Fordham International Law Journal

Volume 22, *Issue* 5 1998 *Article* 5

Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective

Graham Pearce* Nicholas Platten†

*

†

Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective

Graham Pearce and Nicholas Platten

Abstract

The purpose of this Essay is to examine current EU and U.S. approaches to data protection in the context of the debate about transborder data flows. Part I begins by outlining the EU approach and the criteria governing data transfers to third countries. Part II examines the scope for self-regulation by organizations to safeguard personal data. Part III reviews the main features of the U.S. model of data protection. Then Part IV critically examines several recent U.S. initiatives to enhance privacy in the light of the EU criteria. This Essay concludes by assessing the potential for reconciling the discontinuities between the two models.

ORCHESTRATING TRANSATLANTIC APPROACHES TO PERSONAL DATA PROTECTION: A EUROPEAN PERSPECTIVE

*Graham Pearce**
*Nicholas Platten***

INTRODUCTION

The data protection directive[1] ("directive" or "EU directive"), which came into effect on October 25, 1998, has given rise to an intense debate among the European Union ("EU" or "Union"), the U.S. Administration, and U.S. business aimed at averting potential restrictions on personal data flows between Europe and the United States without sacrificing high levels of privacy protection for individuals. While both the United States and Union claim to be committed to safeguarding personal privacy, significant differences exist in determining how this goal is to be secured. The result of this uncertainty has been increasing concern among the U.S. business community about the impact of the directive and claims that its implementation could disrupt transatlantic trade and business planning, as well as impede the development of electronic commerce.

The main focus of these concerns is Article 25 of the directive, which prohibits the transfer of personal data from the Union to countries that do not possess "adequate" data protection arrangements, unless certain tightly defined exemptions apply. The prospect of U.S. businesses having to await the verdict of EU regulatory bodies before being considered safe destinations for personal data flows has led to suggestions that the Union is attempting to establish its model of data protection extraterritorially.[2] More fundamentally, the debate has high-

* Graham Pearce is a Jean Monnet Lecturer at Aston Business School, Aston University, Birmingham, UK.B4 7ET.

** Nick Platten is a Visiting Fellow at Aston Business School, Aston University.

1. Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. L 281/31 (1995) [hereinafter Directive].

2. Alan Westin, Data Protection in the Global Society, Proceedings of Conference at the Aspen Institute, Berlin 1996, American Institute for Contemporary German Studies, The Johns University (1997).

lighted important divisions between EU and U.S. approaches to data protection, which reflect cultural and historical differences about the role of government regulation. In general, there is a much greater confidence in public institutions and dependence upon administrative law in EU Member States than is the case in the United States, where there is far greater esteem for markets and technology.[3] As a result, data protection in the United States is perceived by many European observers as being over reliant on voluntary self-regulation and technological solutions, while some U.S. analysts perceive the European model as being unduly heavy handed and bureaucratic.

Despite these differences, there is growing public concern on both sides of the Atlantic about the impact of the new information and communication technologies ("ICT") on privacy. Moreover, both the Union and the U.S. Administration regard ICT as crucial in promoting economic growth and perceive public confidence in the new technologies as an essential prerequisite. In the United States, several recent consumer surveys have highlighted both a high degree of public concern about privacy and skepticism about the effectiveness of existing U.S. data protection practices.[4] The outcome has been a spate of initiatives from both the U.S. Administration and groups of leading U.S. companies aimed at strengthening privacy safeguards and meeting the EU adequacy criteria. At the same time, however, the U.S. Administration has expressed doubts about the feasibility of self-regulation and now envisages greater use of legislation, albeit targeted at specific sectors—for example to protect medical records and children's privacy.[5]

The purpose of this Essay is to examine current EU and U.S. approaches to data protection in the context of the debate about transborder data flows. Part I begins by outlining the EU approach and the criteria governing data transfers to third coun-

---

3. Peter Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive, Brookings Institute, Washington (1998).

4. LOUIS HARRIS & ALAN WESTIN, COMMERCE, COMMUNICATIONS AND PRIVACY ONLINE: A NATIONAL SURVEY OF U.S. COMPUTER USE, PRIVACY LAWS AND AMERICAN BUSINESS (1997); ELECTRONIC PRIVACY INFORMATION CENTER, SURFER BEWARE: PERSONAL PRIVACY AND THE INTERNET (1997).

5. Vice President Albert Gore Jr., *Remarks as prepared for delivery at New York University commencement* (visited Apr. 10, 1999) <http://www.privacyexchange.org/iss/confpapers/gorespeech.html> (on file with the *Fordham International Law Journal*).

tries. Part II examines the scope for self-regulation by organizations to safeguard personal data. Part III reviews the main features of the U.S. model of data protection. Then Part IV critically examines several recent U.S. initiatives to enhance privacy in the light of the EU criteria. This Essay concludes by assessing the potential for reconciling the discontinuities between the two models.

I. *THE EU APPROACH*

The European approach is based upon the premise that privacy is a human right and data protection is an essential means to protect that right through a coherent and enforceable legal regime. A comprehensive, public policy approach has been chosen, backed by horizontal administrative law and independent scrutiny that applies to all organizations, both public and private. The present EU *acquis* in the field of data protection takes the form of the directive, a framework Data Protection Directive, the impetus for which may be traced back to early national laws from the 1970s[6] and international data protection instruments adopted in the 1980s.[7] The fragmented response to these instruments by EU Member States created a need to harmonize European national data protection laws within the Internal Market, where the development of international networks was bringing about a huge increase in cross-border data flows.[8] A complementary Telecommunications Directive sets out specific sectoral rules to be applied to data protection in the context of telecommunication networks,[9] while the European Commission Com-

6. Early national data protection laws were adopted in Sweden, Germany, and France.

7. *See* Organization for Economic Co-operation and Dev., Recommendation of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, O.E.C.D. Doc. C(80)58 Final, *reprinted in* 20 I.L.M. 422 (1981); Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, Europ. T.S. No. 108, *reprinted in* 20 I.L.M. 317.

8. Graham Pearce & Nicholas Platten, *Achieving Personal Data Protection in the European Union*, 36 J. COMMON MARKET STUD. 529 (1998).

