European Data Protection Law and Restrictions on International Data Flows

Paul M. Schwartz*

We live in a world of international data transmissions. Digitalization of information, combined with continuous and dazzling technological developments, has increased the flow and application of data. Information sharing now takes place on an international scale and involves a tremendous amount of data referring to individuals. Among the critical regulatory challenges raised by such international information flows is how to protect individual privacy.

In Europe, where this issue receives the most concerted attention in the world, the response is found in "data protection law." This term refers to the legal structures that attempt to regulate knowledge and concealment of an individual's personal information. Important trans-European efforts

---

* © Paul M. Schwartz, 1995. Professor of Law, University of Arkansas (Fayetteville). This Article was presented to a faculty symposium at the University of Cincinnati College of Law and at a conference held at the Annenberg Center for Communication Policy Studies in Washington, D.C. Comments and suggestions made on these occasions proved highly useful.

For their comments on previous drafts, I wish to thank Jutta Körbel, Spiros Simitis, Joel R. Reidenberg, and John Applegate. Anne Arendt and David Gay provided superb bibliographic assistance. Terri Yeakley helped me with her usual excellent administrative skills.

1. For an overview of the kinds of personal information involved in transborder exchanges, see Reinhard Ellger, Der Datenschutz im grenzüberschreitenden Datenverkehr 108-29 (1990). Ellger finds that the most intensive transborder data flows occur in the following areas: (1) personnel departments; (2) banks, insurance companies, credit card companies, and credit bureaus; (3) direct marketing; (4) airlines, travel agencies, and other business involved in tourism; (5) companies that seek to deliver goods to or otherwise trade with international customers; and (6) within the public sector: police, customs, tax departments, and public pension agencies. Id. at 129. For a discussion of computer reservation systems that involve international transmissions of personal information, see Joel R. Reidenberg, Personal Information and Global Interconnection: The Challenge of Regulatory Convergence, 18-19 Project Prometheus Persp. 27 (1991).

These international transmissions of data depend on a variety of digital world networks, both wired and wireless. According to a recent report, Bill Gates, the chief executive officer of Microsoft Corp., believes that the future of the computer industry rests with these networks. Richard Brandt & Amy Cortese, Bill Gates's Vision: He's Pushing Microsoft Past the PC and onto the Info Highway, Bus. Wk., June 27, 1994, at 56, 60. The explosion of low-cost networks will continue to alter how we use information technology in the next decade. Id. at 56.

have accompanied data protection within European nations. These efforts aim to create strong European protection for individual privacy in the computer age.

Yet, in an age of international data flows, these measures would be doomed to failure if their reach ended at the borders of Europe. Permitting an abuse of European citizens' personal information outside of Europe would make a mockery of the decades of efforts expended in creating high levels of protection. Many European nations have responded by extending their national laws to regulate extra-territorial activities involving the personal data of their citizens. Under certain conditions, such domestic laws even permit the blockage of transfers of personal data.

In a fashion similar to these domestic measures, both the Council of Europe and the Commission of the European Union have made important efforts at the trans-European level to address the issue of international data transfers. Like the national data protection laws, legal instruments created by these two institutions permit the blockage of data transfers to countries with insufficient protection. These national and Europe-wide measures may pose significant challenges to the free flow of data to the United States.

This Article's goal is not, however, to assess the extent to which American law meets the requirements of these European standards. Rather, this Article carries out a critical task that is preliminary to the forming of any such judgment: It assesses the complex European structure for deciding the permissibility of international data exports. This Article analyzes both the substance of the relevant standards and the applicable process by which these standards are applied.

In Part I, this Article explores the content of substantive European standards regarding international data transfers. Two general standards exist for deciding the permissibility of international data transfers: the "equivalency" and the "adequacy" principles. The data protection law of most European nations sets out an equivalency standard. Part I conducts a brief survey of European laws relevant to the equivalency standard. It then considers the European Union’s Directive on Data Protection (Directive), which, by contrast, contains an adequacy standard. The current uncertainty regarding the relation between the equivalency and adequacy standards complicates analysis of the permissibility of transfers of personal data. Although the Directive seeks to harmonize an existing area of European law, it may lead to dissonance. In this sense, the Directive is illustrative of


3. Such an analysis requires an assessment of the level of protection through attention to all the conditions surrounding a specific planned transfer. See infra notes 103-04 and accompanying text.

broader problems that the European Union is likely to face as it attempts to bring uniformity to diverse national standards.\(^5\)

Part II considers the application of substantive standards regarding international data transfers. This Part examines an administrative body that is unknown in the United States but common to most European nations: the data protection commission, which is an agency that oversees data processing practices.\(^6\) European data protection law has generally granted these agencies authority over international transfers of personal information through the creation of a new kind of coercive international legal action, which this Article terms "the data embargo order."\(^7\)

Part II then explores the nature of data embargo orders. It surveys the relevant aspects of European law and considers how the data embargo order relates to the functioning of data protection commissions. This order reinforces the ability of data protection agencies to stimulate social, political, and legal debate about information technology. Indeed, the data embargo order insures that data protection commissioners will play an important role in this discussion.

I. EUROPEAN RESTRICTIONS ON FLOWS OF PERSONAL INFORMATION

Numerous European standards, national and supranational, permit the blockage of international flows of personal information. To avoid such a blockage, these standards usually require a foreign nation to have an equivalent level of data protection. According to the Directive, however, only an adequate level of protection is needed before such a transfer may take place. An adequacy standard appears to require a lower level of data protection than an equivalency standard. An exploration of these two substantive norms and the relationship between them follows.

