International Lawyer

Volume 35 | Number 1 Article 8

2001

Beyond Safe Harbor: European Data Protection Law and Electronic Commerce

Christopher Kuner

Beyond Safe Harbor: European Data Protection Law and Electronic Commerce

CHRISTOPHER KUNER*

It is understandable that, in the United States, restrictions on the transfer of personal data from the European Union (EU) have received a great deal of attention in recent years. In particular, the recently concluded Safe Harbor negotiations[1] between the U.S. Department of Commerce and the EU Commission have focused attention on restrictions placed by European data protection law (as privacy law is called in Europe) on the transfer of personal data from the Community to third countries.

However, as important as the Safe Harbor negotiations have been, the transfer of personal data from the EU is just one of many European data protection issues that should concern any company doing business online. In fact, transfer of data from the EU may ultimately be less important for a company than issues regarding the application of EU data protection law to its online activities, particularly for companies with substantial European operations. With the growing importance of electronic commerce in Europe, and the adoption on November 21, 2000 of a lengthy paper entitled *Privacy on the Internet: An Integrated EU Approach to On-line Data Protection* by the EU's Article 29 Working Party,[2] the importance

*Christopher Kuner is an attorney in the Brussels office of the international law firm Morrison & Foerster L.L.P., specializing in electronic commerce and legal aspects of the Internet. A particular focus of Mr. Kuner's practice is regulatory developments in Europe relating to e-commerce, at both the EU and the Member State levels.

Mr. Kuner is a member of the Legal Advisory Board of DG Information Society of the European Commission, and a member of legal working groups on e-commerce legal issues of the International Chamber of Commerce (ICC), the Internet Law and Policy Forum (ILPF), and the United Nations Commission on International Trade Law (UNCITRAL). He is also Chairman of Subcommittee R4 (Cybersecurity) of the International Bar Association. The author of numerous articles and the book *Internet für Juristen* (Verlag C.H. Beck), Mr. Kuner is a frequent lecturer on Internet-related topics. Mr. Kuner maintains a website on recent legal developments in Germany in the areas of Internet and e-commerce at http://www.kuner.com, and may be contacted at ckuner@mofo.com.

The author is grateful to Dr. Rosa Barcelo for her valuable insights and assistance in preparing this article.

1. The Safe Harbor went into effect on November 1, 2000. U.S. Department of Commerce, *Safe Harbor*, *at* http://www.export.gov/safeharbor/ (last visited Feb. 13, 2001).

2. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, PRIVACY ON THE INTERNET: AN INTEGRATED EU APPROACH TO ON-LINE DATA PROTECTION, 5063/00/EN/FINAL WP 37, *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf. The Working Party is a committee composed of rep-

of European data protection rules for any company interested in doing business in Europe or dealing with European customers can only increase.

This article cannot possibly give a detailed description of all the legal problems that electronic commerce can give rise to under European data protection law, given the broad scope of the law and the fact that, in the end, the details of compliance are largely a matter of Member State law.[3] Rather, the purpose of this article is to give an introduction to the legal framework for data protection in Europe as it relates to e-commerce, and to point out some of the particular legal problems and uncertainties that arise in practice, and are likely to arise in the future.

I. Brief Introduction to EU Data Protection Law

EU data protection law is a highly complex body of law that is comprised of three main elements. First, European Community law, in particular two directives, namely the EU Data Protection Directive[4] (Directive) and the EU Telecommunications Data Protection Directive[5] (ISDN Directive). The Directive sets forth the general framework for European data protection law, and is intended to provide a harmonized floor of protection among the fifteen EU Member States. In accordance with EU law, the Directive was supposed to be implemented (i.e., national law is supposed to have been amended to reflect the Directive's provisions) in all the Member States by late October 1998, but not all have done so, and five (France, Germany, Ireland, Luxembourg, and The Netherlands) were sued by the Commission on January 11, 2000 for failure to do so.[6] Since national and local data protection laws can vary quite a bit, the Directive serves as a useful benchmark to evaluate legal rights and responsibilities.

The ISDN Directive was originally intended to apply more or less exclusively to the telecommunications sector, though its broad wording, and the ever-increasing convergence

---

resentatives of the European Commission and the Member States that is responsible, *inter alia*, for issuing opinions and recommendations on European data protection law. The opinions and recommendations of the Working Party are advisory and thus not, strictly speaking, legally binding on the EU Member States, but are regarded as highly persuasive. *See* EU Data Protection Directive, Recital 65 and art. 29(1), *available at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

3. The fifteen Member States of the EU are, at present, Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden, and the United Kingdom. In addition, the Directive is applicable to the members of the European Economic Area, namely Iceland, Lichtenstein, and Norway.

4. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L281) 31, *available at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

5. Directive 97/66/EC of the European Parliament and of the Council of December 15, 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 1998 O.J. (L24) 1, *available at* http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html.

6. *See* Press Release, European Commission, Data Protection: Commission Takes Five Member States to Court (Jan. 11, 2000), *available at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/2k-10.htm. However, as the press release makes clear,

> In those Member States where the implementing legislation is not yet in place, individuals are entitled to invoke some of the directive's provisions before national courts, in accordance with the case law of the Court of Justice (Marleasing case, C-106/89, 13.11.90). In addition, individuals suffering damage as a result of a Member State's failure to implement the directive are in some cases entitled to seek compensation before national courts, under the terms of the Court of Justice's case law in the Francovich case (C-6/90 and C-9/90, 19.11.91).

between traditional telecommunications and Internet commerce, always left open the possibility that it could apply generally to all electronic commerce as well. Then, on April 27, 2000, the European Commission published a paper entitled *The Processing of Personal Data and the Protection of Privacy in the Communications Sector*,[7] which contains amendments to the ISDN Directive. The paper makes explicit for the first time that the ISDN Directive is to cover TCP/IP services as well as traditional telephony; in fact, the broad definitional scope of the amendments (under them, the Directive is to apply to "the processing of personal data in connection with the provision of publicly available communication services in public communication networks in the Community")[8] suggests that it could apply to the entire Internet.

Secondly, beyond the two directives, there are also data protection provisions in other instruments of EU law (such as the recently-enacted Electronic Signatures Directive)[9] and interpretative documents issued by various EU institutions.

National law of the Member States, which is supposed to implement the EU Directive, shows a multiplicity of approaches, even in those Member States that have implemented the Directive. Moreover, since most national data protection laws were originally drafted before the Internet age, they are typically ill-suited to the fast-moving world of electronic commerce. To deal with the special demands of Internet communication, some Member States have passed special data protection laws for the online environment.[10]

Finally, there are numerous local and state laws, regulations, and recommendations. For example in Germany, there are data protection laws at the state (*Länder*) level, as well as numerous other ones dealing with specialized topics. The state and local data protection authorities also issue pronouncements and recommendations (for example, regarding so-called "data protection-friendly technologies")[11] that, while not strictly having the force of law, tend to be very persuasive in practice.

It is also helpful to remember several features of EU data protection law that are particularly relevant to electronic commerce, including a wide scope. The Directive covers the processing of personal data, which terms are construed very broadly. It describes personal data as "any information relating to an identified or identifiable natural person"; an identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[12] Processing in turn is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[13] The breadth of

7. Processing of Personal Data and the Protection of Privacy in the Communications Sector, COM(00)385 final, *available at* http://europa.eu.int/eur-lex/en/com/dat/2000/en_500PC0385.html.

8. Press Release, *supra* note 6, at 10.

9. Directive 1999/93/EC, December 13, 1999 on a Community framework for electronic signatures, art. 8, 2000 O.J. (L13) 12, 16, *available at* http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf.

10. *See, e.g.*, Teleservices Data Protection Act (*Teledienstedatenschutzgesetz*) (1997) (Ger.), *available at* http://www.iid.de/iukdg/gesetz/iukdg.html.

11. *See, e.g.*, Datenschutzfreundliche Technologien, issued in January 1998 by the German "Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder."

12. Directive 95/46/EC, *supra* note 4, arts. 2(a), (b).

13. *Id.*

these definitions means that, in practice, the rule of thumb is that most all types of data and processing are covered by EU data protection law, unless it can be shown clearly that they should not be covered (e.g., if data is completely anonymous).

