and professional terminology and conducted in exclusive forums with little systematic input from the

public or formal review by government agencies. Institutions such as ICANN and W3C do not need the support of national governments for their authority or legitimacy.

Whether a scenario of corporate dominance becomes the norm for policy decisions regarding on-line privacy and data protection will depend, I believe, on the persistence of public interest groups which either participate directly in the policy deliberations of global consensus entities or monitor their activities from outside. For example, the Center for Democracy and Technology (CDT) is a member of W3C and also scrutinizes the activities of ICANN. (For additional information about CDT, go to www.cdt.org.) Other consumer protection and privacy advocacy groups, which increasingly are working together on consumer privacy issues, have developed expertise on the issue areas and experience in operating in international forums. Additionally, it appears possible that adding “network architecture” to policy debates that are currently framed in terms of “trade” and “privacy/data protection” may expand the scope of conflict. I believe that the inclusion of groups representing network architecture interests may offer privacy groups new allies. It may well be that technical and computer specialists, who tend not to be motivated principally by financial incentives, bring ethical concerns about privacy to the table as well as their technical expertise. Activities of groups such as Computer Professionals for Social Responsibility and various subgroups of the Institute of Electrical and Electronics Engineers and the Association for Computing Machinery provide evidence for such interests. Common interests between privacy groups and technical groups could precipitate the formation of different coalitions so that the “trade” perspective becomes less dominant and the privacy protection perspective is given another opportunity.

Conclusions

Harmonization of transborder data flows and the principles that regulate those flows has become an integral part of the global communications and economic systems. But that harmonization is still incomplete. Based on the last 30 years of policy discussions, several conclusions seem apparent. First, as a result of the EU’s persistent support for privacy and data protection principles, inclusion of some degree of privacy protection is likely. The evolution of agreement on those principles has failed to develop beyond the rhetorical stage; evolution of agreement on implementation and specifics has been thwarted. The iterative processes of harmonization have not successfully formed collective identities and interests around privacy and data protection. Success has stayed at the more abstract level and has been fueled by the collective interest in global trade. The iterative processes examined here have not resulted in a shared reconstruction of privacy and data protection by either the EU or the United States.

This failure is attributable to both the intractable positions on normative and practical issues but also to the process of EU-U.S. harmonization. To date, the EU as a state actor has played a forceful role; the United States as a state actor has played a largely reactive and passive role; transnational corporations as non-state actors have been assertive in both the national and transnational debates. Some have suggested that a broader involvement by international organizations, including a treaty-level "General Agreement on Information Privacy" (Reidenberg, 2000), might change the dynamic of debate and provide opportunities for more collective development of principles of privacy and data protection. But if the international forums are dominated chiefly by corporate organizations and reflect business needs, then the process of harmonization examined above is likely to be replicated. Such a process would continue to privilege trade interests and corporate actors.

The reluctance of the United States to involve itself as a state actor also contributes to the failure of the harmonization process to develop a more collective meaning of privacy and data protection. This reluctance is apparent not only in the EU-U.S. negotiations but also at the annual conference of Data Protection Commissioners where attendees note that there is little continuity in U.S. representation by government agency and staff (Reidenberg, 2000). The U.S. absence and its acquiescence to business interests has thwarted opportunities for interaction that might produce the formation of more collective harmonious positions. Although the incentives of global trade interdependence and some degree of transnational convergence on domestic values are in place, collective identity formation is not inevitable (Wendt, 1994). In the case of privacy and data protection, the countervailing forces have been powerful and the mechanisms have not facilitated a cooperative interaction.

Events since September 11, 2001, will also affect the evolution of the harmonization of privacy and data protection policies. The terrorist attacks are likely to have a similar effect on national priorities, placing more emphasis on anti-terrorism policies, and fostering more cooperation among states. This cooperation is apt to be in the direction of strengthening law enforcement and intelligence gathering capabilities, and weakening traditional civil liberties protections. Salbu (2002) argues that Europe, with its stronger acceptance of the government's role in protecting public welfare, may be more receptive to initiatives that strengthen the government's anti-terrorist capabilities.

The European Parliament's decision to require Internet service providers and telephone companies to retain traffic data for law enforcement purposes is evidence for change in that direction. If the privacy and data protection issue becomes redefined as an anti-terrorism and civil liberties issue, rather than a trade and human rights issue, the normative issues and the institutional mechanisms will also change and the business influence will be minimized.