A. The Equivalency Principle: European National Laws and the Council of Europe's Data Protection Convention

The domestic laws of most European nations call for an equivalent level of protection in a third country before a data transfer can be permitted. This approach is echoed by the Council of Europe's "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (Convention).\(^8\) This document is a European treaty opened for signature in 1981 and acceded to by nineteen nations.

5. See infra notes 93-123 and accompanying text (discussing the Directive's adequacy standard and its effect on the level of data protection among the European Union's Member States).

6. For an illustration of the German, French, and Swedish models, see Flaherty, supra note 2, at 26-29, 101-03, 172-74.

7. This term refers to an order that blocks or limits a foreign transfer of personal data. European law usually assigns the power to issue such orders to a national data protection authority. See infra part II.A (discussing the data embargo order).

1. National Laws in Europe

On the national level, many European data protection laws expressly permit the blockage of international transfers of personal information. Indeed, developments at the Europe-wide level have not altered the significance of these diverse measures. Most European nations require "equivalent protection" in another country before allowing transfers of personal data outside their borders. Some differences exist in the wording of these laws, however, and, as a result, existing limitations on European data flows can be understood only by analyzing the laws of each country individually. A brief discussion of the statutory provisions in Belgium, Denmark, France, Germany, the Netherlands, Portugal, Spain, and the United Kingdom illustrates the various approaches.9

Among the nations that explicitly set out an "equivalency" standard are Portugal and Spain.10 Other countries, such as Belgium and France, do not express an explicit statutory standard in their national data protection laws. However, the data protection laws of Belgium and France suggest that some international transfers are impermissible.11 Indeed, the French statute provides for development of a substantive standard for judging data transfers without legislative amendment of the national data protection law. It permits the Conseil d'État to issue a decree regulating transmissions of personal data between France and other countries.12 The Conseil d'État has not, however, availed itself of this opportunity to establish such a criterion.13

Other countries, while avoiding specific use of "equivalency" language, have statutory standards permitting exports of personal data only if the treatment of the information in the receiving nation is consistent with native protection. The laws of Great Britain and Denmark exemplify this approach. Great Britain forbids any transfer that "is likely to contravene, or lead to a contravention of, any of the data protection principles" as they relate to such data.14 Similarly, the Danish Data Protection Law prohibits

9. All European data protection laws will be cited according to the English text contained in Data Protection in the European Union: The Statutory Provisions (Spiros Simitis et al. eds., 1994) [hereinafter Data Protection Statutes].

10. Law for the Protection of Personal Data with Regard to Automatic Processing, Law 10/91 (Apr. 29, 1991) ("una protección equivalente"), reprinted in Data Protection Statutes, supra note 9, at § 33; Law on the Regulation of the Automatic Processing of Personal Data (Oct. 29, 1992), reprinted in Data Protection Statutes, supra note 9, at § 32 ("un nivel de protección equiparable").

11. Law Concerning the Protection of Personal Privacy in Relation to the Processing of Personal Data (Dec. 8, 1992), art. 22, reprinted in Data Protection Statutes, supra note 9; Act 78-17 on Data Processing, Data Files and Individual Liberties (Jan. 6, 1978) [hereinafter French Data Protection Law], § 24, reprinted in Data Protection Statutes, supra note 9.

12. Id.


transfers by private organizations that cause a “material weakening” of the protection provided by domestic data protection law.\textsuperscript{15}

The Netherlands takes another approach by distinguishing between data exporters established within and without their country. Data exporters established in the Netherlands are held to an “equivalent protection standard.”\textsuperscript{16} In contrast, exporters established outside of the country who fall under the jurisdiction of the Dutch Data Protection Law must provide “adequate safeguards for the protection of the privacy of the data subjects in relation to that file.”\textsuperscript{17}

Germany boasts the most intricate legal standard in the European Community for deciding the permissibility of international data transmissions.\textsuperscript{18} Indeed, this statute makes more than its fair contribution to upholding German law’s reputation for complexity. The relevant provisions, which analysts have interpreted as requiring equivalent levels of foreign protection before an international data transfer, merit careful examination.

Germany’s Federal Data Protection Law offers different statutory language for transfers carried out by the government than for transfers by private companies. When government seeks to carry out an international transfer of personal data, the law commands consideration of one general requirement and two alternative provisions.\textsuperscript{19} The general requirement for government transfers takes the form of a statutory provision establishing an

\textsuperscript{15} The Danish Private Registers Etc. Act (Consolidated) (June 8, 1978), § 21(3) [hereinafter Danish Private Registers Act], reprinted in Data Protection Statutes, supra note 9. In contrast to other European countries, Denmark regulates the public and private sectors in separate laws. The public sector contains no provision concerning data exports. The Danish Public Authorities’ Registers Act (Consolidated) (Oct. 2, 1987), § 16-21 [hereinafter Danish Public Registers Act], reprinted in Data Protection Statutes, supra note 9.


\textsuperscript{17} Id. § 48. Complicating the Dutch scheme, some data exports do not fall under the direct jurisdiction of the Dutch Act. For example, one case without direct jurisdiction exists when the personal data file and the data user are located exclusively outside of the Netherlands. The Dutch Data Protection Law does not permit transfers to such files and data users if they “would have a serious adverse effect on the privacy of the persons concerned.” Id. § 49. For an explanation of the jurisdiction provisions of the Dutch Data Protection Law, see A.C.M. Nugter, Transborder Flow of Personal Data within the EC, 187-90 (1990).