9. Council Directive No. 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Information and the Protection of Privacy in the Telecommunications Sector, O.J. L 24/1 (1998) [hereinafter Telecommunucations Directive].

munication, a European initiative in electronic commerce,[10] leaves the way open for further measures to address specific data protection concerns emerging from the development of electronic commerce.

The directive comprises a mixture of obligations on those who control the processing of personal data, together with rights for individuals who are the subject of data processing.[11] These basic rules, implemented through national legislation, apply throughout the Union and have in effect removed all barriers to the free flow of personal data between EU Member States. A clear distinction must be drawn, however, between the liberalizing effect of the directive on intra EU data transfers and its impact on transfers to third, i.e., non-EU countries. The directive seeks to ensure that the high level of protection within the Union's borders should not be circumvented in cases where data processing is being conducted outside the Union, but based upon personal data originally collected or stored in one of the Member States.[12] Personal data that are undergoing processing or are intended for processing after transfer to a territory outside the Union will only be permitted if the country in question provides an adequate level of protection, unless an exemption applies. This mandatory requirement distinguishes the EU directive from both the Organization of Economic Co-operation and Development ("OECD") Guidelines and Council of Europe Convention on data protection, neither of which requires signatory states to restrict data exports to countries that do not provide similar privacy safeguards. It is this provision that is at the heart of the current debate between the Union and the United States.

A. *Judging the "Adequacy" of Data Protection in Third Countries*

It is common practice for data to be transferred to states outside the Union for processing. Indeed, over the years, European states have developed procedures for determining those

10. European Commission, A European Initiative in Electronic Commerce, COM (97) 157 (1997).

11. David Bainbridge & Graham Pearce, *EC Data Protection Law*, 12 COMPUTER L. & SECURITY REP. 160 (1996).

12. Spiros Simitis, *Foreword* to DATA PRIVACY LAW (Joel Reidenberg & Paul Schwartz eds., 1996).

circumstances in which data may be transferred.[13] The EU directive seeks to harmonize these practices by applying a common set of rules. Many third countries do not possess any form of data protection legislation and, even where regulation is present, it is limited in scope or execution. Nonetheless, the adequacy principle is not intended to compel third countries to apply regulations that are identical in formal or substantive terms to the EU model—data protection may be achieved in different ways.

B. *A Prototype Approach*

The EU directive sets forth in Article 25(2) a non-exhaustive list of factors to be taken into account when judging the adequacy of protection in third countries, from which it is clear that the objective is not to secure "equivalence" but to establish whether data protection principles are in place.[14] In essence, this provision requires an assessment of both the relevant data protection rules and the effectiveness of these instruments. Building on the text of the directive, the "Article 29 Group," the Working Party established by the directive comprising Data Protection Commissioners from each EU state and EU Commission officials, has prepared a set of First Orientations on transfers of personal data to third countries: Possible ways forward in assessing adequacy[15] ("Adequacy Paper"), which sets out a prototype approach for judging adequacy. This approach has been refined in a "synthesis" document regarding the manner in which Articles 25 and 26 of the directive should be applied.[16] It provides a methodology for assessing the level of third country protection and outlines the issues that are likely to arise from its application.

---

13. Scott Blackmer, *Transborder Personal Data Flows: Administrative Practice, Briefing Report for Privacy and American Business Meeting on Model Data Protection Contracts and Laws* (visited Apr. 10, 1999) <http://idt.net/~pab/bio.htm> (on file with the *Fordham International Law Journal*).

14. Directive, *supra* note 1, art. 25(2), O.J. L 281/31, at 45-46 (1995).

15. European Commission, Directorate General XV, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy, XV D/5020/97-EN Final, adopted on June 26, 1997.

16. European Commission, Directorate General XV, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, XV D/5025/98, adopted on July 24, 1998 [hereinafter Transfers of Personal Data to Third Countries].

The Working Group documents cite the principles to be used in appraising the adequacy of protection in a third country. These principles fall into two categories, reflecting the functional approach envisaged by the EU data protection model: the content of the rules protecting personal data on the one hand, and the mechanisms to ensure their effective application on the other. The objective is to assess the fundamental elements of the protection afforded. The principles are summarized below.

- *The purpose limitation principle.* Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this process is compatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society, for example national security or the investigation of criminal offences.
- *The data quality and proportionality principle.* Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant, and not excessive in relation to the purposes for which they are transferred or further processed.
- *The transparency principle.* Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this information is necessary to ensure fairness.
- *The security principle.* Technical and organizational security measures should be taken that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller must not process data except on instructions from the controller.
- *The rights of access, rectification, and opposition.* The data subject should have a right to obtain a copy of all data relating to him or her that are processed and a right to rectification of those data where they are shown to be inaccurate. In certain situations, he or she should also be able to object to the processing of the data relating to him or her.
- *Restrictions on onward transfers.* Transfers of personal data from the recipient to another third party should not be permitted, unless a means is found of contractually bind-

ing the third party in question, thereby providing the same data protection guarantees to the data subjects.

This final principle is intended to prevent the controllers of personal data from using a country with "adequate" provisions as a "staging post" for onward transfers to a country without adequate safeguards to evade the protection afforded by the directive.

In addition, the approach highlights some transfers as posing particular risks to privacy and which, therefore, may merit special attention, for example:

- *transfers of sensitive data*, including medical records or data pertaining to personal, political, or religious beliefs,
- *automated individual decisions*, where the purpose of the transfer is the taking of an automated decision, for example, in the case of assessment of credit worthiness—the individual should have the right to know the logic involved in this decision and be able to challenge it, and
- *direct marketing*, where data are transferred for the purposes of direct marketing, the data subject should be able to "opt-out" from having his or her data used for such purposes at any stage.

II. *TRANSFERS TO THIRD COUNTRIES—ALTERNATIVE SOLUTIONS*

A. *Exemptions*

Article 26(1) of the EU directive allows the possibility of exemptions from the requirement for adequate protection. Views on the potential usefulness of these exemptions, however, differ. Some industry commentators, perhaps unsurprisingly, have taken the view that large numbers of transfers may be covered by the various options set out in Article 26(1). Conversely, the Article 29 Group has underlined the need to adopt a restrictive approach in their interpretation and application.