II. Limitation on Purpose and Scope of Processing

Under the Directive, personal data must not be processed without consent of the data subject, unless processing is necessary for the performance of a contract with the data subject or some explicit exception applies[14] that rule has important ramifications for electronic commerce. Almost every kind of e-commerce transaction involves the processing of some personal data, and traditional means for obtaining consent (such as asking a customer to click "I agree" on a pop-up box) may not be practicable in the context of e-commerce. Moreover, EU data protection law requires that processing be strictly limited to the purpose originally notified to the data subject.[15] This gives rise to legal issues because of the view of European regulators that the Internet leads to a large amount of invisible or non-transparent processing of personal data.[16] These principles have led to the principle of data minimization, meaning that processing of personal data must be restricted to the minimum amount necessary.[17] In practice, these restrictions mean that websites carrying out electronic commerce activities must pay attention to a number of legal considerations, in particular:

- whether they are adequately informing users about the types of processing carried out on their personal data;
- what legal basis is to be used to allow the processing of personal data;
- whether personal data are being transferred to third parties without the full knowledge or explicit consent of users; and
- whether adequate security measures are being used to protect the integrity of data processing.

A less obvious, but still important, area of concern for electronic commerce, is the implication of EU data protection law for technology design. Generally speaking, liability for violations of EU data protection law is placed on the data controller,[18] that is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. . . ."[19] This

14. *See id.* art. 7.

15. *Id.* art. 6(1)(b).

16. *See* ARTICLE 29 WORKING PARTY, RECOMMENDATION 1/99 ON INVISIBLE AND AUTOMATIC PROCESSING OF PERSONAL DATA ON THE INTERNET PERFORMED BY SOFTWARE AND HARDWARE, 1999 DG MARKT 5093/98, 4, *available at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp17en.htm. The recommendation states, "Presently it is almost impossible to use the Internet without being confronted with privacy-invading features that carry out all kinds of processing operations of personal data in a way that is invisible to the data subject." *Id.*

17. This is reflected, for example, in the German Teleservices Data Protection Act, art. 3(4), *available at* http://www.kuner.com/.

18. *See* Directive 95/46/EC, *supra* note 4, at recital 55. It states "Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller. . . ." *Id.*

19. *Id.* art. 2(d).

has traditionally meant that manufacturers of hardware, software, or other equipment that collects or processes personal data have not been legally liable for any data processing performed by their products. However, this situation is beginning to change.

As EU data protection authorities are becoming increasingly frustrated about the level of compliance with data protection requirements, and as it has become increasingly evident that they do not have the resources to police compliance of the processing of data on the Internet, there has been increasing emphasis by the authorities on the idea of ensuring before-the-fact compliance with the law by encouraging the development of privacy-enhancing technologies, including hardware and software used for processing data on the Internet. One of the most prominent examples of this attitude is reflected by the proposed amendments to the ISDN Directive referred to earlier. In the commentary to the amendments, there is a warning that the Commission may propose, or may allow the Member States to impose, technical standards for Internet hardware and software if manufacturers do not design products that are data-protection friendly:

> [T]he Commission may propose measures under Article 3.3(c) of Directive 1999/5/EC on telecommunications terminal equipment which explicitly foresees the possibility of requiring manufacturers of terminal equipment to construct their product in such a way that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected. Such measures could be proposed if industry does not act upon the Recommendation of the Working Party without further delay.[20]

It is thus likely that both Member State and EU data protection law will in the future require hardware and software products to comply with certain minimum data processing standards.[21]

Finally, it is important to consider the sanctions for non-compliance with EU data protection rules. So far, there have been few cases of companies being subjected to civil or criminal penalties for not complying with EU data protection rules in their e-commerce activities, for several reasons. First, EU data protection regulators (meaning, in most cases, national or local authorities at the Member State level) typically lack the resources and personnel to engage in widespread enforcement activities. Second, the sheer volume of Internet traffic has made it difficult for them to monitor compliance with data protection rules. Finally, the Safe Harbor negotiations seemed to occupy the attention of EU regulators that they might have otherwise given to enforcement activities.

A number of factors now make enforcement of EU data protection rules much more likely. First, as described above, the Safe Harbor negotiations have been concluded. Second, increasing concern about the security of data processing on the Internet by the European public has increased political pressure on data protection authorities to take action against violations of the laws. Finally, implementation of the Directive is likely to give impetus to an increase in enforcement activities, since the Directive obligates the Member States to create a direct cause of action on behalf of data subjects for violation of their rights,[22] which was not possible under the laws of many Member States before entry into force of the

20. Directive 1999/93/ED, *supra* note 9, at 6.

21. The possibility of imposing liability on manufacturers who fail to produce non-compliant products is supported by Recital 55 of the Directive, which states, " . . . sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive." *See* Directive 94/46/EC, *supra* note 4, at recital 55.

22. *Id.* art. 23(1).