\textsuperscript{18} Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz) vom 20 Dezember 1990 (Dec. 20, 1990) [hereinafter German Data Protection Law], reprinted in Data Protection Statutes, supra note 9. The critical provisions are: §§ 16, 17 (discussing international data transfers by the government), and §§ 28, 29 (concerning data transfers by private organizations). As noted below, German data protection law has no specific provision for international transfers by private organizations; the same sections that apply to these organizations’ domestic transfers regulate such data exports. See infra notes 19-27 and accompanying text (examining and discussing the German data protection model).

\textsuperscript{19} German Data Protection Law, supra note 18, §§ 16, 17(2).
ordre public, or public policy, clause.20 According to the applicable public policy clause, the government may transfer personal information beyond the nation’s borders only when no ground exists for belief that the transfer violates the goal of a German law.21 This public policy provision requires state scrutiny of the data recipient’s planned processing, the foreign country’s protection, and German law’s requirements.22 Leading commentators have interpreted this clause as prohibiting governmental data transfers to nations whose protection is not equivalent to German standards.23

By contrast, international data transfers by private companies are regulated by more general language. The critical statutory language relates to companies’ “transmissions” (Übermittlungen) of personal data, whether this action takes place on a domestic or international level.24 The statute requires an evaluation of whether the “affected party” has a “legitimate interest” in preventing the transfer of the personal information.25 As is the case for the government’s international transfers of personal data, the decision regarding the existence of a legitimate interest against transfer depends on whether an equivalent level of protection exists in a foreign country. As Spiros Simitis succinctly states in his treatise on German data protection law, “Whenever equivalency is lacking, there is a harm to the

---

20. Id. § 17(2). German law also contains other ordre public clauses. See art. 6, Einführungsgesetz zum Bürgerlichen Gesetzbuch, Vom 18 Aug. 1896 (RGBl. S. 604) (BGBl. III 400-1).

21. See German Data Protection Law, supra note 18, § 17(2) (“A communication shall not occur if there is reason to assume that this would be a violation of the purpose of a German law.”).

22. Spiros Simitis, § 1, in Kommentar zum Bundesdatenschutzgesetz 77-78 (Spiros Simitis et al. eds., 1992) [henceforth Simitis et al., Data Protection Treatise].


In addition to the requirements of the ordre public clause, Germany’s Federal Data Protection Law requires the consideration of two additional provisions when an international transfer of personal information by the government is at stake. These two provisions offer further support for a German requirement of “equivalent” protection in a foreign land. The first alternative requires that the data export be essential to fulfill a proper task of the official agency and that it follow all the requirements of the Federal Data Protection Law for the storage, processing, and application of personal information. German Data Protection Law, supra note 18, § 16(1). The second alternative requires both that the designated recipient possess a “justifiable interest” in receiving the data, and the affected party lacks a “legitimate interest” in preventing the transfer. Id. § 16(2). These two alternatives share an important trait: both require that exportable information receive the same level of protection in the recipient nation as under German law. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 77-78.

24. The German Data Protection Law defines “transmission” of “personal-specific information” as “the disclosure of individual stored data, or data generated by data processing, to a third party (recipient) in such a manner . . . that the data are passed on to the recipient by the storing facility.” German Data Protection Law, supra note 18, § 3(5)a. The permissibility of a private body’s data “transmissions” are controlled by § 28 or § 29. Id.

25. Id. §§ 28(1), 28(1)a, and 29(1)1.
affected party's 'legitimate interest.'”26 The determination that equivalent protection exists must be made before transmission of data abroad.27 Thus, in data transfers by both government and private companies, German law requires that personal information be transferred only to foreign countries offering equivalent data protection.

2. The Council of Europe's Data Protection Convention

The Council of Europe, an intergovernmental organization established in 1949, seeks to create greater unity among European nations. At present, the Council's “Convention on Data Protection” is the most important Europe-wide agreement regarding the processing of personal information.28 The Convention is a “non-self-executing treaty”; its standards do not directly impose binding norms on signatory nations.29 However, it does require signatory nations to establish domestic data protection legislation that will both give effect to the Convention's principles30 and provide a common core of safeguards for the processing of personal information.31 Domestic standards can, in turn, exceed these basic safeguards. As Article 11 of the Convention states, domestic law can "grant data subjects a wider measure of protection than that stipulated in this convention.”32

The Convention's common protective core contains a number of elements. Among the most important is Article 5's requirement of "data quality.”33 "Data quality" refers to a number of concepts relating to fair information practices. In its broadest sense, data quality requires that personal information be "obtained and processed fairly and lawfully.”34 It also requires that personal information be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes.”35 Moreover, the concept of data quality limits the processing of personal data to circumstances that are "adequate, relevant, and not

26. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 84. See Auernhammer, supra note 23, at 378 (noting the need for examination, first, of whether data protection law exists in the importing nation and, if it does, whether the law is “essentially equivalent” to German law).
27. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 84.
29. Ellger, supra note 1, at 463. See Nugter, supra note 17, at 26 (“Individuals may not invoke the Convention before their national court.”).
31. See Convention, supra note 8, art. 4(1) (“Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.”).
32. Id. art. 11.
33. Id. art. 5.
34. Id.
35. Id.
excessive in relation to the purposes for which they are stored." Beyond data quality, the Convention calls for individual rights permitting access to and correction of personal data. Domestic law is to provide judicial remedies for violations of these rights.