The first of these exemptions covers cases where the data subject gives his or her consent *unambiguously* to the proposed transfer. Consent must be freely given, specific, and informed. Logic would seem to dictate that in this context "informed consent" will require data subjects to be properly informed of the particular risk that his or her data are to be transferred to a

country lacking adequate protection. If this information is not provided, this exemption will not apply. Because the consent must be unambiguous, any doubt about the fact that consent has been given would also be liable to render the exemption inapplicable. An implied consent, for example, where an individual has been made aware of a transfer and has not objected, would not qualify for this exemption.

The second and third exemptions cover transfers *necessary* either for the performance of a contract between the data subject and the controller or for the conclusion or performance of a contract concluded *in the interest of the data subject* between the controller and a third party. These exemptions appear generous but are likely, according to the Article 29 Group, to be limited by the requirement that all of the data transferred must be necessary for the performance of the contract. Thus, if additional non-essential data are transferred or if some of the data are in fact transferred for follow-up marketing rather than the strict performance of the contract, the exemption will be lost. Despite these caveats, these two exemptions will have an impact. They are often likely to be applicable, for example, to those transfers necessary to reserve an airline ticket for a passenger or to transfers of personal data necessary for the operation of an international bank or credit card payment.

The fourth exemption has two strands. The first covers transfers necessary or legally required on important *public interest grounds*. This strand may cover certain transfers between public administrations, for example between tax or customs administrations or services responsible for social security.[17] Care, however, must be taken not to interpret this provision too widely; a simple public interest justification for a transfer does not suffice; it must be a question of *important* public interest. The second strand concerns transfers in the context of international litigation or legal proceedings necessary for the establishment, *exercise, or defense of legal claims.*

The fifth exemption concerns transfers necessary to protect the *vital interests of the data subject*, for example the urgent transfer of medical records to a third country where a EU citizen had become dangerously ill. Recital 31 of the directive, however, defines vital interest narrowly, as an interest "which is essential for

17. Directive, *supra* note 1, recitals para. 58, O.J. L 281/31, at 37 (1995).

the data subject's life." This phrasing would seem to exclude, for example, financial, property, or family interests.

The final exemption concerns transfers made from *registers* intended by law for consultation by the public. The intention is that where a register in a Member State is available for public consultation or by persons demonstrating a legitimate interest, for example via the Internet, then the fact that the person consulting the register is located in a third country and that the act of consultation in fact involves a data transfer, should not stand in the way of the ability of the person to consult the register. Nonetheless, Recital 58 makes it clear that entire registers or categories of data from registers should not be permitted to be transferred under this exemption. The mass transfer of public register data for commercial purposes or the trawling of publicly available data for the purpose of profiling specific individuals would not, therefore, benefit from the exemption.

B. *Contractual Solutions*

An exemption of a different sort is included in Article 26(2) of the EU directive, following which Member States may authorize specific third country transfers if the data controller adduces *adequate safeguards by way of a contract.* The idea is that a company in a third country might provide contractual guarantees to the organization transferring the data from the Union regarding the protection to be given to the data transferred. Thus, transfers could take place even where there are no enforceable industry codes and the country has not adopted adequate privacy safeguards. The approach has attracted the attention of the U.S. business community. The International Chamber of Commerce has prepared model clauses for contracts governing the international transfer of personal data "which it believes could avoid the looming threat of a transatlantic cyber war."[18]

The application of contracts for transborder transfers has been examined by the Article 29 Group, which, while acknowledging their role, has also drawn attention to their potential shortcomings.[19] For example, the law in a third country may re-

18. INTERNATIONAL CHAMBER OF COMMERCE, ICC MODEL CLAUSES FOR USE IN CONTRACTS INVOLVING TRANSBORDER DATA FLOWS (1998); Francis Williams, *Data Protection Plans for Electronic Commerce*, FIN. TIMES, Sept. 25, 1998.

19. European Commission, Directorate General XV, Working Party on the Protec-

quire that the disclosure of information takes precedence over a contract, and individuals may find it difficult to investigate cases of non-compliance in third countries where there are no supervisory bodies. The Article 29 Group believes that the adequacy of a contractual solution should be judged in the same way as any more generally applied regulatory or non-regulatory system of data protection—it should embody a core set of data protection principles and render them enforceable. In practice, the Article 29 Group suggests, the contractual solution may be best suited to those situations where data transfers are similar and repetitive, for example credit card transactions, airline reservations, or internal company transfers and where parties to the contract are large multinational operators subject to public scrutiny and regulation. Some independent commentators, however, are skeptical as to whether, in the absence of industry codes, individual contracts are able to meet the adequacy criteria even in these situations.[20]

C. *White Lists*

Given the number of transfers of personal data leaving the Community on a daily basis and the multitude of actors involved, it will not be possible for EU data protection authorities to examine each case in detail. This stark reality has led the Article 29 Group to turn its attention towards the type of mechanisms that will need to be developed to rationalize the decision-making process for large numbers of cases, allowing decisions, or at least provisional decisions, to be made without undue difficulty, delays, or excessive costs. Although procedures for dealing with data transfers will vary from one Member State to another, the Article 29 Group has proposed that at Community level a "white list" of third countries, to whom it could be assumed transfers of personal data would be safe, be developed.[21] Such a list may be "provisional" or "for guidance only" and, therefore, without prej-

---

tion of Individuals with Regard to the Processing of Personal Data, Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries, XV D/5005/98, adopted on Apr. 22, 1998.

20. Graham Greenleaf, *A Proposed Privacy Code for Asia-Pacific Cyberlaw*, 2 J. COMPUTER MEDIATED COMMUNICATIONS 1 (visited Apr. 10, 1999) <http://shum.huji.ac.il/jcmc/vol2/issue1/asiapac.html# RTFToC1> (on file with the *Fordham International Law Journal*).

21. Transfers of Personal Data to Third Countries, *supra* note 16.

udice to cases that might raise particular concerns. The inclusion of a country in a white list would be based upon individual cases, rather than a simplified and abstract appreciation of a legal text or code. Once several representative cases of transfers to a particular third country have been considered, and for each it has been judged that the protection afforded was adequate, the country could be white listed.

