Hastings Law Journal

Volume 54 | Issue 4 Article 6

1-2003

Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?

Andrew Charlesworth

Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?

ANDREW CHARLESWORTH*

Introduction

In mid-2002, the Commission of the European Union ("EU") initiated a review[1] of the operation of the 1995 Data Protection Directive ("DPD"),[2] which the fifteen EU Member States were to have implemented into their national laws by October 1998. It might seem strange to the casual observer for there to be a wide-ranging review of the impact of a piece of legislation that was barely six years old, and which had been implemented in most of the Member States for considerably under three years.[3] However, the Commission's desire for a re-evaluation of the legislation stemmed largely from the perception that the aims of the Directive, whether these were to ensure the effective flow of personal information in the European Single Market, or to ensure the right of European citizens to control the uses to which their personal data were put, were not being adequately met by national legislative implementations and administrative practice.

---

* Andrew Charlesworth, Senior Research Fellow in IT & Law and Director of the Centre for IT & Law, Departments of Law and Computer Science, University of Bristol, UK., a.j.charlesworth@bristol.ac.uk. The Centre for IT & Law is sponsored by Vodafone Group Services Ltd, Barclaycard, Herbert Smith, Hewlett Packard Laboratories and the Law Society Charitable Trust.

1. *See* Press Release, European Commission, Data Protection: Commission Seeks Views on Privacy Legislation (June 25, 2002) (IP/02/923).

2. Council Directive 95/46/EC, 1995 O.J. (L 281) 31–50 [hereinafter DPD].

3. Although the implementation date for the Directive was October 1998, by October 1999 only six of the fifteen Member States had achieved full implementation. The UK, for example, did not achieve full compliance with the Directive until March 2000. Indeed, at the start of the Commission's review process in 2002, three Member States, France, Luxembourg and Ireland still did not appear to have fully implemented the Directive's provisions into their national laws.

A further matter to be considered was that the Directive was drafted, debated, and implemented at a time of rapid technological change. The Commission originally introduced the draft legislation in 1990,[4] but this version proved highly unpopular with the Member States and the commercial sector. After protracted discussions with the Member States and the European Parliament, the Commission produced a considerably restructured proposal in October 1992.[5] Despite the radical overhaul, a Common Position was not reached in the Council of Ministers until February 1995, and the Directive was only finally adopted in October 1995, five years after its initial introduction.[6] When one plots this gestationary timeline against, for example, a timeline of Internet developments,[7] it is clear that the technological environment at the end of that period was very different from that at the start. In 1990, the Internet was largely uncommercialized, and key tools such as Wide Area Information Servers ("WAIS"), Gopher, PGP, and the World Wide Web were still a year away; by 1995 Internet users were already acquainted with Netscape, RealAudio and JAVA, as well as the terms "spam" and "banner ads," and by the time the Directive was supposed to be implemented by the Member States in 1998, the terms "e-commerce," "e-auctions," and "portals" were common parlance.

The Internet was not the only technological arena undergoing explosive change during this period; the commercial sector too was coming to terms with a range of new technologies which, in combination with the transnational opportunities provided by the increasing popularity of free trade, were transforming business practices. Many of those practices involved the transfer of personal information about EU citizens, not just within the EU, but considerably further afield, to countries where the cost of "back office" or "remote processing" could be significantly reduced.[8]

4. Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) 314 (July 27, 1990).

5. Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data, COM (92) 422 (Nov. 27, 1992).

6. *See* Nick Platten, *Background to and History of the Directive*, *in* DAVID IAN BAINBRIDGE, THE EC DATA PROTECTION DIRECTIVE at 13–32 (1996); Graham Pearce & Nick Platten, *Achieving Personal Data Protection in the European Union*, 36 J. COMMON MKT. STUD. 529 (1998).

7. *See* Robert H. Zakon, Hobbes' Internet Timeline v6.0 *at* http://www.zakon.org/robert/internet/timeline (Feb. 5, 2003).

8. Robert Marquand, *Fast, Cheap, and in English, India Clerks for the World*, CHRISTIAN SCI. MONITOR, Apr. 30, 1999, at 7 (noting that India has become an extremely popular location for such processing with estimates suggesting that the back-office sector in India grew from $15 million to $300 million between 1996 and 1999 alone).

The Commission's review process was thus driven, in part, by the perception that the Directive had not aged well given the rapid developments in the related fields of information technology and modern business practice, and also by the recognition that, far from creating a harmonized area of law, the broad statements of intent in the Directive had resulted in the Member States creating a diverse patchwork of legal and administrative rules, which not only hampered transborder data flows between EU Member States and non-Member States, but also militated against the key aim of the Directive by creating barriers to the efficient flow of personal data between the Member States themselves.

Thus, while some positive benefits had arisen from the implementation of the DPD, notably the acceptance across the EU of the need for a minimum level of legislative protection for personal data privacy, premised on the Council of Europe Convention 108/81 for the protection of individuals with regard to automatic processing of personal data,[9] and the Fair Information Practice Principles in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,[10] there remained a lack of coherency and consistency to the Member States' approach which prevented the attainment of true harmonization—the "one law from many."

The Commission itself can be criticized for failing to provide sufficient oversight and guidance in the implementation process, and its key policy review body, the Article 29 Working Party,[11] has been criticized as both lacking transparency in its deliberations, and flexibility in its opinions.[12] In the view of a significant number of data controllers, this has resulted in varying degrees of over-regulation by the Member States. When combined with a lack of willingness by some national data protection regulators to endorse the use of alternative measures to aid efficient and effective compliance with the law, for example, the lack of consensus over the use of contractual

9. Council of Europe Convention 108/81, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 20 I.L.M. 317 (E.T.S. 108), 20 I.L.M. 422 (E.T.S. 181).

10. Organisation for Economic Co-Operation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Oct. 1, 1980 (final), C(80) 58, 20 I.L.M. 422.

11. The Article 29 Working Party is an advisory group, set up by the DPD, composed of representatives of the data protection authorities of the Member States. It acts independently and examines any questions concerning the application of the national measures adopted under the DPD to foster the uniform application of such measures. *See* http://europa.eu.int.

12. *See* International Chamber of Commerce, Comments on the Review of the EU General Data Protection Directive, 2–3 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/icc_en.pdf (May 28, 2002).

terms by data controllers to overcome the problems posed by national adequacy rulings (or, more accurately, the lack of them) in the area of transborder data flows, this has made it almost impossible for data controllers to comply with the requirements of the Directive.

The Commission's initiative, which took the form of a somewhat unscientific consultation by means of a set of online questionnaires for data controllers and data subjects,[13] a call for position papers from interested parties,[14] and a two-day conference held in Brussels on September 30–October 1, 2002,[15] looks likely to result in the Commission making few, if any, changes to the substantive legislation, seeking instead to adjust the EU data protection regime through administrative change at the Member State level. Such changes would involve simplifying the notification process for data controllers; ensuring better dialogue between the Community data privacy institutions (notably the Article 29 Working Party), national data protection authorities, and data controllers; requiring a greater degree of cooperation between the national data protection authorities; increased promotion of the use of self-regulatory mechanisms and Codes of Conduct; making provision for more flexible arrangements for transborder data flows, in particular for flows to non-EU states; and encouraging the use of privacy enhancing technologies ("PETs").[16] The Commission's aim is thus to attempt to attain the as yet distant goal of functional data privacy harmonization without having to further water down the individual data privacy protection provided by the Directive, or by trying to adopt further, more prescriptive, legislation to force the Member States into conformity, an approach which would likely face stern resistance from both Member States and the commercial sector.[17]

13. Questionnaire for on the implementation of the Data Protection Directive (95/46/EC): Results of the on-line consultation *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/consultation-citizens_en.pdf (June 20–Sept. 15, 2002).

14. Consultation on the implementation of the Directive 95/46/EC *at* http://europa.eu.int/comm/internal_market/privacy/lawreport/paper_en.htm.

15. Data Protection Conference and Report on the implementation of Directive 95/46/EC: Programme and Speeches *at* http://europa.eu.int/comm/internal_market/privacy/lawreport/programme_en.htm.

16. Speech by Commissioner Frits Bolkestein, Closing Remarks at European Commission Conference on "Data Protection," Oct. 1, 2002 *at* http://europa.eu.int/comm/internal_market/en/speeches/spch-02-439_en.htm.

17. *Id.* (stating that given the difficulties in reaching an agreement acceptable across the Member States with regard to the 1995 Data Protection Directive, the likelihood of the Commission attempting a more restrictive form of Directive, or even a Regulation, remains very much an option of last resort).

While some of the proposed administrative changes would appear to be relatively uncontroversial—for example, the use of a more open and transparent Article 29 Working Party to identify divergences in Member States policy and to suggest methods by which these could be reduced; and the simplification of the notification process, a system that is universally unpopular, not even viewed with any enthusiasm by the UK, the Member State from whose data privacy legislation it was derived—several of the other proposals are likely to be rather less popular with some national authorities and the general public. While they may be presented in terms of increasing harmonization and optimizing enforcement, they may also be viewed as either weakening the protection provided by the Directive, or potentially misleading data subjects about the extent to which their personal data is in fact protected.

I. New Proposals for Optimizing Enforcement

Much of the information in this section is drawn from discussion at the Commission's Data Protection Conference in Brussels and also from the written responses of interested parties to the European Commission's request for position papers on the implementation of Directive 95/46/EC.[18] It should be noted that the written responses received by the Commission were overwhelmingly dominated by those submitted by commercial interest groups and law firms; responses and representations from individuals, or from consumer or citizen representative groups, were few and far between. A number of the organizations that responded to the European Commission's request for position papers were concerned primarily, or exclusively, with their own sphere of operations.[19] However, a clear set of generic issues of concern can be derived from wider study of the position papers.