References

- American Civil Liberties Union. (1998, November 18). *Letter to task force on electronic commerce, International Trade Administration, Department of Commerce Re: draft international Safe Harbor privacy principles, signed by A. Cassidy Sehgal-Kolbert*. Retrieved July 7, 2000, from <http://www.ita.doc.gov/td/ecom/com2abc.htm>
- Assey, J. M., & Eleftheriou, D. A. (2001). The EU-U.S. privacy safe harbor: smooth sailing or troubled waters? *CommLaw Conspectus*, 9, 145–158.
- Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca, NY: Cornell University Press.
- Bigelow, R. (1979). Transborder data flow barriers. *Jurimetrics Journal*, 20(1), 8–17.
- Branscomb, A. W. (1994). *Who owns information? From privacy to public access*. New York: Basic Books.
- Buss, M. D. J. (1984). Legislative threat to transborder data flow. *Harvard Business Review*, 62, 111–119.
- Cate, F. H. (1997). *Privacy in the information age*. Washington, DC: Brookings Institution Press.
- Commission of the European Communities. (2000, July 27). *Commission decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the U.S. Department of Commerce*. Retrieved August 15, 2000, from <http://www.ita.doc.gov/td/ecom/DecisionSECGEN-EN.htm>
- Cooper, D. M. (1984). Transborder data flow and the protection of privacy: The harmonization of data protection law. *Fletcher Forum*, 8, 344.
- Dix, A. (1996). The German RailwayCard: A model contractual solution of the “adequate level of protection” issue? *Proceedings of the 18th International Privacy and Data Protection Conference*. Retrieved July 7, 2000, from <http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm>
- Eger, J. M. (1978). Emerging restrictions on transnational data flows: Privacy protections or non-tariff trade barriers? *Law and Policy in International Business*, 10(4), 1065.
- European Parliament and the Council of the European Union. (1995). *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*. Retrieved July 8, 2000, from http://europa.eu.int/comm/internal_market/en/dataprot/law/
- Evans, A. C. (1981). Data protection in Europe. *Journal of World Trade Law*, 15(March–April), 150–158.
- Finnemore, M. (1996). *National interests in international society*. Ithaca, NY: Cornell University Press.
- Flaherty, D. H. (1989). *Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: University of North Carolina Press.
- Harvey, J. A., & Verska, K. A. (2001, February). What the European data privacy obligations mean for U.S. businesses. GigaLaw.com. Retrieved June 4, 2002, from <http://gigalaw.com/articles/2001-all/harvey-2001-02-all.html>
- Holden, B. (1996). *The ethical dimensions of global change*. New York: St. Martin’s Press.
- IBM Global Services. (1999, October). *IBM multi-national consumer privacy survey* (Conducted by Louis Harris & Associates). New York: Author.
- Kahin, B., & Nesson, C. (1997). *Borders in cyberspace*. Cambridge, MA: MIT Press.
- Keohane, R., & Nye, J. (1977). *Power and interdependence*. Glenview, IL: Scott Foresman.
- Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.
- Mosquera, M. (2001, March 27). Transatlantic privacy war heats up. InternetWeek.com. Retrieved from http://www.internetweek.com/story/INW_20010327S0010
- National Business Coalition. (2000, April 5). *Letter to Ambassador David L. Aaron Re: Safe Harbor agreement under EU privacy directive signed by Susan D. Pinder*. Retrieved July 8, 2000, from <http://www.export.gov/safeharbor/Comments400/NatBusCoalonEcomComments.htm>
- Newman, E. (2001). Human security and constructivism. *International Studies Perspectives*(2), 239–251.

- Patrick, P. H. (1981). Privacy restrictions on transnational data flows: A comparison of the Council of Europe draft convention and OECD guidelines. *Jurimetrics Journal*, 21(4), 405–420.
- Regan, P. M. (1993). The globalization of privacy: Implications of recent changes in Europe. *The American Journal of Economics and Sociology*, 52(3), 257–274.
- Regan, P. M. (1999). American business and the European Data Protection Directive: Lobbying strategies and tactics. In C. J. Bennett & R. Grant (Eds.), *Visions of privacy: Policy choices for the digital age* (pp. 199–216). Toronto, Ontario, Canada: University of Toronto Press.
- Reidenberg, J. R. (1999). The globalization of privacy solutions: The movement towards obligatory standards for fair information practices. In C. J. Bennett & R. Grant (Eds.), *Visions of privacy: Policy choices for the digital age* (pp. 217–228). Toronto, Ontario, Canada: University of Toronto Press.
- Reidenberg, J. R. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, 52(May), 1315–1376.
- Salbu, S. R. (2002). Corporate governance, stakeholder accountability, and sustainable peace: The European Union Data Privacy Directive and international relations. *Vanderbilt Journal of Transnational Law*, 35(March), 655–695.
- Schwartz, P. M. (1995). European data protection law and restrictions on international data flows. *Iowa Law Review*, 80(3), 471–496.
- Schwartz, P. M., & Reidenberg, J. R. (1996). *Data privacy law*. Charlottesville, VA: Michie.
- Shaffer, G. (2000). Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards. *Yale Journal of International Law*, 25(1), 1–88.
- Swire, P. P., & Litan, R. E. (1998). *None of your business: World data flows, electronic commerce, and the European privacy directive*. Washington, DC: Brookings.
- TransAtlantic Consumer Dialogue. (2000). *Submission of the TransAtlantic Consumer Dialogue (TACD) concerning the U.S. Department of Commerce draft international Safe Harbor privacy principles and FAQs* published on March 15, 2000. Retrieved July 7, 2000, from <http://www.export.gov/safeharbor/Comments400/NatBusCoalonEcomComments.htm>
- U.S. Department of Commerce. (2000, August). *Safe Harbor overview*. Retrieved July 7, 2000, from <http://www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm>
- U.S. Department of Commerce. (n.d.). *Safe Harbor list*. Retrieved June 4, 2002, from <http://www.ita.doc.gov/td/ecom/FRN2.htm>
- Wendt, A. (1994). Collective identity formation and the international state. *American Political Science Review*, 88(2), 384–396.

PRISCILLA M. REGAN is an Associate Professor in the Department of Public and International Affairs at George Mason University. Prior to that, she was a Senior Analyst in the Congressional Office of Technology Assessment and an Assistant Professor of Politics and Government at the University of Puget Sound. She has published over twenty articles or book chapters, as well as *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995).