First, this approach has the potential to afford a degree of legal certainty to organizations regarding those countries that could be considered as generally ensuring adequate protection. Second, it would provide a clear and public incentive to those third countries still in the process of developing their data protection systems. Third, a list at a Community level would help establish a coherent approach and prevent the emergence of differing and perhaps conflicting white lists among data protection authorities in EU States.

The adoption of a white list is not, however, without its difficulties. Principal among them is that many third countries do not have uniform protection in all economic sectors. In the United States, the situation is even more complex in that specific laws exist only in certain areas, such as credit reporting and video rental records. An added difficulty arises in countries with federal constitutions like Australia, Canada, the United States, and Switzerland, where differences often exist between the various states or provinces that make up the federation. As a consequence, it would be impossible, at present, to include very many third countries on a white list, which limits its usefulness in terms of providing the legal certainty desired. A further risk is that some third countries might come to see non-inclusion on a white list as a politically provocative step and might misconstrue non-inclusion as a judgement on their data protection system.

Despite these drawbacks, the need for such a list remains, and it is likely one will be developed even if, for reasons of presentation, it is not referred to as a white list. Moreover, it might not be limited to countries possessing horizontal data protection laws, but could include specific sectors where data protection is deemed adequate. This approach is likely to be favored in the United States where sectoral approaches are the norm. In effect, countries could be "partially" white-listed to cover a broad mass of transfers, but not necessarily in every case.

D. *Self-regulation*

The functional approach to evaluating adequate protection advocated by the Article 29 Group and the European Commission deliberately leaves open the possibility that, theoretically at least, adequacy could be delivered by industry self-regulation, rather than law. The acceptance by the Union that law is not a pre-requisite of adequacy has opened up the possibility that businesses in countries such as the United States, where government regulation is restricted, could nevertheless be considered safe destinations for international data flows if they were to develop industry codes incorporating veritable personal data protection.

Self-regulation is a broad term encompassing a wide range of different arrangements. At its best, it can offer real guarantees that an industry complies in practice with a particular set of rules, backed by genuinely dissuasive sanctions and a quasi-judicial complaints procedure. At its worst, it is pure window dressing. For the Article 29 Group, any evaluation of self-regulatory mechanisms should begin by an examination of the content of the data protection code or instruments *and* how they are to be applied in practice. The core principles of a self-regulatory code are unlikely to pose major problems in terms of evaluation, but determining how they will work in practice is far more challenging. Furthermore, difficulties may arise, particularly for consumers, when several different codes are adopted by competing representative bodies within the same industry or sector.

To help avoid some of these difficulties, the Union and United States are currently exploring the possibility of agreeing on a benchmark set of enforceable data protection principles that companies must adhere to and respect if they wish to benefit from a presumption that they are a safe destination for exporting personal data from the Union. From a EU perspective, it is important that any such benchmark guarantees respect for the principles contained in the OECD Guidelines and, given the U.S. reliance on industry self-regulation, the European Commission is seeking to ensure the presence of mechanisms that will guarantee effective enforcement of these rules.[22]

---

22. Ulf Brühann, The International Scene and the EU Directive: 5 Weeks Before Its Entry into Force, Address Before the Twentieth International Conference of Privacy and Data Protection Commissioners in Santiago de Compostela (Sept. 15-17, 1998).

III. *THE U.S. APPROACH*

Interest in the "information superhighway" has expanded rapidly in the United States over recent years. Indeed, because of the links between ICT and economic development, the U.S. Administration has come to regard its promotion as a key objective, central to which is the need to safeguard the privacy of personal data. There appears, therefore, to be a good deal of common ground between the Europeans and the Americans on this issue. The Americans, however, are cautious about supporting federal data protection legislation, unless they are convinced that the risks involved are indisputable and there is genuine evidence of market failure. Where action has been initiated, it has been in the form of segmental initiatives involving a patchwork of rules including constitutional, common, statutory, and regulatory laws.[23] A diversity of regimes exists at federal and state levels, which apply to some groups of businesses, but not others, while other rules only pertain to federal or state governments.

Despite an aversion to federal involvement, privacy issues have begun to arouse public and political interest in the United States. The Electronic Privacy Information Center ("EPIC") found that of 100 "top" web sites in the United States, only seventeen percent met basic standards of privacy protection, while Business Week recently reported that seventy-two percent of online users would use the Internet more if they felt that the privacy of their personal data and communications were respected.[24] An Act to Protect Children's Online Privacy was adopted by the U.S. Congress in October 1998,[25] while the Bennett-Jeffords Bill on the protection of medical records remains outstanding. Moreover, the U.S. Administration has recently produced a number of reports dealing with the privacy of personal data, but each has emphasized self-regulation and voluntarism.[26] "Governments should adopt a non-regulatory, market

23. *See* John F. Mogg, *Comments to the European-American Business Council* (visited Apr. 10, 1999) <http://www.privacyexchange.org/iss/confpapers/Mogg98.html> (on file with the *Fordham International Law Journal*).

24. ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 4; Heather Green et al., *A Little Privacy Please*, BUS. WK., Mar. 16, 1998, at 98.

25. H.R. 3783, 105th Cong. (1998) (Children's Online Privacy Protection Act).

26. Richard S. Rosenberg, *Privacy Protection on the Internet: The Marketplace Versus the State* (visited Apr. 10, 1999) <http://www.ntia.gov/ntia/privacy/files> (on file with the *Fordham International Law Journal*).

lead approach to electronic commerce .... [N]ew and unnecessary regulations, bureaucratic procedures on commercial activities . . . should be avoided and where government action is needed it should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."[27] The preference is for a decentralized, contractual model of law rather than one based upon top-down regulation, of the form adopted in Europe. Even in its most recent pronouncements, the United States remains steadfastly committed to private sector solutions for the implementation of consumer friendly, self-regulatory privacy.