The Convention also contains an important provision regarding transnational flows of personal data. In its Preamble, the Convention expresses a goal of "reconcil[ing] the fundamental values of the respect for privacy and the free flow of information between peoples." The Convention reconciles these values by requiring free flows of data among signatory nations unless otherwise expressly provided. The most important of its exceptions to this free flow rule applies to a signatory nation that has created "specific regulations for certain categories of personal data." The Convention permits, but does not require, signatory nations providing these specific regulations to block data exports to another treaty party that lacks equivalent levels of protection. Although this treaty does not explicitly discuss direct transfers of data to nonsignatory nations, it has been interpreted as requiring equivalent standards in these lands. Thus, nonsignatory nations, such as the United States, are considered subject to the Convention's provisions for "equivalent" protection.

The Convention is not meant to displace national regulations. Rather, by requiring signatory nations "to give effect to the basic principles for data protection," it seeks to create an important stimulus and point of reference for domestic data protection activities. The Convention has, however, been the subject of some criticism. European commentators have pointed out the diversity of national interpretations of the Convention's requirements. For example, some nations have decided to follow Article 6 and create special protection for certain kinds of sensitive data while others have not. Considerable differences also exist in national data protection law regarding the extent of information disclosed to individuals.

36. Convention, supra note 8, art. 5.
37. Id. art. 8.
38. Id.
39. Id. pmbl.
40. Id. art. 12.
41. Convention, supra note 8, art. 12(3)(a).
42. See id. (stating that a nation with specific regulations may limit exports to a second signatory nation when the other party's regulations do not provide equivalent protection).
43. See id. art. 12; see also Ellger, supra note 1, at 475-83. Professor Spiros Simitis has complained of the "poor formulation" of the Convention's text. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 113.
44. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 114-15.
45. Id. at 107.
46. Convention, supra note 8, art. 4(1). For a discussion of the influence of the Convention, see Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 98-99.
47. Nugter, supra note 17, at 249, 253; Schweizer, supra note 28, at 543.
48. Schweizer, supra note 28, at 543.
about their files. Yet, as examples from Irish and French law illustrate, the Convention has not been without some positive influence.

In its regulation of data transfers outside of Ireland, the Irish Data Protection Act of 1987 makes explicit reference to the Convention. Indeed, the effect of this language is to incorporate the Convention by reference into Irish data protection law. In evaluating a proposed transfer of personal data to a nonsignatory nation, the Irish Data Protection Commissioner must determine if the export would “lead to a contravention of the basic principles for data protection set out in . . . the Convention.” This provision serves to prohibit data transfers to lands that do not meet the Convention’s minimum standards. In France, the data protection commission, the Commission nationale de l’informatique et des libertés (CNIL), has frequently applied the Convention’s notion of “data quality.” This provision has influenced decisions of the CNIL regarding health care data, credit information, and education records. In the CNIL’s interpretation, the Convention merely provides additional specification for underlying concepts already present in French data protection law. Ireland and France are only two of the European nations where the Convention has served to strengthen the protection of personal information.

The Council of Europe’s official data protection “recommendations” have furthered the Convention’s role as a stimulus and point of reference for domestic legislative efforts. These documents, which the Council’s Committee of Ministers issues, seek to strengthen data protection in individual Member Nations by specifying how the Convention’s core principles should apply to specific sectors of data processing activities.

49. Id.
50. Irish Data Protection Act of 1987 (July 6, 1987), art. 11(2) [hereinafter Irish Data Protection Law], reprinted in Data Protection Statutes, supra note 9.
51. See id. See also Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 98-99 (noting reliance on the Convention in the Irish Data Protection Law). Indeed, this incorporation is by more than just reference: Article 1 of the Irish Act states that the Convention’s text is to be set out in “the First Schedule to this Act.” Irish Data Protection Law, supra note 50, art. 1(1) (emphasis omitted).
52. Irish Data Protection Law, supra note 50, art. 11(3).
54. Id.
55. Id.
56. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 99.
57. These recommendations concern personal data used in automated medical data banks, for scientific research and statistics, for the purpose of direct marketing, for social security purposes, in the police sector, for employment purposes, for payment and related operations, and for transfer by the government to third parties. For the text of these recommendations, see Data Protection Statutes, supra note 9.
58. See Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 121.
The Council's Committee has issued eight recommendations thus far.


The Directive or, more formally, "European Parliament and Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," is a proposed regulation of the European Union that, once promulgated, will bind its twelve Member Nations. Although most domestic laws in Europe and the Council of Europe's Convention call for testing data transfers by an "equivalency standard," the Directive takes a different approach. It requires "an adequate level of protection" to be in place in any third country.59

Because of the critical importance of this document, this Article first examines its background and general contents. It then examines the Directive's standard for judging the permissibility of international data transfers.

1. **The Background of the Directive**

The European Union seeks to create a wide-reaching union among the citizens of its twelve Member States. Its goals of integration are broad. As one textbook explains, "The aspirations of the [Union] ... encompass economic, social and political matters."60 Although the Union has devoted great effort to creating a common economic market, that market must have a foundation of more than just shared fiscal concerns. Jacques Fauvet, the president of the French Data Protection Commission, formulates the critical issue as, "Do we want a Europe of merchants or one of human rights?"61

As President Fauvet's statement indicates, the data protection commissioners of individual European nations have directed the Union's focus to privacy issues. These officials have insisted that data protection be viewed as a precondition for the intensive economic cooperation that the Union is creating.62 Complaining of the "sweeping abstinence" of official Union institutions concerning data protection,63 the commissioners have sought the creation of binding standards for all Member Nations and for the Union's own institutions.64 A high point of this effort came at the

---


62. For the French efforts in this regard, see id. at 75-77.

63. The words are those of Dr. Alfred Einwag, then the Federal Data Protection Commissioner of Germany. Alfred Einwag, Grenzüberschreitender Datenverkehr aus Sicht des Bundesbeauftragten für den Datenschutz, 6 Recht der Datenverarbeitung 1, 2 (1990).