18. Consultation on the implementation of the Directive 95/46/EC, *supra* note 14.

19. *See* European Market Research Alliance, Position Paper regarding the Review of the EU General Data Protection Directive (Aug. 23, 2002) *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/emra_en.pdf; Comité Européen des Assurances, Comments by Comité Européen des Assurances concerning the Application of Directive 95/46/EC on Personal Data Protection *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/cea_en.pdf (Nov. 12, 2002); British Music Rights, Implementation of Data Protection Directive (95/45/EC) *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/britishmusic_en.pdf (Oct. 14, 2002). The most unusual submission is probably that from British Music Rights whose only apparent interest in the Directive is to ensure that it should not obstruct the ability of intellectual property rights' owners to obtain from Internet service providers the names and addresses of individuals disseminating illegal copies of copyrighted materials online.

The four areas that will be considered here are:

- the need to establish a coherent legal regime relevant to data protection;
- the need for changes to administrative practices in the area of business related transborder data flows between the Member States, and between Member States and third party States;
- the wider use of PETs; and
- the promotion of self-regulation and Codes of Practice.

The use of the latter two methods, in particular, is often discussed in the context of attempting to find alternatives to formal legal regulation, but here they are considered as supplementary to it. This combined legislative and administrative approach may, to an extent, ameliorate the more obvious criticisms made of these administrative methods when they are proffered as a solution for achieving personal data privacy in their own right.[20]

A. A Coherent Legal Regime for Data Protection

Commentators from outside the EU sometimes appear to view the EU's data privacy regime as a tightly drawn supra-national framework in which all Member States are in close agreement.[21] While such a minimalist portrayal may be of value when arguing the pros and cons of the approach taken by the Directive and the approach taken by other non-EU states, a more nuanced analysis soon shows that the EU data privacy regime is far from a coherent whole. Indeed, the perception amongst commercial organizations operating within the EU seems to be that, while they may object in principle to various elements of the Directive, it is often the inconsistencies between Member State implementations that cause them the greater financial and administrative problems. These inconsistencies stem primarily from three main sources: first, that not all the Member States have implemented the Directive; second, that the harmonization proposed in the Directive has not in fact occurred; and third, that there are now several pieces of potentially conflicting EU legislation dealing with issues related to data privacy.

20. *See also* Andrew Charlesworth, *Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual in* LAW AND THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE 79 (Lilian Edwards & Charlotte Waelde eds., 2000); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. REV. 847 (1998); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999); Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices*, 2000 WIS. L. REV 743.

21. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS (1998).

(1) Failure to Implement

In order for there to be effective harmonization of the legal regime for data protection in the EU, it is essential for all Member States to have implemented the Directive. Achieving this goal, however, has proven to be no easy task, due to significant resistance on the part of some Member States. When the date for implementation passed, in October 1998, the Commission would have stepped up its formal pressure on those Member States who failed to meet the deadline by requesting reasons for the failure. By July 1999, it had begun the second stage of formal infringement proceedings under Article 226 EC[22] by sending "reasoned opinions" to nine Member States[23] noting their failure to notify all the measures necessary to implement the Directive. Finally, in January 2000 the Commission brought legal actions before the European Court of Justice against five Member States—France, Luxembourg, the Netherlands, Germany, and Ireland—on the grounds of continuing failure to meet their Community obligations. Since then, Germany, the Netherlands, and Luxembourg have notified implementing measures. However, to date, only Luxembourg appears to have received a formal ruling against it by the European Court of Justice for non-implementation[24] and the current status of the cases brought against France and Ireland is unclear. Neither has implemented the

22. Article 226 EC provides the procedure by which the European Commission can enforce the observance of EC law by the Member States. This takes place in several stages:

there are informal negotiations between the two parties;

if no satisfactory conclusion is reached, the Commission will send a letter of formal notice pointing out the specific infringements of Community law, for example non-implementation of a Directive within the set time period, and asking Member State to explain the reason for the infringement;

if the Member State neither provides an acceptable reason, nor remedies the infringements, the Commission issues a 'reasoned opinion' which sets out the legal grounds and submissions that the Commission will be seeking to rely upon should proceedings be started before the European Court of Justice, the measures the Commission feels should be taken to end the breach, and a time limit for the Member State to comply;

if the infringement continues, the Commission may bring a procedure for enforcement before the European Court of Justice requesting a ruling that the Member State has not fulfilled its obligations under EC law.

Continued infringement by a Member State after the ECJ has found a failure to meet its Community obligations may result in financial penalties being imposed under Article 228 EC.

23. France, Luxembourg, the Netherlands, Germany, the United Kingdom, Ireland, Denmark, Spain, and Austria.

24. Case 450/00, Commission v. Luxembourg, 1 E.C.R. 7069 (2001) *available at* http://www.etat.lu/memorial/memorial/a/2002/a0911308.pdf (Luxembourg adopted a new data protection law in August 2002, which entered into force in December 2002).

Directive, although both have now placed draft implementing legislation before their national legislatures,[25] which action may have persuaded the Commission not to pursue the legal avenue. However, as both nations have pre-existing national data privacy laws,[26] this presents potential problems for companies operating within those countries in terms of deciding which law they are required to comply with, the existing national law, or the EU Directive. This has brought calls for a more vigilant approach to implementation by the Commission, as well as for the Commission to have further recourse to the European Court of Justice.

(2) Lack of Harmonization

It is obvious from the discussions at the Commission's Data Protection Conference in Brussels, and in the representations made by many of the organizations that responded to the European Commission's request for position papers, that a pressing concern was the fact that where Member States had implemented the Directive they had signally failed to liaise with regard to issues such as terminology and procedural requirements, so as to achieve practical, as opposed to theoretical, harmonization of national laws, and that this was causing difficulties for organizations wishing to transfer personal data within the EU, and from the EU to third party nations.

It is, of course, unlikely that the Commission would have expected the Directive to have achieved full harmonization of Member State laws in the short to medium term, or indeed that full harmonization would necessarily have been the Commission's goal. The nature of EU directives, as opposed to EU regulations,[27] is to set out a legislative goal for the Member States, to be reached by a certain date, but to allow them significant discretion as to how exactly that goal will be obtained within their national legal systems.[28] This element of discretion afforded to the Member States often allows for agreement to be reached in the Council of Ministers, where

25. European Commission, Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data *at* http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm.

26. Data Protection Act No. 25, 1988, *available at* http://www.dataprivacy.ie/6ai.htm (data protection provision in Ireland); Loi N° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *available at* http://www.cnil.fr/textes/docs/loi78-17.pdf (data protection provision in France).

27. EU regulations become part of a Member State's national law in their entirety and without any need for Member State implementation—they are thus deemed to be "directly applicable." Treaty Establishing the European Community, Nov. 10, 1997 O.J. (C 340) 3 [hereinafter EC TREATY], art. 249(2).

28. *Id.* at art. 249(3).

agreement on more prescriptive legislation in the form of a regulation, might be harder, if not impossible, to obtain.

Thus, while the use of regulations in the area of harmonization is not unknown, in practice most harmonizing legislation takes the form of directives. In this case, as the attitude of the various Member States to the concept of personal data privacy during the negotiations leading to the adoption of the Directive varied from indifference, through pragmatic acceptance, to its elevation to a quasi-human right, the choice by the Commission of a harmonizing Directive rather than a Regulation is hardly surprising. On the principle that past experience has shown that Member States have become increasingly adroit at implementing interpretations of directives that suit their national predilections and biases, the Commission would almost certainly have expected that there would be considerable initial differences between the Member States' implementing laws, and that to achieve effective harmonization might take time and require either further intervention by the Commission, informally via negotiation, or formally by way of the Article 226/228 EC compliance mechanism, or by the European Court of Justice in the form of Article 234 EC preliminary rulings[29] on the interpretation of the Directive.

This approach to harmonization of Member States' laws, while serving the Commission well enough in other areas of EU activity, seems to be untenable in the area of data privacy, largely because, as discussed earlier, it is unable, within an acceptable timeframe, to achieve the degree of harmonization now required by the pace of developments in information technology and modern business practice. The extent to which the existing legal framework for data protection lacks basic consistency is demonstrated neatly by the fact that of the fifteen Member States, four protect the personal data of "natural" and "legal" persons in their data protection laws,[30] while the remaining eleven protect only the personal data of "natural" persons.

29. *Id.* at art. 234.

> The Court of Justice shall have jurisdiction to give preliminary rulings concerning:
>
> (a) the interpretation of this Treaty;
>
> (b) the validity and interpretation of acts of the institutions of the Community . . .
>
> Where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the Court of Justice to give a ruling thereon.

Id.

30. Austria, Denmark, Italy, and Luxembourg.

In comparison to most national legislation, which tends to be drafted in precise detail, EU directives are often drafted in fairly sweeping terms, in part to avoid interfering unduly with the Member States' right to choose the form and method of implementation. This provides considerable scope for interpretative license on the part of the Member States, even in relatively uncontroversial areas. A common complaint about the DPD is that a number of its key terms were either not defined, or not adequately defined, and that neither the Commission nor the Article 29 Working Party provided adequate terminological guidance to the Member States during the implementation period. This resulted in differing legislative rules and administrative practices being adopted by the Member States. When one considers that examples of differing definitions between the Member States include those for such key terms as "data controller," "data processor," "sensitive data," "anonymous data," "consent," "third party," "establishment," and "equipment," one may get some sense of the difficulties involved for a commercial organization in achieving cross-border data privacy compliance.

Where definitions were provided in the DPD, they were often so wide-ranging as to be rendered meaningless when passed through the implementation process. For example, while the definition of "sensitive data" (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life[31]) in the Directive is quite broad to begin with, some Member States appear to have defined "sensitive data" considerably more widely than others. For example, Portugal includes data about the "private life" of the individual within the definition, thereby requiring express consent for collection of data on consumer and household habits,[32] whereas in the UK such data would almost certainly be treated as "non-sensitive" personal data and would require a correspondingly lower degree of protection.