To help encourage the development of ICT, in 1993 the Administration established a federal agency—the National Information Infrastructure Task Force ("NII").[28] In 1995, the NII adopted a core set of data protection principles intended for horizontal application across all sectors of the U.S. economy.[29] These principles were close to the standards set in both the EU directive and the OECD Guidelines, however, they have yet to be adopted as federal government policy. In April 1997, spurred on by developments in the Union and Canada, the NII outlined several alternative approaches for securing data protection, including an enhanced segmental approach, based upon existing arrangements, but with additional controls in certain sensitive areas and a federal privacy entity, with or without a regulatory function.[30] This announcement was followed in January 1998 by a further consultation document, Elements of Effective Self-regulation for Protection of Privacy[31] ("Elements Paper"), aimed at encouraging a more discriminating approach to data protection among the U.S. business community and setting out for the first time the specific principles required in any self-regulatory re-

27. PRESIDENT WILLIAM J. CLINTON & VICE PRESIDENT ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997).

28. Steven Saxby, *Public Sector Policy and the Information Highway*, 2 J.L. & INFO. TECH. 221 (1994).

29. INFORMATION POLICY COMMITTEE, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995).

30. INFORMATION POLICY COMMITTEE, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (1997).

31. Elements of Effective Self-Regulation for Protection of Privacy (visited June 29, 1999) <http://ntia.doc.gov/reports/privacydraft/198dftprin.htm> (on file with the *Fordham International Law Journal*).

gime. In November 1998, the Department of Commerce ("DOC") released a new consultation document, the International Safe Harbor Principles, ("Safe Harbor Principles") which firmed up the earlier Elements Paper into a benchmark standard to which U.S. companies could self-certify, the hope of the U.S. Administration being that the Union would be able to accept this standard as adequate.[32]

Over the past two years, U.S. business has also taken a more active interest in privacy issues. In 1996, the Electronic Frontier Foundation linked with CommerceNet to establish eTRUST (TRUSTe from June 1997), including agreement on a series of protocols aimed at establishing global trust and standards in the Internet. A year later, a number of major U.S. companies, including Netscape, Microsoft, and IBM, announced their intentions to enhance privacy in the online environment by establishing an Open Profiling Standard ("OPS") to provide for secure transmission of personal data. In July 1998, the Online Privacy Alliance, comprising a wide range of U.S business interests, announced its commitment to a privacy seal and an online privacy dispute resolution program.[33] The Better Business Bureau Online ("BBBOnline")—a body backed by a further coalition of leading U.S. companies—has also announced its intention to develop a self-regulation initiative to protect consumer privacy on the Internet.[34] Its draft program, established in June 1998, creates a privacy seal together with procedures for resolving consumer complaints.

Anxious to support self-regulation and avert legislation, these initiatives were warmly welcomed by the U.S. Administration. Indeed, following the launch of the Online Privacy Alliance, Undersecretary of Commerce David Aaron stated on July 28, 1998, that he believed that all the elements of effective privacy policies were now in place and that the way was now open to

---

32. Department of Commerce, Task Force on Electronic Commerce, *International Safe Harbor Principles* (visited on Apr. 10, 1999) <http://www.ita.doc.gov/ecom/aaron114.html> (on file with the *Fordham International Law Journal*).

33. Online Privacy Alliance, *Effective Enforcement and Self-regulation* (visited Apr. 10, 1999) <http://www.privacyalliance.org/resources/enforcement.shtml> (on file with the *Fordham International Law Journal*).

34. Better Business Bureau Online, *BBBOnline Privacy Policy* (visited Apr. 10, 1999) <http://www.bbbonline.org/privacy/index.html> (on file with the *Fordham International Law Journal*).

confirm that U.S. companies that validate these policies will meet the U.S. administration's privacy requirements.

IV. *EVALUATION OF RECENT U.S. APPROACHES*

In order to illustrate the tensions between the EU and U.S. models of data protection, the proposals of the DOC and the BBB Online have been examined in the context of the content and enforcement principles set out in the Adequacy Paper prepared by the EU Article 29 Group. A third initiative, which relates specifically to safeguarding the privacy of personal data on the Internet and which involves several major U.S. companies and the World Wide Web Consortium ("W3C"), is also investigated.

A. *Department of Commerce*

The Elements Paper[35] was intended as a consultation document for U.S. business and comprised a description of the level of protection that is considered effective and a discussion of the principles that might make up effective self-regulation. Perhaps quite deliberately, it lacked clarity both in structure and language as to those provisions that are essential or optional and which requirements are alternatives or cumulative obligations.

1. Principles of Fair Information Practices

In contrast to the EU approach, which is based upon the general application of the stated criteria, the DOC document is limited to data relating to consumers and implies that it may only be relevant in the online context. The need to ensure that individuals are provided with information about the purposes of data processing—the transparency principle—is partly met by the awareness principle in the DOC document. Nonetheless, there is a potentially significant distinction here. The EU adequacy standard envisages an active duty to provide information individually to the data subject, whereas the DOC paper implies that it is sufficient merely to make the information available. Similarly, while the choice principle in the DOC document is relatively clearly stated, it does not include a requirement to

35. Department of Commerce, *supra* note 31.

specify the purpose for which data are collected before the time of collection, which is an OECD Guidelines requirement.

There are also significant differences between the rights of access, rectification, and opposition to processing, referred to in the EU document, and the DOC consumer access principles. Crucially, the DOC recognizes that the consumer has a right only to "reasonable" access to their data, which falls well below the EU standard. Regarding the right of rectification, the Adequacy Paper grants this "where data are shown to be inaccurate," whereas the DOC paper limits it to the rather less precise notion of "where necessary." The right of opposition is catered for by the U.S. paper's choice principle, which establishes a right of opt-out. The Union aims to restrict onward transfers of data unless certain safeguards are in place, but this restriction is dealt with in only a discursive manner in the DOC paper and then only in relation to security.

The U.S. paper meets the adequacy criteria in recognizing that data should be accurate, relevant, and not be excessive in relation to the purposes for which it is to be collected. The former refers to the need for accuracy of "the extent necessary for the purpose" and while the Adequacy Paper makes no such caveat, the EU directive itself refers to "reasonable steps" being necessary to ensure accuracy. The data security principle, which is expressed in more forceful language than is used elsewhere in the DOC document, approximates to the corresponding principle in the EU adequacy standard.