64. Id.
Eleventh Annual Meeting of Data Protection Commissioners in Berlin during 1989, when the commissioners of the Member States of the Community issued a resolution demanding Europe-wide action.65

This emphasis on privacy protection has become necessary because European integration has increased the sharing of data among Member Nations and even created new, intense demands for personal information. As the Federal Data Protection Commissioner of Germany observed, "[T]he European Community is also becoming an information and data community."66 Accordingly, the European Union has placed new demands on Member States regarding the collection of personal information. It already has established data banks concerning law enforcement and border controls.67 The Union is considering the creation of data banks concerning agricultural subsidies, political asylum, and customs.68

The Union's period of inaction regarding the protection of personal privacy is over; after two official drafts, its Directive on Data Protection is close to enactment. This directive seeks the "harmonization" of European data protection law.69 "Harmonization" is a technical term of European Community law that refers to formal attempts to increase the similarity of legal measures in Member Nations.70 A harmonizing directive does not seek absolute uniformity of law, but the establishment of "a basic structure, with more or less detailed provisions, to which Member States must conform."71

Compared to the Council of Europe's Convention on Data Protection, the Directive does, indeed, have great promise for creating harmonization in this area. To begin with, by its very nature the Convention is fated to have a more limited legal influence. The Convention can have direct binding effect only to the extent that it is adopted in domestic statutes.72

In contrast, citizens and data protection commissioners alike can directly


68. Id.


70. Bermann et al., supra note 69, at 430.

71. Id.

72. Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 108.
rely on a directive should a member nation fail, by a stated deadline, to promulgate domestic law that implements its measures. Moreover, reliance on a directive's principle effect is possible when domestic law, even if punctually promulgated, fails to implement the directive correctly and completely. Finally, the Directive will do more to harmonize European law than the Convention because of its greater detail. Its additional specifications should increase the shared elements within domestic European data protection laws.

After several drafts, the Directive is close to its final form. The Directive seeks to ensure a high level of protection within the Union for "the fundamental rights and freedoms of natural persons, and in particular their right to privacy." Without sufficient data protection, the processing of personal information is not permissible. The Directive sets out mandatory critical principles for personal data processing. These principles address the conditions required for data processing, including the information about data use that must be given to individuals. The Directive also provides rights of access and correction to the individual and sets out the necessary provisions for judicial remedies and penalties for the breach of guaranteed rights.

The Directive not only focuses on required principles for data protection, but also attempts to structure national and international oversight of compliance with its provisions. It requires the creation of "supervisory authorities" in each nation, who are to "act with complete independence in exercising the functions entrusted to them." The Directive obligates member states to consult these data protection commissions when promulgating "administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard

73. Weatherill & Beaumont, supra note 60, at 116.
74. Id.
75. Thus, the English text of the Directive takes up 57 pages in Data Protection Statutes, compared to the Convention's 11 pages. Data Protection Statutes, supra note 9.
77. Directive, supra note 4, art. 1(1).
78. See id. art. 7 (personal data may be processed only if stated conditions set out in Directive are met).
79. Id. arts. 6-25.
80. Id.
81. Id. arts. 12, 22-24. For strong criticism of the Directive's exceptions to its requirement of a right of access, see Simitis, supra note 67, at 459.
82. Directive, supra note 4, art. 28(1).
to the processing of personal data." Member States are to inform the data protection commissions when they carry out "any wholly or partly automatic processing operation," and the commissions are to be granted the authority to hear claims concerning the protection of "rights and freedoms in regard to the processing of personal data." Further, these national data protection commissions are to "cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."

In addition to requiring independent national data protection commissions, the Directive creates a new institution of data protection oversight on the Europe-wide level. It calls this new oversight body, the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" (Working Party). The Working Party has "advisory status" at the Commission and consists of representatives of the national data protection commissions, Community institutions, and the Commission of the European Union. The Working Party is given broad authority to "act independently" and "may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community." The Directive also instructs this body to provide the Commission with opinions "on the level of protection in the Community and in third countries."

2. The Directive and International Data Transfers

The Directive first sets a strong standard for protection among Member States and then insists on a free flow of information within the Union. Equivalency is the required standard for data protection among Member States. To obtain this level, the Directive sets out detailed requirements that seek to harmonize the domestic law of the Member States. Outside of the Union, however, the Directive will have no such effect and the level of protection will vary more dramatically by nation. As a result, it generally permits transfers of personal information only to nations with "an adequate level of protection."

This Article now discusses the Directive's adequacy standard and its approach to judging the level of foreign data protection. It also sets out

83. Id. art. 28(2).
84. Id. art. 18(1).
85. Id. art. 28(4).
86. Id. art. 28(6).
87. Directive, supra note 4, art. 29.
88. Id.
89. Id. arts. 29(1), 30(3).
90. Id. art. 30(1)(b).
91. The Directive states, "Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all the Member States. . . ." Id. pmbl. at para. (8).
92. Directive, supra note 4, art. 25(1).
the Directive’s provisions for creating lists of nations with inadequate data protection law and analyzes the controversy surrounding the question of whether this document sets minimum or maximum standards for Member States.