Additionally, it can be seen that, if applied strictly, the categories of "sensitive data" require the same test to be applied both to data which are of extreme sensitivity, and to data which fall within the broad definition, but which may be considered relatively trivial in nature. This can be seen in the context of "data concerning health," which could cover anything from the processing of data relating to an individual's AIDS/HIV+ status, which is undeniably highly sensitive

31. DPD, *supra* note 2, at art. 8(1).

32. EU Committee of the American Chamber of Commerce in Belgium, Position Paper on the review of Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/amcham_en.pdf (Aug. 7, 2002).

personal data, to the processing of data relating to an individual's absences from University tutorials due to illness, which seems to be an altogether less potentially damaging activity. As the British Bankers Association puts it:

> Minor injuries are bracketed with highly sensitive personal information and require the same degree of specific consent. All processing [sic] should undertake risk assessment, and ensure that suitable measures are taken to ensure fair and lawful processing takes place and also that appropriate security measures are applied.[33]

Certainly, with hindsight, the decision to create two categories of personal data in the Directive seems an unnecessary complication, as data controllers are in any event required to process fairly and lawfully, regardless of the type of data. Indeed, the UK Information Commissioner, in her response to the UK Home Office's Public Consultation exercise on the implementation of the Directive in 2000, commented that:

> The concept of "sensitive data" is misguided. Sensitivity depends on context. It is best addressed by appropriate interpretation of the data protection principles. The conditions for processing sensitive data do not achieve their aim.[34]

However, whatever the merits of such a change, unless the existing Directive is to be heavily amended, or even replaced, it seems unlikely that the distinction between "sensitive" and "non-sensitive" data can be easily removed.

Concerns have also been raised that, by creating such broad definitions as that for "personal data,"—"any information relating to an identified or identifiable natural person"[35]—the Directive was causing significant unnecessary difficulties with established and uncontroversial business practices. An example of this was raised by a number of parties, including the International Chamber of Commerce[36] and the European Privacy Officers' Forum ("EPOF"),[37] which noted that the existing definition of "personal data" in the Directive and in Member State laws made no distinction between an individual's personal data in their employment capacity, as opposed to their personal capacity, and suggested that to treat "professional

33. British Bankers' Association, Data Protection in the Community: EU enquiry on the implementation of privacy legislation, Comment 12 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/bba_en.pdf (Sept. 20, 2002).

34. Lord Chancellor's Department, Data Protection Act 1998: Post-Implementation Appraisal, art. 8 *at* http://www.lcd.gov.uk/ccpd/dparesp.htm#part13 (Dec. 2001).

35. DPD, *supra* note 2, at art. 2(a).

36. International Chamber of Commerce, *supra* note 12, at 2.

37. The European Privacy Officers' Forum, Comments on Review of the EU Data Protection Directive (Directive 95/46/EC) *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/epof_en.pdf (July 31, 2002).

data," which caused no obvious threat to the individual's right of privacy, in this manner was an unnecessarily strict approach.[38] This interpretation would seem to accord with the attitude of the UK Information Commissioner's Office, which has taken the broad line that, in the absence of a pressing privacy rationale,[39] "professional data" such as information specific to the employment, business, or professional responsibilities of a data-subject including name, job title, workplace contact details, and description of activities and transaction would not normally require application of the full panoply of data protections.[40]

A final example of the difficulties caused by the definitional vagaries of the Directive can be seen with the concept of "consent." The construction of the Directive means that there is a significant role for data subject consent with respect to the fair and lawful processing of their data, both "non-sensitive" and "sensitive." While there are other grounds under which fair and lawful processing may take place, for example, the "balance of interests" ground, which allows processing which is necessary for the legitimate interests of the data controller where the processing does not cause undue prejudice to the fundamental rights and freedoms of the data subject,[41] consent is often the ground on which data controllers would prefer to justify their processing.[42] However, the Directive is vague as to how consent might be conveyed, beyond providing that the standard should be higher in the case of "sensitive" data.

38. *Id.* at 3–4.

39. For example, employment details about individuals who work in the area of animal experimentation, and who might be identified and targeted for physical attack by animal rights campaigners on the basis of that information, or an employee who has been the subject of spousal abuse and who wishes for their whereabouts to remain undisclosed.

40. This issue has been raised, in particular, in the context of websites (which are generally, by their very nature, accessible to the world, which raises the matter of data transfer outside the EU/EEA to countries without adequate protections for data privacy) and the extent to which employers are entitled to place details of their employees on websites without first obtaining their consent.

41. DPD, *supra* note 2, at art. 7(f). This basis for processing is not itself uncontroversial, as the Member States have adopted different approaches to its interpretation—providing a harmonized approach on the issue of what is "unduly prejudicial to the fundamental rights and freedoms of data subjects" requires agreement on what those fundamental rights and freedoms are, as well as on the scope for, and degree of, prejudice in any given context. Here again, commercial enterprises are likely to be prevented from constructing a Europe-wide "balance of interests" test for their data processing operations. *See* EU Committee of the American Chamber of Commerce in Belgium, *supra* note 32, at 6.

42. Allen & Overy, Data Protection Directive (95/45/EC) Questionnaire: Position Paper for Discussion at the Data Protection Conference from Allen & Overy on Behalf of its Clients, 2 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/allen-overy_en.pdf (Aug. 30, 2002).

> [Consent] shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.[43]
>
> [Non-sensitive] personal data may be processed only if . . . the data subject has unambiguously given his consent.[44]
>
> [Sensitive personal data may be processed only] if the data subject has given his explicit consent to the processing of those data.[45]

Quite what the practical difference is between "unambiguous" and "explicit" consent remains unclear—the Directive does not specify that consent should be obtained in any specific form. Certainly, the Member States do not appear to have reached a common consensus on the matter. For example, it appears that Italy requires that consent must be "freely expressed," "specific," and "documented in writing,"[46] which may cause difficulties with consent which has purportedly been given online. In Germany the standard for consent appears to be based on the "opt-in" model, where the data subject must make some positive indication of consent, such as ticking a check box, while in the UK, it appears that implied consent, such as where the data subject has failed to tick an opt-out box, or where a customer, having been notified of new data processing purposes, continues to use the facilities provided by a company, will suffice, at least for the processing of non-sensitive data.[47]

Leaving aside definitional issues in the legislative implementation, the legal requirements and administrative procedures adopted by the Member States and their national data protection authorities also vary greatly. An example of this would be the various implementations of the Directive's requirement for a data controller to delete customer data. Citigroup noted that:

> [i]n Spain, the requirement is to delete all data from records held by the data controller as soon as the relationship ends, which makes it difficult to resolve questions or disputes of former customers. In the UK, data can be kept for a reasonable period of time after the relationship ends. In Greece, the retention period for data can be extended only with the approval of the local Data Protection Authority.[48]

It also appears that the data retention requirements in Member States' data protection laws do not always mesh with the

43. DPD, *supra* note 2, at art. 2(h).

44. *Id.* at art. 7(a).

45. *Id.* at art. 8(2)(a).

46. Confindustria, Implementation of Directive 95/46/EC in Italy, 1 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/confindustria_en.pdf.

47. EU Committee of the American Chamber of Commerce in Belgium, *supra* note 32, at 6.

48. Citigroup, Review of the EU Data Protection Directive, 3 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/citigroup_en.pdf (Aug. 22, 2002).

requirements of their own financial services laws and regulations, let alone those of other Member States. With regard to data security measures, here too the legal requirements are far from uniform, with the Spanish law on database security being held up as an example of security taken to extremes, as it requires that each database has a security protocol describing the full technical system, the security measures, and the circumstances that affect the database, and a mandatory audit every two years.[49] In contrast, the UK provisions leave the data controller to determine the level of security appropriate to the data held, and there is no requirement to state the level of that security or a requirement of audit.

The notification requirement, whereby data controllers must notify the national authorities of the countries in which they process data of the nature and scope of their processing operations, arouses particular angst among commercial data controllers, with many of the respondents to the Commission's call for position papers indicating their dislike of the process. Most would find the process unnecessary and burdensome, even if it were a standardized process across the EU,[50] but as one respondent commented:

> Countries such as Denmark, Finland, Germany, Sweden, and the UK have adopted a minimalist approach with broad exemptions and short, relatively simple notification forms. Other countries, such as France and Spain, have adopted few or no exemptions, and use lengthy, complicated forms. Moreover, DPA notification forms generally are inflexible, and do not permit an adequate description of the data processing operation.[51]

Many respondents thus suggested the abolition of the entire notification process, although the majority recognize that unless there is a major alteration to the Directive, such a radical change is probably not an option. As an alternative, a number of respondents suggested that companies processing data in more than one Member State might be permitted to notify in a central EU data protection office, or be able to notify in a single Member State and have that

49. EU Committee of the American Chamber of Commerce in Belgium, *supra* note 32, at 10.

50. The UK Information Commissioner Elizabeth France herself has queried the usefulness of notification in her response to the Home Office's Public Consultation exercise in 2000, noting that "[t]he notification provisions impose burdens which are disproportionate to any benefits. If retained, they should be limited to the provision of details about controllers and the nature of their business." Lord Chancellor's Department, *supra* note 34, at Part B.