The EU paper requires that additional safeguards, such as the need for explicit consent, are required in respect to the processing of sensitive data. The DOC paper, however, takes a more restrained stance and simply states that "affirmative choice," or opt-in, may be appropriate for certain kinds of information, such as medical data or data about children. This stance represents a sharp difference of approach from the specific criteria established in Article 8 of the EU directive.[36] The direct marketing opt-out seems to be covered by the choice principle in the DOC paper. It remains unclear, however, whether the individual has the right to opt out at any time, not only at the time of collection or within a time limit of being informed. Moreover, while the EU directive seeks to ensure that individuals have the

36. Directive, *supra* note 1, art. 8, O.J. L 281/31, at 40-41 (1995).

right to know the logic of any decisions about them taken by automatic means, the U.S. paper makes no reference to such a provision.

2. Enforcement Mechanisms

The DOC document states that the basic principle of an effective regime should include "mechanisms to assure compliance with the rules and appropriate recourse to an injured party when rules are not followed."[37] This provision implies that there are two objectives for the mechanisms. It is also suggested that they may take a variety of forms and that business may need to adopt "more than one," but it is unclear whether they are merely a menu of possibilities, one or more of which may be applied. It is left to the organization itself to design the means that best suit its needs and those of its customers.

The EU paper refers to the need for a good level of compliance with the data protection principles and this compliance can be broadly equated with the DOC's paper's requirement for consequences and its suggestions regarding rectification. It is far from clear, however, whether "meaningful consequences" are comparable with the Adequacy Paper's "effective and dissuasive sanctions." The need to offer individuals support and help in dealing with data protection issues is dealt with under the consumer recourse principle, which suggests that companies should offer consumers mechanisms that are readily available and affordable to resolve complaints and disputes. Nonetheless, the element of independent investigation inherent in the Adequacy Paper is missing. The EU paper also stresses redress, independent arbitration, compensation to the injured party, and the imposition of sanctions. The DOC paper makes no reference to independent adjudication, arbitration, or compensation.

B. *The Better Business Bureau Online*

1. Nature and Scope

This scheme is a self-regulatory initiative aimed at the protection of personal data in the online context. To be part of the program a company must maintain a U.S.-based website and adopt a privacy policy containing certain required elements.

37. Department of Commerce, *supra* note 31.

There is some possibility of using the "deceptive practice" provisions of the Federal Trade Commission Act against a website that professes to comply with a declared privacy policy, but fails to do so in practice. This aspect is, however, a general possibility and not a particular feature of the BBBOnLine program. Nonetheless, BBBOnLine does envisage a system of compliance assessment and the possibility of independent arbitration.

There are no explicit exemptions or restrictions in the program requirements. There is an implied restriction of the purpose/transparency provisions to data collected from the individual online, i.e., exclusion of data collected from third parties, and the access principle similarly covers only data collected online from the individual. The program requirements apply only to individually identifiable data, an expression intended to exclude data collected invisibly via cookies or other web protocols. In some EU Member States, such "invisible" data is considered as personal data.

2. Principles of Fair Information Practices

The purpose limitation principle does not exist in any clear form under the BBBOnline scheme. The privacy policy of participating companies must disclose the intended uses of individually identifiable information, but there is no prohibition on using the information later for uses not intended at the time of collection. There is a requirement to inform individuals about any choices that they have regarding the uses and disclosures of the data, but no requirement to provide such choices, except in relation to disclosures for marketing purposes. As regards other elements of the data quality principles, e.g., proportionality, participants in the program must ensure that information collected online is accurate, complete, and timely for the purpose that it is to be used. With regard to transparency, there is a requirement to provide information about the identity of the collector of the information, its intended uses, and the choices that individuals have about the way that information is used and disclosed. Only with regard to disclosures to third parties for marketing purposes, however, is the provision of choice a requirement. The individual would receive no information about disclosures to third parties for non-marketing purposes.

There is a general issue regarding the manner in which data

subjects are furnished with information. The requirement is to provide information in a privacy policy displayed on the website's home or entry page and linked to any page on which the site collects identifiable data. The probable effect of these provisions is that the individual user will have to click upon a "privacy policy" icon to be able to see the information. Information is therefore available, but not actively provided.

The BBBOnline scheme does, however, include a requirement to provide individuals *with access to individually identifiable information* collected from them online. This requirement excludes data collected from third parties or public sources. Arguably, the right of rectification is broader—a requirement on participants to establish effective and easy to use mechanisms to permit individuals access to correct inaccurate information. The right to object to the use of data for direct marketing purposes applies only to communication of data to third parties. There is no opt-out from the website using its own data for sending marketing material.

In respect of security, participants must take reasonable steps to ensure that individually identifiable data collected online is secure from unauthorized access. There are no requirements regarding other security issues, such as unauthorized or accidental disclosure or loss of data. Moreover, there are no specific requirements regarding sensitive categories of data, and, apart from the requirement to provide an opt-out from disclosures to third parties for marketing purposes, there are no conditions concerning the onward transfer of data to third parties not governed by the BBBOnLine program or an equivalent scheme.

3. Enforcement Mechanisms

The award of the privacy seal depends on prospective participants successfully completing BBBOnLine's "Privacy compliance assessment process." This process is understood to include a serious "form-filling" exercise through which companies show how they intend to conform with the program's requirements. The process must be repeated annually. With respect to consumer complaints, BBBOnLine has established a Privacy Policy Dispute Resolution Program, involving conciliation, mediation, and ultimately arbitration, and participants agree to abide by its

decisions. The scheme seeks, however, to be corrective, rather than a means by which individuals will be able to obtain compensation. Consumers will be able to bring complaints by e-mail or free telephone line. The company concerned will be able to table written evidence to which the consumer may respond. But BBBOnLine does not have its own investigative powers, and its decision about complaints will be based upon the written evidence before it. Appeals are possible. The consequences of a failure by a company to respect a decision would be removal of the seal and public identification of the company concerned, although some BBBOnLine statements have intimated that these measures might only be taken against repeat offenders. Referral to the appropriate government agency, e.g. the Federal Trade Commission or OCC, is also promised for serious or frequent offenders. Complaints against companies not part of the program will also be heard, but clearly the sanction of seal removal would not be applicable in these cases. Such non-BBBOnLine companies would also be judged only against their own published policies, not the BBB OnLine program.