Directive. It is thus not surprising that some Member State data protection authorities have begun examining compliance with their data protection laws by websites much more closely.[23]

A prime example of the new, more aggressive attitude toward enforcement is the fine of ten million pesetas (U.S.$57,000) levied in July 2000 by the Spanish Data Protection Authority on Microsoft Iberica SRL for processing personal data without the consent of data subjects. The issue arose when, in May 1999, officials of the Authority carried out an inspection at Microsoft Iberica SRL, and discovered that the entity owned a database containing the personal data of Spanish citizens that did not comply with Spanish data protection rules. The database was initially hosted in the United States but contained private data of Spanish citizens who had accessed Microsoft services via its website, http://www.microsoft.com. Later, Microsoft US transferred the database to Microsoft Iberica in Spain. Microsoft Iberica argued that Spanish data protection law did not apply, since the databases were hosted in the United States and thus U.S. law should apply. Microsoft also argued that it had either obtained appropriate consent from data subjects or a contractual relationship existed between Microsoft US and the data subjects. However, the Spanish Data Protection Authority found that Microsoft had not provided adequate information about the data processing to the data subjects. Furthermore, the Authority said that even though Microsoft US had established in its privacy policy that data subjects could choose to refuse to have their data transferred to third parties, and that some data subjects had made this choice, their wishes were not respected, and data were transferred to Microsoft Iberica anyway. The Authority then fined Microsoft based on violations of Spanish law, which requires explicit consent from the data subjects prior to the processing and transfer of private data. The fine was first set at fifty million pesetas (U.S.$250,000), and was later reduced to ten million pesetas.

III. Application of European Data Protection Law to Electronic Commerce

Because of the implications of European data protection law discussed above, one of the most basic and yet important questions that companies involved in electronic commerce need to answer is whether or not it applies to their activities. This question is of particular relevance to companies with websites in the United States and other non-EU countries, since it is clear that EU-based websites will be subject to European law.[24] The implications of being subject to EU data protection law are clear:

- The data controller will be subject to the full range of obligations under EU law, as well as the possibility of fines and other sanctions, that can be brought both by EU data protection authorities and data subjects in Europe.

23. For example, a study on compliance was recently published by the CNIL (the French data protection authority). *See* CNIL, *Actualité*, *at* http://www.cnil.fr/actu/index.htm.

24. It is important to note that the Safe Harbor arrangement does not affect the application of the Directive, at least in the view of European regulators. This means, for example, that U.S.-based companies cannot evade compliance with EU law by complying with the Safe Harbor in situations where EU law would otherwise apply. *See* EUROPEAN COMMISSION, OPINION 4/2000 ON THE LEVEL OF PROTECTION PROVIDED BY THE SAFE HARBOR PRINCIPLES, 2000 DG MARKT CA07/434/00, *available at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32en.htm.

- The controller may be obliged to register with the data protection authority in each Member State of the European Union where processing takes place.[25] Although the content of such notifications varies from one Member State to the other, some minimum content is required in all Member States, in particular: (a) the name and address of the controller and the representative of the controller, if any; (b) the purpose or purposes of the processing; (c) a description of the category or categories of data subject and of the data or categories of data relating to them; (d) the recipients or categories of recipients to whom the data might be disclosed; (e) proposed transfers of data to third countries; and (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of the processing.
- In cases where EU law applies by virtue of the controller's use of equipment in the EU (see below), the controller is also obliged to name a representative in the EU that will be liable in case of the controller's non-compliance with the law.[26]

Unfortunately, the application of EU data protection law to electronic commerce is far from clear.[27] Consider, for example, the following scenario, which often arises in practice:

> Company X sells consumer software over the Net and has its headquarters in California. It sells almost exclusively in the United States and Canada, but occasionally sells to isolated customers in Europe. Company X's website is only in English, and it has only a few marketing people in Europe, but no subsidiaries there. Company X's website uses cookies to authenticate customers and users. Given the above scenario, to what extent does Company X need to comply with EU data protection law?

To answer this question, it is necessary first of all to consider the basic rules for the application of European data protection law, which are set forth in article 4 of the Directive.[28] The Directive provides for three scenarios in which EU data protection law may apply:

- First, if the data processing is carried out in the EU and the data controller is established there;
- Second, if the data controller is not established in the EU, but in a place where its national law applies by virtue of public international law; and
- Third, if the data controller is established outside the EU but equipment is used in the EU for the purposes of processing data.[29]

In cases where the controller is established in more than one EU Member State, it must comply with the law of each Member State where it has an establishment. However, if a

25. Currently, exceptions to the registration obligations exist in Sweden, Denmark, and Finland. Also, the data protection laws of The Netherlands and Germany allow a choice between registration or appointing a third-party privacy officer. It is presently unclear whether it is possible to name a single representative for the entire EU, or whether a representative must be named in each Member State where processing takes place.