51. Covington & Burling, Comments on Implementation and Application of the 1995 Data Protection Directive, 5 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/covington-burling_en.pdf.

notification recognized as valid in the other Member States on the principle of "mutual recognition."[52]

It will be apparent from the foregoing that the harmonization problem will be difficult to overcome as, left to their own devices, the Member States appear unlikely to manage a rapid convergence of their data protection laws. The Commission is thus essentially faced with a short list of choices:

- It could decide to exchange the Directive for a Regulation. The key benefit of this would be the ability to set a uniform set of definitions and standards across the Member States by removing the Member States' discretion to choose the manner and form of an implementing measure. The main objection to such a move is that it would be difficult and ultimately extremely time-consuming to attempt to reach agreement on a set of definitions and standards that would then be imposed on the Member States. Even though it is arguable that the Member States are now much closer in their understanding of the nature and scope of data privacy law than they were in the early 1990s, there are still significant differences that would be difficult to overcome. Additionally, given the on-going implementation of the Directive, and the associated work taking place in relation to cross-border data transfers both within and outside the EEA, to undertake such a radical change in EU policy would probably be counter-productive.
- It could undertake a major revision of the existing Directive. Given that the Directive has clearly failed on a number of levels to achieve even a minimum harmonization of Member State laws, a major revision might seem appropriate. That having been said, such a major revision would face similar time problems as the first option, and there would be further scope for Member State delays in implementation. It also appears that the Commission is unconvinced that the difficulties faced by commercial organizations are caused, or exacerbated, by the Directive itself rather than by national implementation, or national enforcement practices. If that is the case, a revision of the Directive is unlikely to lead to a significantly improved degree of harmonization than can be achieved, in time, by the existing legislation.
- It could pass additional specific directives in various areas of activity. This approach was being mooted even before the Commission began its review, and both the Directorate-General for Employment and Social Affairs of the European

52. *Id.* at 4–5; *see also* Confederation of British Industry, Comments on Directive 95/46 EC re data protection, 11–12 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/cbi_en.pdf (Aug. 10, 2002).

Commission[53] and the Article 29 Working Party[54] have produced documents relating to employee data privacy, which suggests that this might be an area where a specific directive could be considered. However, further specific legislation is likely to meet with stiff resistance from both Member States and from commercial organizations which are still, in many cases, coming to terms with the original directive. Indeed, as noted below, many commercial organizations believe there are already too many pieces of legislation that incorporate data protection elements. New specific legislation would, in any case, be unlikely to have a significant harmonizing effect, and, if passed in relatively controversial areas, such as employment, might in fact have quite the opposite effect.

- It could continue to use existing mechanisms for cooperation at the EU level to work towards common application of the Directive. While there are some problems, such as the "non-sensitive"/"sensitive" data divide and the notification procedure, where the most obvious method of resolution is a revision of the Directive, it may well be more effective for the Commission to use existing mechanisms such as Notices and Recommendations to clarify the interpretation of provisions, and where Member States prove recalcitrant in their legislative or administrative implementation, to resort to Article 226/228 proceedings for incorrect and/or non-implementation.

A number of respondents called for a closer cooperation between industry, the Commission, the Article 29 Working Party and the Article 31 Committee[55] in the development of European approaches to key issues. While this might indeed be a positive step towards a more effective and efficient EU-wide implementation of the Directive, one would note that the interests of industry, while legitimate, are not the only interests that are at stake. EU citizens must also have a voice in this ongoing process, and the risk is, as was obvious both at the Commission's Data Protection Conference, and

53. European Commission, DG Employment and Social Affairs, Article 29 Working Party Opinion on the Processing of Personal Data in the Employment Context *at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf (Sept. 31, 2001); European Commission, DG Employment and Social Affairs, Second stage consultation of social partners on the protection of workers' personal data *at* http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf (Oct. 30, 2002).

54. European Commission, DG Employment and Social Affairs, Article 29 Working Party Opinion on the Processing of Personal Data in the Employment Context *at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf (Sept. 13, 2001).

55. The Article 31 Committee consists of government experts (usually from Ministries of Justice) which consider the legislative aspects involved in implementing the DPD.

in the representation of the position papers, that the citizens' voices may be signally underrepresented in the harmonization process.

(3) Uncoordinated Legislative Approach

A common complaint regarding data privacy law in the EU is that there has been a failure by the European Union institutions to co-ordinate those pieces of EU legislation which have data privacy elements, and that this has resulted in a lack of clarity in Community objectives, caused further inconsistencies in Member State implementation, and made it extremely difficult for commercial organizations to create consistent EU wide policies. With regard to the issue of conflicting legislation, one respondent to the Commission wrote:

> [T]he Distance Selling Directive,[56] the new Electronic Communications Data Protection Directive,[57] the E-Commerce Directive[58] and the Electronic Signatures Directive[59] all include provisions relevant to data protection. Some of these adopt different approaches on the same issue (e.g. opt in vs. opt out in relation to unsolicited emails) or impose more onerous provisions in relation to certain sectors of the market (e.g. the more stringent data protection obligations under the Electronic Signatures Directive which are imposed on certification service providers in relation to their use of personal data). This has caused confusion about which Directives are to be followed when, and exactly what requirements companies have to follow.[60]

This seems a justifiable complaint, although in defense of the Commission, the technical advances since the early 1990s were inevitably going to create new issues that were not necessarily clearly covered by the Data Protection Directive, such as the seemingly uncontrollable increase in the amount of "unsolicited commercial e-mail" ("UCE") or "spam," and the use of "spyware" and other web surveillance techniques to collect data on web users. Some Member States have attempted to avoid producing confusing implementing

56. Council Directive 97/7/EC, May 20, 1997, On the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19–27.

57. Council Directive 2002/58/EC, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37–47.

58. Council Directive 2000/31/EC, June 8, 2000, On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1–16.

59. Council Directive 1999/93/EC, Dec. 13, 1999, On a Community Framework for Electronic Signatures, 2000 O.J. (L 013) 12–20.

60. Tite & Lewis, Data Protection Directive 95/46/EC: Response to the European Commission's Three Yearly Review, 3 *at* http://europa.eu.int/comm/internal_market/en/dataprot/lawreport/papers/tite-lewis.pdf (Aug. 30, 2002) (all footnotes in this quotation are attributable to the author).

legislation—the UK government has decided not to pass additional measures relating to UCE, despite the EU's adoption of the E-Commerce Directive which contains specific measures in relation to UCE, on the grounds that the UK Data Protection Act 1998 already provides the necessary elements.[61] It would seem, however, that the Commission will have to give careful consideration to the future development of legislation in this area.

B. Administrative Practices and Transborder Data Flows

(1) EU/EEA Data Flows

The problem with the lack of practical harmonization of Member State laws becomes most apparent where organizations are involved in the transfer of personal data between Member States, or into and out of the EU/EEA, as it is difficult for companies to establish a set of operating rules for data protection within their organization that are acceptable to the national regulatory authorities of all the Member States. This is seen, not unnaturally, as a considerable and largely unnecessary impediment to business efficiency.

Before the Directive was adopted, most Member States' data protection laws effectively applied only to the processing of personal data within the state's borders. Thus, the nationality or legal domicile of data subjects was not the determining factor in deciding if national law was to be applied; but rather whether there was a link between the relevant data controller or data processing operation and the territory of the state. If the data controller and the data processing operation had close links to the territory of a state, in that the data controller resided or was established in the territory and/or the processing was carried out in the territory, then the state's country's data protection law normally applied to the controller and the processing operation. Only in rare cases did Member States attempt to apply data protection legislation to data processing taking place outside their territories, primarily due to the obvious difficulties inherent in the conflict of laws arena.

Article 4 of the Directive addresses the choice of law issue, stating that each Member State must apply its national legislation to

61. Although whether this is in fact the case remains a matter of some debate, the UK government having adopted this position following heavy lobbying by UK Internet Service Providers and their representative organizations. It is likely that ISPs felt that the requirements of the E-commerce Directive would place pressure on them to take measures against UCE, and those sending UCE, whereas the Data Protection Act 1998 places the impetus upon the data subject/end-user to take action against misuse of their data, however, placing the burden on the end-user would not seem to reflect the language of the E-Commerce Directive.

the processing of personal data carried out by data controllers established in that Member State. Where a data controller is established in several Member States, each of those establishments must comply with the obligations laid down by the relevant national law.[62] Where the data controller is not established in a Member State, but under international public law the Member State's national law would apply, it must apply its national legislation to the processing of personal data.[63] Where the controller is not established in any Member State, but makes use of equipment situated on the territory of a Member State, that state's national legislation must be applied to the processing operation, unless the controller only uses the equipment for the transit of the data through a Member State,[64] and the data controller must designate a representative established in the Member State.[65] The purpose of these rules was to ensure that data subjects were not exposed accidentally or deliberately to situations where they would have no recourse to any legal system to protect the rights granted by the Directive, and to avoid the same processing operation being governed by the law of more than one country.[66]

This might, perhaps, have been effective if the Member States had transposed the Directive in a consistent fashion, but as with so many other areas of the Directive, there are significant differences between the Member States' interpretation of the nature and scope of Article 4. As was noted in the consultation process,

> Finland's data protection law applies to the processing of personal data where the controller's place of activity is located within Finnish territory or in general comes under Finnish jurisdiction. By contrast, Sweden's data protection law applies to data controllers established in Sweden. This raises the question of which country's law should apply to the processing of personal data carried out in Sweden by a company established only in Finland.[67]

The issue of what "establishment" means has also arisen—it is key to the application of Article 4, but essentially undefined in the Directive, except that recital 19 states that the criterion of establishment "implies the effective and real exercise of activity through stable arrangements."[68] This does not provide a great deal of guidance, particularly since the recital then goes on to state that "the legal form

62. DPD, *supra* note 2, at art. 4(1)(a).

63. *Id.* at art. 4(1)(b).

64. *Id.* at art. 4(1)(c).

65. *Id.* at art. 4(2).

66. *See* Commentary from the European Commission in relation to the 1992 Amended Proposal for the Directive, COM(92) 422 final (Oct. 15, 1992).

67. EICTA, Comments on the General Data Protection Directive 95/46/EC (the "Directive"), 4 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/ecta_en.pdf (July 30, 2002).

68. DPD, *supra* note 2, ¶ 19.

of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect." Particular problems arise when considering processing of data via the Internet, where the circumstances may be such that it is difficult enough for a data subject or data protection authority to determine the physical location of the data controller, never mind to work out where it is "established."[69] A more uniform interpretation of "establishment" will inevitably be required if Article 4 is to be meaningful.