In some ways the BBBOnline scheme improves significantly on the DOC's Elements Paper and subsequent safe harbor proposals. It includes a clear and unequivocal requirement to provide subject access to all identifiable data collected from individuals. The program has a compliance verification element that goes beyond simple self-certification, and there is a relatively user-friendly dispute resolution system. By EU standards, however, the purpose principle remains weak, and, as with the Safe Harbor Principles, there is no real protection in respect of data collected from third parties or public sources. Onward transfer to non-participating companies is also a problem. With respect to enforcement, the independence of BBBOnLine as an arbiter is not clear, and there are no real powers of investigation into complaints. Moreover, the system fails to provide for the awarding of damages to data subjects.

C. *Platform for Privacy Preferences and the Open Profiling Standard*

The debate about comparative privacy standards in the Union and United States is taking place against a background of rapid technological change. In the absence of an international consensus on the legal measures needed to manage global data

flows, those responsible for designing and managing the architecture of the new technologies have begun to develop technological solutions to privacy protection. The work of the W3C, which includes Microsoft and Netscape among its members, is indicative of this trend. The consortium is currently developing a filtering technology to enable Internet users to regulate their own access to websites on the basis of their own privacy preferences. The approach is one that combines market-based and technological solutions by which Internet users will be provided with control over how much personal information is collected and used online. The Platform for Privacy Preferences Project ("P3P") conceives of privacy and data protection as something to be agreed between the Internet user whose data are collected and the website that collects the data. It is based on users consenting to the collection of his personal data by a site—the Open Profiling Standard ("OPS") is intended to provide for secure transmission of a standard profile of personal data—provided that the site's declared privacy practices, such as the purposes for which data are collected and whether data are passed on to third parties, satisfy the user's requirements.

The technical protocols now being developed by the W3C will have a direct impact on the level of privacy enjoyed by online users for years to come. In June 1998, the Article 29 Working Group produced an opinion on the project setting out a number of reservations. It stated that in Europe the new protocols, likely to be included in the next generation of Internet software browsers, are viewed as an opportunity to extend Internet privacy.[38] It voiced concern, however, that if not developed and implemented carefully, the new protocols could potentially diminish levels of protection for European citizens, become a source of legal confusion, and provide only limited protection to a small number of informed Internet users. Essentially, the consortium has sought to develop a single vocabulary through which a user's preferences and a website's practices are articulated. The possibility of adapting this vocabulary to the needs and regulatory context of specific geographic regions, however, is not envisaged.

38. European Commission, Directorate General XV, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), XV D/5032/98, adopted on June 16, 1998.

The Union's view is that a technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. The use of P3P, in the absence of such a framework, risks shifting the onus primarily onto the individual user to protect himself, a development that would undermine the internationally established principle that it is the data controller who is responsible for complying with data protection standards. Such an inversion of responsibility also assumes a level of knowledge about the risks posed by data processing to individual privacy that cannot realistically be expected of most citizens.

There is also a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations—for example granting individual users a right of access to their data, if the individual user consents to this as part of the online negotiation. In fact, those businesses, organizations, and individuals established within the Union and providing services over the Internet will in any case be required to follow the rules established in the EU directive as implemented in national law as regards any personal data that they collect and process. P3P might, thus, cause confusion not only among operators as to their obligations, but also among Internet users as to the nature of their data protection rights. Browsing software that is distributed within the Union will, therefore, need to be designed and configured so as to ensure that online agreements that contradict the prevailing data protection laws in a particular country are not possible.

For users based in the Union and contacting with websites established in non-EU countries, the prime concern is that the organization to whom they are providing personal data might not be subject to the EU directive or any adequate set of effectively implemented data protection rules. Crucial to the decision of whether to provide data to such sites will be not only the approximate content of any applicable rules, but also whether there are any sanctions for non-compliance. These users should know, most importantly of all, whether a simple and effective means of obtaining a remedy is available if the rules are broken. An online platform for privacy preference should in theory be

capable of providing such information to users. The P3P vocabulary as presently constituted, however, does not require the provision of information about sanctions or remedies to users.

Given that most Internet users are unlikely to alter any preconfigured settings on their browser, the "default" position regarding a user's privacy preferences will have a major impact on the overall level of online privacy protection. According to the Article 29 Group, P3P should be implemented into browser technology with default positions that reflect the user's interest to enjoy a high level of privacy protection, including the ability to browse websites anonymously, without finding himself blocked or inconvenienced in his attempts to gain access to sites. Where an operator requests, as a condition for access to his site, the provision of a profile of identifiable data, the user should be asked each time for his consent for the provision of this information to the particular site in question. Where a site does not require such information, access could be seamless. The EU group has suggested that the major browsing software manufacturers have a responsibility to implement P3P and OPS in a manner that enhances rather than reduces levels of privacy protection.

CONCLUSIONS

Despite efforts to reconcile the conflicting approaches to data protection in the Union and the United States, there remain major disagreements about the scope of privacy safeguards and how they should be achieved. These differences stem from divergent views about the role of government and public policy in protecting individual privacy and the extent to which reliance can be placed upon organizations to regulate their own activities. By contrast to the omnibus approach to personal data protection in the Union, the U.S. Administration eschews federal action, except in specific sectors and remains committed to market driven solutions.