26. *See* Directive 95/46/EC, *supra* note 4, art. 4(2).

27. *See, e.g.*, Lee A. Bygrave, *European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation*, 16 COMPUTER L. & SECURITY REP. 252 (2000); *see also* Peter P. Swire, *Of Elephants, Mice and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998).

28. The wording of article 4 leaves it unclear as to whether the article is only a choice of law provision, or whether it is also intended to apply to jurisdiction. It is assumed here that the likely intent of the drafters was that the provision should apply to both areas.

29. Directive 95/46/EC, *supra* note 4, at art. 4(1).

EU-based controller also processes data in other Member States without being established there, then such processing is governed by the law of its home jurisdiction.

To take the first possibility, it is necessary to determine who is the data controller. A factual inquiry would be necessary to see if Company X was the controller of the data in the EU, but if the data processing was carried out by an Internet user surfing directly on Company X's U.S. website (rather than on a European website run by the Company), then Company X should probably be held not to be a data controller.[30] Company X's sales to customers in Europe would not by themselves make the Company established in Europe.[31]

As the second possibility applies only in special circumstances (such as regarding embassies of EU Member States), we can move on to the question of whether the Directive would apply to Company X by virtue of the third possibility, that is, whether it makes use of equipment in the EU to process data. Heretofore, there has been great uncertainty in Europe as to what constitutes equipment under the Directive. It is clear, for example, that servers located in the territory of an EU Member State that a European user can access would constitute such equipment, while a server located outside Europe that a European user accesses by means of the telephone network would not.[32] The greatest uncertainty has concerned cookies[33] sent to the hard drives of users in Europe from servers based outside the EU. It seems clear that devices such as cookies were not contemplated when the Directive was drafted.

Recently, in its paper *Privacy on the Internet: A Integrated EU Approach to On-line Data Protection*, the Article 29 Working Party has taken the position that, in the case of the sending of "a text file installed on the hard drive of a computer which will receive, store and send back information to a server situated in another country" (i.e., a cookie), the national law of the EU Member State of the user will apply to the processing of such data.[34] This means, in effect, that EU data protection law is to apply to the entire Internet, since many websites around the world use cookies as one of the simplest and most effective methods now available for authenticating visitors to their websites.

It is not clear if EU regulators are fully aware of the implications of such a breathtakingly broad assertion of jurisdiction. When one examines academic writings, case law, and legislation relating to international jurisdiction, it becomes clear that, prior to the Internet, there never existed a situation in which a state purported to extend its jurisdiction to many millions of entities in different countries around the world based on the fact that they were accessible by, or processed data of, citizens of the home jurisdiction.

30. Note, however, that there may be more than one controller in a particular instance, and that the controller may "change from one data-processing operation to another, even within one information system." Bygrave, *supra* note 27, at 254.

31. Recital 19 of the Directive defines establishment as implying "the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or subsidiary with a legal personality, is not the establishing factor. . . ." Directive 95/46/EC, *supra* note 4, at recital 19. However, it is not clear, whether, under the Directive, the establishment in the EU must be connected in some way to the data processing in order to lead to the application of EU law. *See* ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE 127 (1st ed. 1997) (suggesting that the key factor is the place of the "establishment in the scope of which the processing takes place" (translation by author)).

32. *See id.* at 129–30.

33. Cookies are small text files sent automatically by many Internet servers to users who access Web pages, and are generally used to authenticate users.