Yet a further bone of contention is the question of the scope of the phrase "makes use of equipment, automated or otherwise," notably whether this formulation would stretch to cover Internet-only contacts from outside the EU, for example, when a British consumer visits the website of a New York-based company. The Article 29 Working Party courted controversy in a recent Working Paper[70] by suggesting that while "not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law . . . it is not necessary that the controller exercise full control over the equipment,"[71] in short, suggesting that, for example, where cookies are placed on the hard disk of a user's computer, or JavaScript or a banner ad is used, "the user's PC can be viewed as equipment in the sense of Article 4(1)(c) of Directive 95/46/EC."[72] This means that the that the national law of the Member State where the user's PC is located would apply to the conditions under which his personal data may be collected by placing cookies on his hard disk, or by running JavaScript routines. While, the French text of the Directive, which can be read more liberally than the English, might support this interpretation, it has met with stiff resistance from the business community which has responded with suggestions that such a broad interpretation of the phrase would be unworkable in its application to the Web, and might compromise existing measures such as the U.S. Safe Harbor agreement, because the direct application of EU data protection law to a U.S. company, by virtue of its processing of personal data from EU citizens gathered through its websites, would remove any incentive to join the Safe Harbor.[73]

69. Global Privacy Alliance, Untitled Position Paper, 12 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/gpa_en.pdf (Aug. 5, 2002).

70. Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final (WP 56) *at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp56_en.pdf (May 30, 2002).

71. *Id.* at 9.

72. *Id.* at 11.

73. Global Privacy Alliance, *supra* note 69, at 17.

Thus, the application of Article 4 has proven problematic. As noted above, the harmonization process has struggled in the face of the Member States' "margin of appreciation" when implementing the Directive, and as a result across the EU, Member States' data protection laws are anything but uniform. This means that multinational companies which are established in more than one Member State find that each of their branches are faced with a different set of local laws with which to comply. Matters may worsen if the branches wish to transfer data to the parent company. For example, consider the situation where Company A is established in France, with subsidiary B established in Italy, subsidiary C established in Spain, and subsidiary D established in Germany. If the subsidiaries B, C, & D wish to transfer data to A for processing for purposes determined by them, A will have to be aware of, and apply, the differing laws of Italy, Spain, and Germany to the processing for the respective subsidiaries. Company A will also be unable to provide its subsidiaries with a uniform set of data protection guidelines, due to national variations.[74]

(2) Data Flows External to the EU/EEA

The problems relating to transborder data transfer are further exacerbated in the case of transfers outside the EU/EEA as the Directive sets detailed conditions for transfer of personal data to third party countries, forbidding transfers where, subject to limited exceptions, non-Member States fail to ensure an "adequate level of protection" for personal data.[75] The Commission has the power to assess that a third country ensures an adequate level of protection,[76] but where no such assessment has occurred, it may be necessary for data controllers within the EU to use the Directive's other legal bases for transferring data. The main exceptions provided are when the data subject has consented to the transfer,[77] when the transfer of data is necessary for the performance of a contract between the data subject and the controller,[78] and when the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.[79] The Directive does not make provision for transfers on the basis of a

74. UNICE, Implementation of 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 of 24 October 1995: Preliminary Comments, 2 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/unice_en.pdf (Aug. 30, 2002).

75. DPD, *supra* note 2, at art. 25(1).

76. *Id.* at art. 25(6).

77. *Id.* at art. 26(1).

78. *Id.*

79. *Id.*

"balance of interests," i.e., allowing a transfer to be made in pursuance of the legitimate interests of the exporting data controller unless it is unwarranted because of prejudice to the rights, freedoms or legitimate interests of the data subject. Member States may authorize transfers of personal data to a third country which does not ensure an adequate level of protection where the data controller provides adequate safeguards, in particular, via appropriate contractual clauses.[80]

A determination of the adequacy of protection of data privacy in a non-EU/EEA country to which personal data are to be transferred requires consideration of two criteria. First, the substantive rules that will apply to the data, and second, the methods of enforcement available to ensure that compliance with those substantive rules is enforced. The first of those criteria will be fulfilled if the substantive rules that apply to the transferee will achieve the same, or a similar, effect to those contained in the Directive. There are a number of ways that this might be achieved: national legislation in the jurisdiction to which the data are transferred; codes of conduct at an industry or sectoral level; or specific contractual provisions between the EU/EEA-based transferor and the non-EU/EEA transferee; or elements of all three.[81]

In this area too, the main problems seem to stem from lack of clarity in the Directive, lack of consistency between the Member States in their implementations, and a failure by the Commission to provide the necessary administrative backup required to ensure that the system outlined in the Directive would work effectively in practice. On the basis of the foregoing discussion, it comes as no surprise to find that the key term in Article 25—"adequacy"—is not defined in the Directive and no clear threshold for achieving adequacy is provided, and that as a result, it has largely been left to data controllers to determine, on an ad hoc basis, whether a country's data protection regime is adequate. The Commission itself has only managed to issue four adequacy decisions, finding Canada,[82] Hungary,[83] Switzerland,[84] and the U.S. Safe Harbor[85] to meet the EU's

80. *Id.* at art. 26(2).

81. *Id.* at art. 25(2).

82. Commission Decision (2002/2/EC) of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, 2002 O.J. (L2), 13–16 *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_002/l_00220020104en00130016.pdf.

83. Commission Decision (2000/519/EC) of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary, 2000 O.J. (L215), 4–6 *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_215/l_21520000825en00040006.pdf.

requirements, and has expressed the opinion that it is unlikely to be in a position to issue many more future decisions due to lack of resources. This suggests that EU data controllers who wish to export personal data to other non-EU/EEA states will continue to need to make use of the Article 26 exceptions. However, these have proven difficult to use. For example, several Member States are unwilling to accept employee consent for the transfer of personal data outside the EU/EEA as they "are of the opinion that employees do not have the necessary freedom to consent meaningfully to the transfer of such data because of their inherent dependence on their employers."[86] The ability of EU data controllers and non-EU data importers to enter into an agreement to protect data exported to third countries, using either ad hoc contract clauses or the Commission's Standard Contractual Clauses,[87] is also seen as unsatisfactory. Ad hoc contract clauses more often than not require prior authorization by the data protection authorities of the Member State from which data are to be exported, which makes the process time consuming and cumbersome,[88] and the Commission's Standard Contractual Clauses are seen as unworkable for many businesses because of the onerous nature of their terms.

> [T]he Standard Clauses impose significant burdens on business that go beyond common commercial practice, necessary compliance incentives, and perhaps most significantly the requirements of

84. Commission Decision (2000/518/EC) of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 2000 O.J. (L215), 1–3 *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_215/l_21520000825en00010003.pdf.

85. Commission Decision (2000/520/EC) of 26 July 2000 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, 2000 O.J. (L215), 7–47 [hereinafter Commission Decision 2000/520/EC]. The Commission made its decision on the adequacy of the Safe Harbor ruling despite the misgivings of the Article 29 Working Party and the fact that the European Parliament, in a Resolution dated 5 July 2000, expressed the view that the arrangement needed to be improved.

86. Global Privacy Alliance, *supra* note 69, at 6 n.18.

87. Commission Decision (2001/497/EC) of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001 O.J. (L18), 19–32 *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf; Commission Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, 2002 O.J. (L6), 52–63 [hereinafter Commission Decision 2002/16/EC] *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_006/l_00620020110en00520062.pdf.

88. Commission Decision 2002/16/EC, *supra* note 87, at ¶ (2). The United Kingdom is one of the few Member States that does not require any prior authorization, but the Office of the Information Commissioner will review contracts if a complaint is filed against the data transfer.

> Member State law and the Directive. They require more than adequacy, and even more than equivalence with the Directive. They also require joint and several liability on the part of the EU exporter and the non-EU importer, submission to EU jurisdiction by the importer, audits of the importer by the EU data exporter (or a selected body) and burdensome constraints on onward transfers.[89]

Even where there is an "adequacy decision" in relation to a data importer to whom a data transfer is to be made from an EU Member State, which should in principle be treated in the same way as a data transfer within the EU,[90] several of the Member States impose further requirements before permitting transfers:

> [T]he Spanish Data Protection Authority requires data transferors to provide documents that are not related to the transfer and refuses to include the database concerned in the Spanish Registry until the transferor does so. This mandate effectively requires de facto prior approval for data transfers to countries that already provide an adequate level of protection, something that adequacy findings, for example, are supposed to preclude.[91]

Even the Safe Harbor agreement negotiated by the Commission with the U.S. government has been greeted with decidedly mixed views in Europe, partly because of the relatively low uptake by U.S. companies,[92] and partly because the Safe Harbor excludes U.S. financial institutions.[93]

On the basis of the foregoing, it seems a not unreasonable assessment to suggest that with regard to transborder data flows, the Directive in its current form, and as implemented by the Member States, is a far from satisfactory arrangement. Even if one takes the complaints in the position papers submitted by commercial interests to the Commission with a proverbial grain of salt, there are clearly changes that can be made to the existing choice of law/jurisdiction and data transfer procedures that would signally improve the

89. Global Privacy Alliance, *supra* note 69, at 7; *see also* Tite & Lewis, *supra* note 60, at 1.

90. *See* Commission Decision 2000/520/EC, *supra* note 85, at ¶ 2 ("The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.").

91. Global Privacy Alliance, *supra* note 69, at 8.

92. At the time of writing, 332 U.S. companies had notified the Department of Commerce that they adhered to the safe harbor framework developed by the Department of Commerce in coordination with the European Commission. *See* U.S. Department of Commerce Safe Harbor List, *at* http://www.trade.gov.

93. It should be noted that U.S. financial institutions do not particularly want to be part of the Safe Harbor framework, as they are lobbying the U.S. government and the Commission for an adequacy ruling on the basis of existing U.S. financial privacy legislation, including the amended Fair Credit Reporting Act of 1970 and the Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act). For criticism of an adequacy ruling on that basis *see* Charlesworth, *supra* note 20, at 113.

European and international business environment without significantly impairing the protection provided to data subjects. Leaving aside the issues of more specific EU definitions of key terms, and better Member State harmonization, which are discussed above, there are several administrative advances which could be made.