These contrasting approaches are apparent in several recent documents prepared in the Union and by the U.S. Administration and U.S. business. There appears to be a reluctance on the part of U.S. companies to acknowledge that privacy is a fundamental human right that needs to be reconciled with legitimate business interests. Not only is there a distaste for legisla-

tion, but also there appears to be an unwillingness among U.S. business, even where self-regulatory codes have been introduced, to accept internationally agreed standards on privacy. For the Europeans, acceptance of the OECD Guidelines is a prerequisite for concluding an agreement with the United States on the adequacy issue. But, as John Mogg, Director-General of Directorate General XV at the European Commission, stated in an address to U.S. business leaders in Washington in April 1998, "most of what we see is not meaningful . . . the industry codes we have seen have no teeth."[39] From a European perspective, it is inexplicable that while the U.S. Administration strongly supports the global regulation of Internet activities relating to intellectual property and taxation, it is opposed to the implementation of privacy safeguards

The prospect of a fundamental shift in the United States in favor of a comprehensive privacy law remains remote, although threats to consumer privacy on the Internet could yet see a reversal in U.S. political opinion. In the short term, many U.S. businesses believe that Article 26(2) of the EU directive, which provides for the creation of adequate safeguards by way of a contract, may offer a solution, particularly for companies engaged in a large number of similar transfers, while in the medium term the United States hopes to convince the Europeans that industry self-regulation is capable of providing genuinely effective protection. The European Commission has become more sympathetic to these approaches during its discussions with the U.S. Administration. It is by no means certain, however, that contracts and self-regulation alone will be sufficient to persuade the Union that U.S. companies are safe harbors for personal data on EU citizens. Indeed, reliance on these provisions remain problematic, and U.S. businesses will increasingly find themselves depending upon a variety of options in efforts to convince the Union that they have met the adequacy requirements.

From a European perspective, the key weakness of the U.S. model lies in its approach to the transparency and access principles and the still half-hearted approach to enforcement. The ability of individuals to control the use of their personal data, to obtain access to it, to gain support in the exercise of their rights and, ultimately, to obtain appropriate redress where rules have

39. Mogg, *supra* note 23.

been breached are perceived as essential to meeting the EU adequacy criteria. The presence of an independent U.S. data protection entity at federal level, charged with powers to hear and investigate complaints and, if necessary, to initiate judicial proceedings would, in European terms, represent a major step towards achieving these objectives. The fragmentation of U.S. data protection responsibilities is likely to become increasingly apparent as the EU directive becomes operational and appropriate institutional arrangements in the United States would seem essential, both to defend its business interests and to resolve potential political friction between the Union and the United States. Such an entity would be an ideal interlocutor for European data protection authorities and for consumers seeking redress.

In practice, it seems probable that the privacy standards of some major U.S. companies will be accepted as adequate by the Union and will be designated as "safe harbors" in data protection terms, but some will fail to meet the criteria. From the outset the EU approach is likely to be cautious. Its first priority will be to take action against specific transfers that pose particular threats to personal privacy. Transfers involving sensitive data, the human resource data bases of multi-nationals and sub-contractors, operating on behalf of EU companies are all potential targets. Secondly, the Union will "cherry pick" those U.S. businesses where the industry sector has well-established bodies and regulatory systems that guarantee effective enforcement mechanisms[40] and gradually begin to recognize these sectors as adequate. At the same time, the Union will be anxious to avoid recognizing a multiplicity of U.S. self-regulators in the same functional area. The intention will be to stimulate other businesses in the United States and other third countries to adopt adequate standards of protection.

The position of the U.S. Department of Commerce remains difficult, having both to represent recalcitrant U.S. business interests and to engage in purposeful negotiations with the Union. Its consultation documents have aimed to reconcile these conflicts, the most recent attempt being its International Safe Har-

40. Peter Q. Swire & Robert E. Litan, *Avoiding a Showdown over EU Privacy Laws*, Brookings Institute Policy Brief No. 29 (Feb. 1998); Colin Bennett & C.D. Rabb, *The Adequacy of Privacy: The European Data Protection Directive and the North American Responses*, 13 INFO. SOC'Y 245 (1997).

bor Principles, which are regarded by the U.S. Administration as a further opportunity to establish a bilateral agreement with the Union. However, recent experience implies that every effort will be made to water down the Safe Harbor Principles to assuage U.S. business interests. The European Commission is clearly aware of this prospect and is likely to respond accordingly. Agreement on the adequacy for EU purposes of the Safe Harbor Principles is possible, but a number of important issues will need to be resolved if this is to happen. It seems unlikely that the Union will be prepared to accept the adequacy of a system based solely on the self-certification of U.S. companies and which lacks any means of redress for individuals, particularly if some of the key data protection principles, such as the right of access, are not properly guaranteed.

While the Union has committed itself to a regulatory approach to data protection, the architecture of the new information technologies is dictated by U.S. companies. They dominate the world market in ICT and are able to exert considerable leverage in determining the privacy protocols to be used in software. Some observers have contended that in the context of myriad data flows, regulation is not feasible. The configuration of information systems, however, can be used to support legal solutions, and the Union has recognized this through its support for privacy enhancing technologies. The links between data protection law and the architecture of the World Wide Web are clearly evident in relation to P3P.[41] It is uncertain, however, whether the W3C will be willing to modify their recommendations and technical protocols to accommodate the values underpinning the EU privacy model, although this is indispensable if national laws are to be observed.

In addition to its involvement with the United States, the Union is increasingly being drawn into bilateral discussions with other states, which may, in the medium term, enable issues relating to transborder personal data flows to be considered in a multilateral context. Other non-EU states including Canada, Australia, Taiwan, Norway, Iceland, Hong Kong, Poland, Hungary, and

41. *See* Graham Greenleaf, *Architecture v. Law*, 21 U. OF NEW S. WALES L.J. 2, (Apr. 10, 1999) <http://www.austlii.edu.au/au/other/unswlj/issues.html# V21N2THEME> (on file with the *Fordham International Law Journal*); Joel Reidenberg, *Lex Informatica*, 76 TEX. L. REV. 553 (1998).

Switzerland either posses or are in the process of adopting privacy laws similar to the Union. In trading terms, Article XIV of the General Agreement on Trade in Services[42] ("GATS") legitimizes the blocking of data transfers, and the Union has already indicated its interest in improving on this arrangement to secure a more binding multilateral agreement under the World Trade Organization, similar to the Agreement on Trade-Related Aspects of Intellectual Property Rights[43] ("TRIPS Agreement") governing intellectual property. This could offer a way forward. Indeed, from an EU perspective, public calls in the United States to guarantee Internet privacy and the adoption of data protection laws by so many of the United States trading partners offer perhaps the best chance of encouraging U.S. companies to acknowledge the benefits of a global accord for safeguarding privacy for both business and consumers.

42. Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, General Agreement of Trade in Services, Apr. 15, 1994, Annex 1B, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 31 (1994), 33 I.L.M. 1167 (1994).

43. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 31; 33 I.L.M. 81 (1994).