34. ARTICLE 29 WORKING PARTY, *supra* note 2, at 28.

In this context, it is useful to differentiate between legislative or judicial jurisdiction and enforcement jurisdiction, that is, between the power of the EU, or an EU Member State, to apply its data protection laws to websites outside the EU that process data of EU citizens by means of cookies or other similar devices over the Internet, and their ability to enforce any such assertion of jurisdiction. The answer to whether the application of EU data protection law to foreign websites using cookies depends on whether one views data protection law as a purely domestic measure to protect EU citizens, or whether one emphasizes the foreign element involved. There seems to be no doubt that certain instruments of EU consumer protection law also apply to non-EU persons or entities that choose to do business with EU citizens.[35] The difference here is that the seller of goods or services to an EU citizen has chosen to do so, while there is no foolproof way for websites that set cookies to limit their activity to non-EU citizens. Moreover, extending jurisdiction to all Web servers around the world that set cookies results in an assertion of jurisdiction exponentially greater than that of asserting jurisdiction over foreign entities that have chosen to do business with EU citizens, both in quantity and in kind. It is hard to resist the conclusion that this is a kind of regulatory overreaching, that is, "a situation in which rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced."[36] Moreover, since the Directive provides that a controller not based in the EU that makes use of equipment in the EU to process personal data must comply with the national data protection law of each Member State in which such data is processed (meaning each Member State in which a user could access the controller's Website),[37] in effect the controller would have to comply simultaneously not only with the law of every EU Member State, but also with the law of its home jurisdiction, which hardly seems to be a reasonable burden to impose.

With regard to the jurisdiction of the EU Member States to enforce their own data protection law on foreign websites outside its borders, the answer is clear that this would be in violation of international law. The statements of one eminent commentator on international jurisdiction in another context are particularly relevant here:

> [I]s it open to a State to have resort to its own legal system and, in particular, its own courts for the purpose of making the conduct of foreigners in foreign countries conform to its own commands? . . . It would seem that the answers to the above questions must be in the negative. Any other result would be repugnant to one's commonsense and the dictates of justice, to that distribution of State jurisdiction and to that idea of international forbearance without which the present international order cannot continue. With one single exception the practice of all States seems to be in accord with this view. When that single State, viz. the United States of America, propounded the opposite philosophy, it was at once confronted with diplomatic protests.[38]

35. For example, it seems to be accepted that Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 (Distance Selling Directive) applies as well to non-EU-based entities that sell goods by mail, Internet, etc., to EU citizens. *See* Council Directive 97/7/EC, 1997 O.J. (L144) 19.

36. Bygrave, *supra* note 27, at 255.

37. Directive 95/46/EC, *supra* note 4, art. 4(1). The Working Party's paper on *Privacy on the Internet: An Integrated EU Approach to On-line Data Protection* states this explicitly: "If the computer is situated in an EU country and the third party is located outside the EU, the latter shall apply the principles of the national legislation of that Member State to the collection of data via the means of the cookie." *See* Directive 97/7/EC, *supra* note 35, at 28.

38. F.A. Mann, *The Doctrine of Jurisdiction in International Law*, 111 RECUEIL DES COURS 9, 145–46 (1964).

The EU will thus be in the position of asserting a jurisdiction it cannot hope to enforce, which seems a particularly hollow and meaningless form of jurisdiction, and which will only undermine general respect for data protection law. It would also be ironic if, as pointed out in the quotation above, EU countries were now to take action that has been criticized when taken previously by the U.S. government. And with regard to the view sometimes expressed by European data protection regulators that, even if they lack the power to enforce their laws outside the EU, they could get violators when they set up shop in Europe, one can only hope that the regulators are familiar with elementary legal principles such as the existence of separate legal personalities by corporate subsidiaries, the disregard of which would result in the trampling of the basic rights that the data protection laws are supposed to protect.

Whatever one's views on this dubious assertion of extraterritorial jurisdiction, the end result for companies is that it pays to ensure that Internet sites served from outside the EU, but could conceivably come within the supervision of EU data protection authorities (e.g., because they collect data from EU residents or otherwise target them), comply with at least the general principles of EU data protection law, or at least that the company running the site has a strategy in place for dealing with inquires from EU data protection authorities. This need is naturally greater the closer the company's connection with the EU, for example, if the company is planning to establish operations in the EU in the near future. However, the question of whether it is worth registering as a data controller in an EU Member State should be approached more cautiously, since doing so will be deemed a submission to the jurisdiction of the respective data protection authorities.

IV. Conclusion

At present, compliance with EU data protection law in e-commerce is as much an exercise of risk management as it is a legal exercise. Most successful e-commerce businesses are based on techniques and technologies that are problematic under EU law, which presents a choice between strict compliance with the law and complying with business realities, which is often a choice between staying in business and not. Thus, the best course is usually to prioritize the potential risks, and decide how much risk a company is willing to deal with. However, there is no question that the regulatory wind in Europe is blowing in the direction of stricter enforcement of data protection laws, and that this will lead to increasing conflict between companies engaged in electronic commerce, and a regulatory structure much stricter than that which many non-EU companies are used to.