The issue of jurisdiction and choice of law, particularly with regard to Internet transactions in personal data, is undoubtedly a complex issue. With regard to the application of law, given that the EU is supposed to have harmonized data protection laws, it would seem reasonable that data controllers, and particularly data controllers who are part of a group company, should be able to designate one EEA country where they are formally registered for data protection purposes—this would also allow for a single notification, as discussed in the previous section. Additionally, the role of the geographic location of the processing in determining the national rules that apply to it seems increasingly dated in terms of modern business practices. Certainly for data controllers established in one or more Member States, it would seem more practical for the processing rules to be based on the location of the controller rather than on where their servers are based.

While it might be argued that this would lead to a "race to the bottom," with data controllers choosing to register in the Member State with the least onerous data protection rules, if the Member State concerned has a satisfactory implementation of the Directive, as ascertained by the Commission (and, where necessary, the European Court of Justice), then the baseline of EU protection will still be maintained. Such a mechanism would encourage Member States to harmonize more effectively, because the imposition of national rules not required by the Directive, or which are significantly more onerous than the norm, will simply lead to data controllers registering elsewhere. It might thus be argued that where Member State authorities charge for registration/notification there will be scope for the market to determine the cost/benefit of registration in a particular Member State, i.e., Member States might have a lower fee for registration/notification but stricter rules, and vice versa.

Another argument is that the law governing the primary relationship between the data controller and the data subject should also be the law applicable to any transborder data flow resulting from that relationship:

> [I]f Dutch law governs the employment contract between a Dutch multinational and an employee in France, why should French law cover the data flows between France and The Netherlands while

> those data flows are only incidental to the employment relationship?[94]

This arrangement, too, has its merits for data controllers established within the EEA, by virtue of simplifying their data protection arrangements.

Where the data controller is not established in any EEA state, but processes non-EEA related personal data within an EEA state, it is tempting to argue that its activities should not be regulated by EU data protection law:

> [A] Hong Kong company based in Hong Kong using a server which happens to be based in Belgium to process data about its Hong Kong employees should be clearly excluded from the provisions of the Directive.[95]

However, this approach would appear to weaken the validity of the EU's own approach to transborder data flows, with the EU demanding that EU personal data be processed in accordance with the Directive wherever in the world it is transferred, while permitting lesser, or no protection, for other nation's citizens' data if it is processed in the EEA by a non-EEA established controller. If the EU, as stated in the Directive's recitals, is concerned that "that the fundamental rights of individuals should be safeguarded," it would seem inconsistent to differentiate between the protection afforded an EU citizen's, and a non-EU citizen's, personal data processed in the EU.

Where the data controller is not established in any EEA state, but collects personal data from EU citizens, for example, by the use of cookies, it seems difficult to justify the imposition of EU data protection law by virtue of Article 4(1)(c) simply because the controller uses "equipment" or "means," such as a data subject's PC, within the EU to collect personal data. While it is clear that Article 4(1)(c) is designed to prevent evasion or circumvention of EU data protection laws by relocation outside the EU/EEA, it may be that a more rigorous test is required to narrow the scope of the Article to a more practical set of targets, for example, a requirement that the data controller intentionally targets EU residents for data collection.[96] Additionally, there seems little justification for applying EU law under Article 4(1)(c) to data controllers established in countries that have been deemed adequate by the Commission, when the national laws of those countries would provide the necessary protection for data subjects.[97]

94. The European Privacy Officers' Forum, *supra* note 37, at 7.
95. Confederation of British Industry, *supra* note 52, at 6.
96. Covington & Burling, *supra* note 51, at 6.
97. The European Privacy Officers' Forum, *supra* note 37, at 7.

Given the financial difficulties facing the Commission with regard to providing "adequacy" decisions for non-EU/EEA states, and the litany of problems that data controllers who seek to use the Article 26 exemptions provide, it would seem that there is considerable scope for rationalizing transborder data flows to non-EU/EEA countries.

One suggestion has been to make provision for transfers on the basis of the "balance of interests," i.e., when the transfer is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.[98] Given that the exporting data controller will be responsible if the transfer results in prejudice to the data subject, it is arguable that the data controller will take this into account when determining the conditions under which a transfer is made. This argument, which is based upon an analogy with the "balance of interests" test for data processing of non-sensitive data under Article 7(f) of the Directive, would seem to overlook the difference in the degree of control that can be exerted by a data subject over the personal data during Article 7 processing and after Article 26 transfer. Analysis of Article 8 and Article 26 suggests that the drafters of the Directive were concerned about providing more extensive protections for both sensitive data and data to be transferred out of the EU/EEA. This may well have been predicated on the difficulty for data subjects in reasserting control over their personal data after transborder transfer, as opposed to just the possibility of being awarded damages for distress and/or damage following unlawful processing. That having been said, the extent to which EU exporting data controllers already have to make decisions about the adequacy of data protection regimes in third party nations, and make administrative and contractual provisions accordingly, suggests that the element of discretion that such a "balance of interests" provision might introduce might not, in practice, be significantly greater than already exists.

The removal of procedures additional to the measures provided for in the Directive would also allow for more efficient data flows. For example, where a state or administrative mechanism (e.g., the Safe Harbor Agreement) is the subject of an adequacy decision by the Commission, Member State data protection authorities should not require further procedures to be followed and should

98. *Id.* at 10; *see also* Clifford Chance Submission to the European Commission: Implementation of the EU Data Protection Directive (95/46/EC), 7 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/cliffordchance_en.pdf (July 30, 2002).

automatically authorize transfers to companies within such states or mechanisms. Equally, where the Commission approves standard contractual terms for the transfer of personal data, contracts using such standard contractual terms should not be subject to further national regulation and inspection.

With regard to the Commission's Standard Contractual Clauses, a number of the parties who submitted position papers suggested that these were too precisely detailed and thus relatively inflexible, and that other approaches would be more appropriate to the commercial environment. Other approaches suggested included: that the Standard Contractual Clauses should be issued as guidance only, thus allowing them to be adapted for particular circumstances and commercial needs;[99] that the Commission might approve alternative contracts—proffered, for example, by business organizations—for EU-wide use;[100] or that a set of contractual terms meeting the requirements of the data protection authorities in one Member State would be granted "mutual recognition" in all other Member States.[101] The first suggestion would probably not help matters unduly, as if data controllers were to be permitted to treat the Standard Contractual Clauses as guidance, this would almost certainly mean that many national data protection authorities would wish to maintain, or increase, their current level of oversight and approval. The second suggestion might be of more value, except for the fact that the Commission is unlikely to want to accept the workload that it would entail. The final suggestion would appear to be the most efficient approach to the problem, although given that it is essentially another form of harmonizing mechanism, this is probably not surprising.

Overall, while some of the suggestions received from commercial organizations clearly would be problematic, in that their aim would appear to be more to lower the data protection baseline that currently exists in the EU, rather than to provide more efficient ways of attaining the current level of protection, there have been a number of measures suggested which would signally improve the lot of EU data controllers needing to transfer personal data between EU/EEA states and to states outside the EU/EEA, without unduly eroding that baseline, and that the Commission and Member States could adopt without requiring profound changes in the Directive or national legislation.

99. Tite & Lewis, *supra* note 60, at 2.

100. Confederation of British Industry, *supra* note 52, at 14.

101. Tite & Lewis, *supra* note 60, at 2–3.

C. Privacy Enhancing Technologies (PETs)

While the Commission has expressed both its hope that technological solutions for data privacy will prove useful in attaining the aims of the Directive, and its intention to promote PETs, there remains considerable disagreement as to what actually constitutes a privacy enhancing technology.[102] A relatively broad definition is: "Privacy-enhancing technologies are protocols, standards, and tools that directly assist in protecting privacy, minimizing the collection of personally identifiable information, and when possible, eliminating the collection of personally identifiable information."[103]

With regard to the suggested role of PETs in providing an alternative avenue for enforcing the concepts contained in the Directive, the key issue is probably the extent to which any proposed technology can be demonstrated to accurately reflect those concepts rather than offer alternative weaker data subject controls over their personal data. Thus, the fact that a technology improves the efficiency of data processing would be of lesser importance than that it could provide some increased element of anonymity or pseudonymity in data subject/data controller transactions.

Member States' regulatory agencies are thus likely to differentiate in this regard between those technologies that implement fair information practices ("FIPs") and those which implement more basic "notice and choice" policies; as discussed elsewhere, it is debatable if the latter should in fact be properly considered as PETs at all.[104] Technologies like P3P[105] have been bruited as PETs, but even leaving aside problems such as the complexity of the P3P protocol, and its perceived data user (and data controller) unfriendliness, a key problem with P3P is that as it is currently implemented in web browsers, like Internet Explorer 6, it

102. John J. Borking & Charles D. Raab, *Laws, PETs and Other Technologies for Privacy Protection* 2001 J. OF INFO., LAW & TECH. 1 *at* http://elj.warwick.ac.uk.

103. Ruchika Agrawal, *Why is P3P Not a PET?*, ¶ 2.1, *at* http://www.w3.org/2002/p3p-ws/pp/epic.pdf (Nov. 12–13, 2002). Agrawal cites "blind" digital signatures, anonymous remailers and web-surfing anonymizers as examples of true PETs. *Id.* at ¶ 2.2.

104. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1.

105. P3P is an

> industry-standard XML-based language that enables an automatic "privacy handshake" between a browser and a web site or cookie . . . [It] is sponsored by the World Wide Web Consortium (W3C) [and] provides web site operators with a standardized XML-based language for writing proxies for privacy policies that can be automatically retrieved and interpreted by P3P-enabled web browsers and other user agents.

James A. Harvey & Karen M. Sanzaro, *P3P and IE 6: Raising More Privacy Issues Than They Resolve?*, GIGALAW (Feb. 2002), *at* http://www.gigalaw.com; *see also* Platform for Privacy Preferences (P3P) Project, *at* http://www.w3.org/P3P.

simply allows users to specify privacy preferences which the browser can then use to read a website's privacy policy (when that policy is rendered into machine readable form by encoding it in XML format) to determine whether the website policy satisfies the user's privacy requirements. If the policy does not meet the user's requirement, the browser will warn the user.