The Directive is quite explicit about the need for limits on transborder data flows in the name of privacy. Indeed, the British Data Protection Registrar, Eric Howe, has likened the Directive’s approach to the erection of a fence around Europe. In his 1993 annual report, he observes:

If there is to be a Community with an acceptable and high level of individual data protection, which thereby permits the unrestricted transfer of personal data throughout the Community, then it is to be expected that there will be a fence around the Community with some means of guarding it. Transborder data flow controls are to be expected and are legitimate.

The fence around the personal information of citizens is established by the controls on transborder data exports in Chapter IV of the Directive.

The approach of the Directive in Chapter IV is to provide a general rule that contains numerous exceptions. The Directive, unlike the Convention, sets out explicit provisions concerning the conditions of transfers to non-Member Nations. It states that transfers are to be permitted “only if . . . the third country in question ensures an adequate level of [data] protection.” The decision as to adequacy is to be made on the Member State level, although the Commission itself may “enter into negotiations” with countries with inadequate data protection “with a view to remedying the situation.” As this Article later discusses, the Directive also provides for other Commission activity concerning international data transfers—most notably, the creation of lists of third countries with inadequate protection. Data flows with these lands, which we can call “data protection outlaw nations,” are not permitted.

From its general requirement of adequate protection, the Directive provides six, independent exceptions. The exceptions apply to situations in which: (1) “the data subject has given his consent unambiguously”; (2) the transfer is necessary to perform a contract involving the data subject, or to implement “precontractual measures taken in response to the data subject’s request”; (3) “the transfer is necessary for the performance of a contract concluded in the interest of the data subject”; (4) “the transfer is necessary on important public interest grounds”; (5) “the transfer is necessary in order to protect the vital interests of the data subject”; or (6)
the transfer is made from a register which is intended to provide information to the public.\textsuperscript{100}

Some European experts have criticized the Directive’s approach to international data transfers. For example, Peter Dippoldsmann has pointed out that it is incongruous to require equivalent protection within the European Union and merely adequate protection for transfers to third nations.\textsuperscript{101} He has noted that individuals are likely to know even less about how their data are used in third nations than within Europe. Transfers to such third nations must, therefore, be seen as inherently of greater risk than data use within the Union.\textsuperscript{102}

Having established an adequacy standard and provided exceptions to it, the Directive also details the approach for determining the level of protection provided by third nations. The Directive calls for an evaluation of adequacy “in light of all the circumstances surrounding a data transfer operation or set of data transfer operations.”\textsuperscript{103} More specifically, it requires that “particular account” be taken of:

[T]he nature of the data, the purpose and duration of the proposed processing operation or operations, the country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.\textsuperscript{104}

This approach calls for a contextual analysis of the protection in place in a third country. The Directive requires an examination of the nature of the data, the conditions of a specific planned transfer, and the type of protection offered by both the legal order and the relevant business practices in the receiving nation.

The Directive’s required analysis of planned data transfers is not without problematic elements. Among others, it allows business practices in the receiving nation to be scrutinized in a potentially uncritical way and specifically permits contracts that add to the level of data protection available in a given country. The Directive specifies that the assessment of the adequacy of protection should take into account business practices in the third country. These “professional rules” can also include “codes of conduct” of a single business or of an entire industry.\textsuperscript{105} Yet, companies

\begin{footnotesize}
\par
100. Id. art. 26(1).
101. Peter Dippoldsmann, Europäische Union und Datenschutz, 27 Kritische Justiz 369, 377 (1994). See Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 136 (noting that it is “not only bewildering but simply untenable” to require a lesser standard for transfers outside of the Union than within it).
103. Directive, supra note 4, art. 25(2).
104. Id.
105. Indeed, the Directive recommends that Member States and the Commission encourage the drawing up of codes of conduct. Id. art. 27. It requires Member States to
\end{footnotesize}
sometimes refuse to share information regarding their professional standards, which are, moreover, generally subject to unilateral change. As a result, some data protection experts have argued that professional rules cannot be considered apart from legislative provisions of the third country in question.

A second weakness in the Directive is the exception to the adequacy principle that permits use of a contract. Article 26(2) permits Member States to "authorize a transfer of personal data to a third country which does not ensure an adequate level of protection" should "appropriate contractual clauses" exist. This exception provides a "contractual solution" to the problem of inadequate data protection. Under this approach, the data exporter and the data importer will draw up a written agreement concerning the transfer. The agreement's provisions should create "sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals."

European experts are skeptical of structuring data protection through contracts rather than legislation. The Directive recognizes this skepticism and thus contains an important safeguard regarding contractual data protection. This safeguard structures the internal European disclosure of proposed applications of a contractual solution. According to the Directive, a Member State that wishes to grant authorization for an Article 26(2) transfer must disclose its intention to the Commission and to the other Member States. Both Member States and the Commission may issue objections to such authorizations.