While in principle, the adoption of such technology by a major software company like Microsoft may be seen as a step forward, P3P has been met with considerable skepticism by both European data protection regulators, and by the very commercial entities that might be expected to use it. From the companies' point of view, P3P is both expensive to initially implement, and it requires considerable effort and resource to keep larger websites up-to-date; it is also not entirely clear what companies are letting themselves in for in terms of their accountability for statements made in their P3P policy, as "the specification's 'vocabulary' isn't rich enough to allow exact translations of written data privacy policies into an XML-based format that can be read by Web browsers and compared against the preferences set by individual users."[106] As a result, companies would prefer that P3P statements and compact policies not be considered legally binding documents.[107]

From the European regulators' perspective, P3P is problematic in that it does not promote a minimum set of privacy or security standards that websites should follow; its use does not guarantee compliance with Article 10 and 11 of the Directive with regard to information to be provided to the data subject; it does not provide an enforcement mechanism to ensure that data controllers are doing what their P3P policies indicate; and given the average user's unwillingness to change default browser settings, the absence of an default set of European user preferences keyed to the EU Directive means that many users would not in fact benefit from the degree of transparency that P3P can provide.[108]

Indeed, if one accepts the definition of a PET above, this iteration of P3P would appear to meet none of the basic requirements, although the Commission appears to feel that if it is

106. Patrick Thibodeau, *P3P Supporters Struggle to Increase Adoption of Data Privacy Standard*, COMPUTERWORLD 20 (Nov. 18, 2002), *at* http://www.computerworld.com.

107. Banking Industry Technology Secretariat, Position Paper: W3C Workshop on the Future of P3P *at* http://www.w3.org/2002/p3p-ws/pp/bits.pdf (Nov. 12–13, 2002).

108. Diana Alonso Blas, The future of P3P: Issues to be addressed in order to allow data controllers using P3P to be compliant with the EU Data Protection Directive *at* http://www.w3.org (Nov. 12–13, 2002); *see also* Article 29 Working Party, Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), XV D/5032/98 (WP 11) *at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1998/wp11_en.pdf (June 16, 1998) [hereinafter Art. 29 Working Party].

used within a suitable regulatory framework, it may be of use in helping individuals manage their online privacy choices, and might therefore be seen to help data controllers comply with their obligations under the Directive to ensure that their processing is transparent to the data subject.[109]

Future development of P3P may involve a more involved set of "negotiation facilities" to let websites interact with consumers, and potentially provide capabilities such as the ability to offer coupons for personal data.[110] This suggest that the future of P3P lies as a "marketplace mechanism" and not a "protection mechanism." In other words, it would facilitate the trading of personal information more readily than it enhanced the options available to data subjects to control their data. While some might see P3P as an aid to privacy: "A world without P3P is a world with less control over privacy, a world with P3P is a world with more control over privacy."[111] From the perspective of the DPD and FIPs, a world with P3P in that form is potentially a world with increasing amounts of personal data being released by data subjects without a clear understanding of the purpose for the collection by data controllers; a world where the temptation inevitably is to request personal data "in exchange" for information or services;[112] and a world where, in the absence of a suitable oversight and enforcement agency, the data subject may not be able to enforce the automated privacy agreement if it is breached, or may not be aware of, or be notified about, the mechanisms for accessing the FIPs. Indeed, a world with P3P may already be a world where both data subject and data controller are in the dark about what is actually being agreed about the collection and use of personal data:

> [S]ince P3P is primarily a technical solution, there is the all-too-likely possibility that webmasters simply will implement P3P policies at the web site as necessary to ensure that the site continues to function properly, without first receiving input from the appropriate legal and business contacts. Therefore, with P3P, there may be an increased risk that a company will face liability for discrepancies between and among their non-P3P policies, their P3P policies and their actual practices.[113]

At present, the debate about PETs does not appear to have progressed significantly from the position in the late 1990s, although

109. Diana Alonso Blas, *supra* note 108.

110. *See* Thibodeau, *supra* note 106.

111. Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net,* 14 BERKELEY TECH. L.J. 759, 762 (1999).

112. *See, e.g.*, the New York Times Registration page which requests information about employment and household income. *See also* Art. 29 Working Party, *supra* note 108.

113. Harvey & Sanzaro, *supra* note 105; *see also* Scot Hacker, *P3P in IE6: Frustrating Failure*, O'REILLY NETWORK (June 7, 2002), *at* http://www.oreillynet.com.

there have been some lively, if only tangentially relevant in privacy terms, side-debates about the role of open source and proprietary software in this area. The discussion at the Workshop on Developments in the Information Society: Internet and Privacy Enhancing Technologies at the Commission's Conference in Sept–Oct 2002 certainly appeared to have great difficulties agreeing on what a PET might be, and the panel of speakers appeared largely split between those favoring a "notice and choice" or "market mechanism" approach and those who felt that any technology that failed to uphold the FIPs might at best be privacy neutral, but was more likely to be a potentially privacy intrusive technology ("PIT").

One paper from a speaker who appeared to fall into the "notice and choice" or "market mechanism" camp was based on the concept of "user empowerment," which was posited as a hybrid proposal. This accepted that a baseline regulation for privacy rights was probably necessary, but went on to argue that above that baseline the most efficient method of dealing with personal data was to let users set their own privacy preferences. The need for "user empowerment" was premised upon the fact that "a regulatory regime that requires all measures to be taken by the company collecting and processing data has the perverse effect of imposing costs on users,"[114] those costs being:

> *A loss of consumer surplus* . . . For example, a number of free e-mail services reply on the ability to deliver targeted advertising to particular users based on personal information gathered about them. If, to protect privacy, the ability of companies to gather and process this information is made too cumbersome, these services will disappear, and users will have no option but to pay for e-mail services this would . . . pric[e] low-income users out of the Internet market entirely, reducing Internet penetration. . . .
>
> *The opportunity cost of not having the service reflect the user's particular privacy preferences.* To the extent that websites adopt one-size-fits-all to comply with privacy laws, an opportunity cost is imposed on those users who have different preferences, and would choose to share more (or less) personal data . . . [T]he suggestion . . . that fully informed and freely given user consent is not a sufficient basis on which to process data, but that there must also be a legitimate purpose (however defined) for the processing, risks imposing this opportunity cost on users who otherwise would have consented to the processing of their data.[115]

114. Jason Albert, Privacy on the Internet: Protecting and Empowering Users, 1 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/albert_en.pdf (Sept. 2002).

115. *Id.* at 1–2.

While both these arguments have some attractions, notably for those with a Posnerian frame of reference,[116] it is not particularly convincing when viewed from the European perspective. The first example is unconvincing, firstly because it is premised on a "privacy as commodity" basis, as opposed to a "privacy as a fundamental right" basis, and secondly, because it sets up a scenario which requires "personal data" where anonymous or pseudonymous data might serve as well. It also posits that processing the information lawfully in such circumstances might be "too cumbersome" without suggesting why or how, and assumes that, in the absence of a permitted trade in personal data, there are no other mechanisms available to support free or low cost e-mail services for low-income users. Despite the balance of the example being weighted so heavily against privacy protection, there appears to be no obvious evidence that the suggested outcome would necessarily be the case.

The second example, is also premised on the "privacy as commodity," and in essence seems to claim that privacy law restrictions amount to an undue interference in "the market." However, there are many potential markets where individuals have items to trade, and could do so on the basis of fully informed and freely given consent, but are prevented from doing so by national laws. For example, if I set up a donor service whereby individuals could obtain a car in exchange for their duplicate organs, such as kidneys, or for other body parts such as a quantity of blood, I might be offering a new and innovative service, and one where individuals could barter their organs with fully informed and freely given consent, but in many countries, even though an individual might be considered to "own" his body, such a sale would be illegal, because the trade in certain items is considered socially undesirable, even where an individual might perfectly legally donate an organ for free. Just because there could be a market does not mean that there should be a market.[117] In any case, the example seems confused, for it seems to suggest that fully informed and freely given user consent should be capable of justifying illegitimate or illegal purposes. Additionally, neither example seems to deal well with the issue of whether what may be seen as "compelled consent" on economic grounds, (i.e., "provide personal data or have no service"), in fact equates with the interpretation of "consent" in terms of privacy as a human right, the basis on which the Directive is supposedly founded (i.e.,

116. Richard A. Posner, *An Economic Theory of Privacy*, REGULATION 19–26 (May/June 1978).

117. For further discussion of the concept of market inalienability, *see* Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987); MARGARET JANE RADIN, CONTESTED COMMODITIES (1996); *but cf.* Walter Block, *Market Inalienability Once Again: Reply to Radin*, 22 THOMAS JEFFERSON L.J. 37 (1999).

"fundamental rights should not be subject to enforced commoditization").

Probably the toughest test that any potentially privacy enhancing technology currently faces in the EU is the ingrained suspicion that such technologies are simply a method of subverting the explicit protection granted by the Directive. The initial aggressive championing of P3P and other technical platforms for privacy protection as an alternative, as opposed to a supplement, to data protection legislation, by parties opposed to formal regulation, has resulted in something of a backlash against privacy technologies generally, particularly as the initial expansive claims of the abilities of some of the early technologies have gradually run out of steam. It would be wrong, however, to dismiss such technologies out of hand. When properly used, and within the framework of formal regulation, there are an array of potential technologies which may prove functional, both in enabling data controllers to meet some of their obligations under the Directive, and in providing data subjects with a better understanding of the legal and technical environments which affect their privacy rights. In general, it would seem that, with regard to the Commission's suggestion that PETs might be used as part of the EU data privacy regime:

- a clear definition of what a PET actually is will be required, and it is suggested that any definition should have regard not to the concepts of "notice and choice," but rather to the concepts contained in the FIPs; and
- while PETs have a role to play within a regulatory-based regime, they should continue to be viewed as supplementary to it, rather than effective substitutes for all or part of that regime.