The Directive hopes to encourage collaboration between Member States by requiring them to share any information about reliance on contractual solutions. This provision is not the only instance in which the Directive structures behavior between Member States. The most dramatic example of such cooperation is the Directive's provisions for blocking transfers of personal data to outlaw nations. The Directive requires that "Member States and the Commission... inform each other of cases where they consider that a third country does not ensure an adequate level of protection." If the Commission then finds that a third country does lack adequate protection, Article 25(3) authorizes Member States to inform the Commission that they "will no longer authorize transfers to the third country and that they may take any other measures they consider necessary to protect the data subjects."
not actually ensure an adequate protection level, Member States are to “take measures necessary to prevent the transfer of data of the same type to the third country in question.” This language obliges Member States to cut off flows of personal information to such lands. No provision in the Directive has potentially greater consequences for the United States.

Also significant for the United States is whether the Directive sets minimum or maximum transfer standards. As discussed in Part I of this Article, most European nations require “equivalency” in foreign lands before permitting international data transfers. The Directive defines a standard of “adequacy,” which sets out a more lenient requirement. If the Directive sets out only minimum standards, it will permit Member States to enforce their higher standards for international data transmission. The Council of Europe’s Convention takes this approach; it sets only minimum standards. Thus far, however, no definitive answer can be given as to whether the Directive takes this approach.

The Directive does, however, contain one indication that it might, in fact, set out only minimum standards. Its Article 25(1) states that a “transfer to a third country of personal data . . . may take place only if [in] . . . compliance with the national provisions adopted pursuant to the other provisions of this Directive.” According to one interpretation, an international transfer of personal information will be in “full compliance” only when it also meets the higher standards of protection found in a relevant Member State’s domestic law.

Pressure exists within the Union to view the Directive as setting only minimum standards. Examples of such pressure can be found in France and Germany. In response to concerns of the French Data Protection Commission, the lower house of the French parliament, which is the National Assembly, adopted a resolution urging national opposition to adoption of the Directive in the absence of an assurance from the European Union that the more protective elements of French law would continue to have binding effect. In Germany, the Federal Data Protection Commissioner, Dr. Joachim Jacob, has argued that the Directive raises the question of “subsidiarity,” the Community doctrine that action must be taken whenever possible at or below the Member State level. Jacob views subsidiarity as requiring that “room be found for national

113. Directive, supra note 4, art. 25(4).
114. Convention, supra note 8, art. 11 (stating that the Council of Europe’s Convention also explicitly permits domestic standards to exceed any of its norms and sets out only minimum standards).
116. Directive, supra note 4, art. 25(1).
118. Fourteenth Annual Report of the CNIL, supra note 61, at 77.
realities and traditions. Moreover, no possibility exists in Europe for further improvements in data protection law unless the Directive is seen as setting only minimum standards.

Beyond data protection law, this debate suggests that the Union will face many problems in its attempts to bring diverse national standards closer to one another. As a leading American casebook in the field states, the success of the Union “depends in large measure on its ability to harmonize Member State laws.” Yet, the Directive indicates that difficulties in harmonization will arise not only in the context of directives that set technical standards for health and safety, but also in directives that seek to increase the level of human rights in the Community. Beyond the great difficulties of harmonization, a proposed directive may face its strongest criticism from the countries that are the most active innovators in the area that the Union seeks to regulate. It is no accident that both France and Germany have been quite critical of aspects of the Directive. From their perspective, the Directive raises the threat that domestic protection will be weakened.

II. NATIONAL AUTHORITY OVER DATA EXPORTS AND THE DATA EMBARGO ORDER

Important differences exist among European nations regarding the conditions for permissible international data transfers. As this Article has indicated, a number of nations have statutory standards that allow the blockage of data exports to countries without equivalent protection. Other countries have left the requisite required level of protection open or provide other standards. In contrast, the Directive requires an adequate level of protection in third countries. In addition to these differences in the substantive standards concerning international data exports, a similar lack of uniformity exists in European law’s allocation of authority for approving or denying such transfers.

A. The Data Embargo Order

European data protection authorities generally enjoy some kind of enforcement power regarding international transfers of personal information. This power can include the authority to block data exports by issuing a “data embargo order.” A new and highly significant kind of administrative power, a data embargo order is a command forbidding a planned international data export or limiting the conditions of the export.

A typology of these orders should distinguish between preventative and structural elements. A preventative data embargo order seeks to

---

120. Id.
121. Id.
122. Bermann et al., supra note 69, at 428.
123. Jacob, supra note 115, at 11-13; Fourteenth Annual Report of the CNIL, supra note 61, at 77.
124. This classification reflects one found in the law of remedies. See Owen M. Fiss, The
RESTRICTIONS - INTERNATIONAL DATA FLOWS

prevent harm. A structural order restructures or otherwise alters a planned data transfer to bring it into conformity with the demands of domestic data protection law. A single order might contain both preventative and structural elements.

Although most European data protection commissioners can issue a data embargo order, their exact authority differs widely. One distinction, as we shall see, concerns the extent to which these orders can be directed towards organizations in the public and private sectors. This Article next discusses relevant laws in Denmark, France, Germany, the Netherlands, and the United Kingdom.

The Danish Data Surveillance Authority (DSA) enjoys the greatest statutory ability to issue international data embargo orders. Although the DSA cannot issue embargo orders concerning governmental data transfers,220 this agency can, and does, require prior authorization when private organizations wish to export certain categories of information.221 In private sector cases in which prior DSA permission is not required, the agency still has the power to block private organizations’ transfers of personal information.222 This coercive power also allows the DSA to order a business to implement specific protections as part of its international information transfers.223 Thus, Danish law permits the data protection authority to exercise preventative and structural power over international data transfers by private organizations.