D. Self-Regulation and Codes of Practice

The issue of self-regulation is a "hot button" topic for both sides of the data privacy debate. There is deep suspicion amongst privacy advocates that most proposals put forward by business for self-regulatory schemes are simply conspiracies to deter effective privacy enforcement by means of legislative rules and independent oversight. On the other hand, businesses see self-regulation as being a much more flexible approach to ensuring privacy protection, as it can be more easily adapted to changing commercial and technical environments, and arguably administered more effectively by privacy officers who are closer to the point of processing. In their view, formal privacy regulation is often difficult to comply adequately with due to lack of clarity, precision and purpose; involves overburdensome and purposeless formalities; and is often only utilized by those with existing grievances.

On the evidence, both sides have legitimate points. The history of industry self-regulation is littered with examples of abuses and failures.[118] However, there are some apparent success stories, and, if self-regulation is carried out scrupulously, significant advantages can accrue both to society and to the self-regulated businesses.[119] I have argued elsewhere[120] that with regard to data privacy, self-regulation in isolation from a baseline of formal state regulation is likely to fail for a variety of reasons:

- Self-regulatory standards for privacy protection are often set in an unaccountable and non-democratic manner by business alone or in combination with NGOs. In such fora, it is perhaps unsurprising that "inconvenient" but vital standards such as rights of access to personal data, credible oversight and enforcement mechanisms, and legal redress for the individual may not be included, or are weakened by exceptions to the point where they are meaningless.
- Self-regulatory standards are often unevenly adopted within and across industries and because they are by definition voluntary, despite good intentions self-regulation can thus come to mean no regulation. At that point, the standards become little more than misleading public relations material designed to soothe public concerns without actually addressing problems.
- Self-regulation can be used by industry to co-opt critics, minimize justifiable litigation, and avoid government regulation even when it is needed. Highly hyped but legally unenforceable privacy policies are no substitute for rights of access to personal data, credible oversight and enforcement mechanisms, and legal redress for the individual.
- Because there is no baseline of privacy protection, a multiplicity of self regulatory initiatives may develop, allowing companies to pick and choose the standards they are willing to adhere to. Additionally, self-regulatory certification systems (such as web seals) can be confusing for consumers and buyers, particularly where there are difficulties in determining the veracity or value of competing systems—the temptation is to treat them all as of equal

118. For the checkered history of the online industry body, TRUSTe, see Charlesworth, *supra* note 20, at 104–05.

119. One example appears to be the development of codes of business ethics in the areas of child labor and sweatshops. *See* Bureau of International Labor Affairs, The Apparel Industry and Codes of Conduct: A Solution to the International Child Labor Problem? *at* http://www.dol.gov/ilab/media/reports/iclp/apparel/apparel.pdf; *see also* Lance Compa & Tashia Hinchliffe-Darricarrere, *Enforcing International Labor Rights Through Corporate Codes of Conduct*, 33 COLUM. J. TRANSNAT'L L. 663–68 (1995).

120. Andrew Charlesworth, *Clash of the Data Titans: US and EU Data Privacy Regulation*, 6 EUROPEAN PUBLIC LAW 253, 273–74 (2000).

> value or worthlessness. Above all, multiple initiatives mean a lack of transparency about personal data processing activities on the part of data users that is an essential part of meaningful data privacy rules.

Yet, the fact that self-regulation may fail to provide an adequate level of protection in the absence of a legislative baseline for data privacy does not mean that there is no place for self-regulation within the EU privacy regime. As noted above, some of the suggested solutions to the difficulties faced by the Member States with regard to transborder data flows may well best be tackled by self-regulatory initiatives. Additionally, in the UK, the Office of the Information Commissioner ("OIC") has (in large part due to underfunding and understaffing) long taken the approach that a key part of the UK data privacy regime would be the promotion of the use of sectoral policies and codes of practice, rather than a rigid scheme of enforcement.[121] It is noticeable when discussing the activities of national data protection agencies with representatives of international businesses that the UK OIC is frequently praised for its constructive and pragmatic approach to the application of data protection laws. This is not to say that the UK OIC is lax in its enforcement of the law, or that UK national transposition of the DPD resulted in significantly weaker national legislation. Rather, the process of consultation and discussion related to the development of sectoral polices and codes of practice has meant that the staff of the OIC are well placed to advise on effective privacy protection mechanisms, and are knowledgeable about the practical difficulties which face national and international businesses.

The state of play with regard to self regulatory schemes in the EU appears to have matured somewhat, with less direct calls for what might be considered PR-enhancing, self-regulatory devices, such as web privacy seals, amongst European companies,[122] and more

121. *See, e.g.*, the UK Further and Higher Education Code of Practice on Data Protection, *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/bipar_en.pdf.

122. Although support remains for such devices, notably a European Privacy Seal awarded if a website followed best data protection practice. *See* Allen & Overy, *supra* note 42, at 3; International Federation of Insurance Intermediaries, Answers to the European Commission Questionnaire for the data controllers on the implementation of the Data Protection Directive, 3 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/bipar_en.pdf (Sept. 23, 2002). Interestingly, the development of such a European Privacy Seal was opposed by the U.S. Council for International Business:

> USCIB supports codes of conduct and seal programs that are voluntary and market-driven. It is important to note that privacy seals are working effectively in the U.S.... However, an EU government developed seal program would fail to account for the existing privacy and consumer trust initiatives that exist today and could actually undermine competitiveness and decrease the voluntary nature of codes of conduct.

requests for national, and possibly EU-wide codes of conduct. It seems that the major stumbling block to this type of development is the fact that, despite the Directive providing for the drawing up of Codes of Conduct at the national level,[123] and providing an oversight mechanism for conformity of EU-level Codes with national legislation,[124] it provides neither the Commission nor the Member States with the power to approve EU-wide Codes of Conduct for particular sectors or enterprises, or any administrative mechanism by which this might occur. This has led to the growth of often incompatible national codes of practice for particular sectors.[125] In contrast, EU-wide Codes of Conduct could be used as harmonizing tools, by virtue of Commission or Member State approval permitting mutual recognition of a Code across the Member States.[126]

As with its desire to keep an open mind on the role of PETs, the Commission's move to explore a wider role for self-regulation as a facilitative device for the effective implementation of a harmonized EU regulatory framework is a positive step towards achieving a solution that satisfies both the demands of EU citizens for adequate protection of their personal data, and the need of commercial organizations to have clear guidance about good practice. It is important, however, that the Commission resists the undoubted pressure to allow self-regulatory practices to displace or replace the legislative protections afforded to personal data in the EU.

Conclusion—Optimizing Enforcement

There is little doubt that the process of harmonizing the laws of the fifteen Member States has a long way to go before EU data protection law reaches the point where the phrase E Pluribus Unum could truly apply. There may be more unity of purpose between the Member States in 2003 than there was in 1995, but there remain significant differences of interpretation and administrative practice. In that regard, the Commission's decision to hold such a wide-ranging review of the implementation of the Directive appears far from hasty.

USCIB Comments for the Review of the E.U. General Data Protection Directive (95/46/EC), 4 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/uscib_en.pdf (July 30, 2002). Leaving aside the question of whom U.S. privacy seals are "working effectively" for, it is difficult to see why a government backed seal, which would surely carry more weight with consumers, would have such a deleterious effect on competition and voluntary codes of practice.

123. DPD, *supra* note 2, at art. 27(1)–(2).

124. *Id.* at art. 27(3).

125. Association of Consumer Credit Information Suppliers, Data Protection Directive (95/46), 5 *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/accis_en.pdf (Aug. 6, 2002).

126. Citigroup, *supra* note 48, at 6.

Both the technological and commercial environments have changed considerably, and in many cases so have the attitudes of governments and commercial organizations towards the utility of privacy regulation. Thus, while there are significant areas where citizens, commercial organizations, regulators, and governments are still engaged in adversarial struggles over the nature and scope of regulation, in many others the main issue now is how best to reach a commonly agreed upon goal.

Many of the suggestions with regard to administrative practices and transborder data flows appear both practical and, in principle at least, either privacy enhancing, or at worst privacy neutral. Where national data authorities can agree on co-operative measures, such as single point notification or the use of Chief Privacy Officers instead of notification, mutual recognition of codes of practice and sectoral policies, and consistent interpretation of statutory definitions, these should be actively pursued and encouraged. Redundant bureaucracy should ideally be excised. This might include the removal of the whole process of notification to national authorities, if no compelling argument for retaining it can be mustered.

In the longer term, the primary aim of national DP authorities should increasingly focus on guidance rather than enforcement, although there will remain an obvious role for enforcement in some areas. Where enforcement is an issue, all national authorities should have their enforcement powers brought into line with those of other Member States. For example, the UK OIC should be granted an independent power of data audit or site inspection, with or without the consent of the data controller, rather than the limited powers currently held under the UK Data Protection Act 1998.[127] Supplemental activities to the legislative framework should be examined, and where necessary, given formal sanction. In this context, the setting of audit standards and the granting of audit accreditation to independent bodies by Member States will be an essential step towards incorporating data protection practices ever more firmly into the organizational ethos of commercial entities.

However, at the same time, measures which seek to reduce the data privacy baseline should continue to be actively resisted, whether these take the form of proposals to replace legislative protections by self-regulatory mechanisms, or by use of new technological mechanisms. The EU privacy baseline must continue to be measured against the Fair Information Principles and should not be permitted to be undercut by market-based privacy interpretations. Indeed, if

127. Andrew Charlesworth, *Implementing the European Union Data Protection Directive 1995 in UK Law: The Data Protection Act 1998*, 16 GOV'T INFO. Q. 203, 226 (1999).

the price for the rapid attainment of a more complete harmonization of EU data protection law is to be a significant weakening of that data privacy baseline, then perhaps the Member States' Ex Uno Plures approach to its application might inadvertently prove to be the best model for EU citizens.

***