The United Kingdom’s data protection authority, the Data Protection Registrar, also has the power to block international transfers of personal information.224 This power extends to data collections of both government and private organizations. The critical instrument of British law in this regard is the “transfer prohibition notice.”225 The Data Protection Registrar may serve such an order on anyone who “proposes to transfer personal data held by him to a place outside of the United Kingdom.”226 The Registrar can either prohibit the transfer outright or prevent it until action specified in the notice is taken.227 The power in the United

---

220. See Danish Public Registers Act, supra note 15, §§ 16-17.
221. These provisions also apply to international transfers of personal data. Id.
222. See Danish Private Registers Act, supra note 15, art. 21(2) (stating that according to the relevant statute, the Danish DSA’s “prior leave” is required when private organizations “hand over” certain kinds of sensitive information “for electronic data processing outside Denmark”).
223. Id. art. 23(1).
224. Id. art. 23(5).
225. See British Data Protection Law, supra note 14, art. 12.
226. Id. art. 12(1)(b).
227. Id. British data protection law also sets out a right of legal appeal when such an order
Kingdom to issue a data embargo order not only has preventative and structural dimensions, but extends to government and the private sector.

In Germany, by contrast, the Federal Data Protection Law grants an extremely limited power to issue such orders. German law does not grant the Federal Data Protection Commissioner any authority to issue data embargo orders concerning either private-sector or governmental data transfers. Rather, German law delegates the critical authority over the data processing activities of private organizations to a “supervisory authority.” The “supervisory authority” is a German legal term of art that refers to a group of state administrative agencies that have been assigned powers over data processing within the private sector.

The supervisory authority has the power to block international data transfers of a private organization in only one narrow circumstance: The supervisory authority can “prohibit the use of given procedures” only when “technical or organizational shortcomings” exist, and normal supervision and the imposition of administrative fines have not improved these shortcomings. According to one treatise’s analysis, this language indicates that prohibitions of data processing activities are possible only when a private organization does not take sufficient action to remove a serious shortcoming that has been the subject of administrative complaint. The general rule is that a “supervisory authority . . . cannot in individual cases make legally binding determinations concerning disputes.”

German law hopes to prevent impermissible data exports by the creation of legal remedies that apply after the transfer takes place and not by pre-transfer embargo threats.

In the Netherlands, as in the United Kingdom, the power to issue data embargo orders extends to both government and private data

---

133. Actually, the Federal Data Protection Commissioner has no power to apply the Federal Data Protection Law in the private sector. See German Data Protection Law, supra note 18, § 24(1) (“The Federal Data Protection Commissioner shall monitor the compliance with the provisions of this Act and other data protection provisions by public bodies of the Federation.”) (emphasis added). However, the Commissioner can lodge complaints with different organs of government should this official “discover any violation of the provisions of this Act or of other provisions on data protection or some other irregularities in the processing or use of personal data.” Id. § 25.

134. Id. § 38. For a description of these bodies and an analysis of how they carry out their duties, see Irene Wind, Die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich 29-93 (1994).

135. German Data Protection Law, supra note 18, § 38(5).


137. Id.

138. Judicial remedies available to the state and private citizens include monetary damages, fines, and, in some cases, imprisonment of individuals who violate German law. German Data Protection Law, supra note 18, §§ 43-44. Yet, the availability of this relief does not alter Germany’s status as an exception to the European trend of crafting broad administrative authority to issue a data embargo order. An equivalently broad grant of power does not exist under German data protection law.
collections. Unlike British law, however, Dutch law grants the power to issue the relevant instrument, a “General Administrative Order,” not to the Dutch data protection agency, the Registration Chamber, but to the Minister of Justice. Dutch law requires the Minister to consult with the Registration Chamber regarding the issuance of these orders. If sufficient safeguards exist in the receiving nation, the Minister of Justice can also issue exemptions from the requirements of Dutch data protection law. As with the orders blocking exports, the granting of exceptions also requires consultation with the Registration Chamber. Permitting exemptions to the applicable legal standards enables the Dutch government to negotiate the conditions of data exports with companies located in nations with insufficient data protection. These negotiations can lead to a “contractual solution” for proposed data exports.

A contractual solution refers to a written agreement between the data exporter and the data importer. The domestic data protection authority oversees the drafting of an agreement to arrive at a negotiated solution to an otherwise problematic international data transfer. In such a contract, the importer promises to provide additional measures of data protection. The threat of a data embargo order may still be present, but the contractual solution shifts regulation toward a negotiated agreement between the private parties involved in the transfer of personal information. Skepticism exists among European experts regarding the merits of a contractual approach to data protection. The weaknesses of a contractual, rather than legislative, approach to data protection can be shown with reference to one notable application of this approach.

In France, the French data protection commission, the CNIL, is granted data embargo power over the public and private sectors. French law also permits data embargo orders with both preventative and structural elements. The CNIL has drawn on this power to negotiate a “contractual solution” concerning a data export by a private organization.

140. Id. §§ 47-48. In cases when such orders concern a governmental minister, the Minister of Justice must seek approval from another minister. Id. § 3(1).
141. See id. § 3(2) (requiring that the Minister of Justice consult the Registration “regarding the draft text of an Order”).
142. Id. §§ 47(2), 48.
143. Id.
144. Nugter, supra note 17, at 308-09; Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 87-88.
145. Section 24 of the French Data Protection Law gives the Conseil d'Etat, acting “[o]n the proposal of or advised by” the CNIL, the power to establish regulations regarding international data transmissions by private organizations. French Data Protection Law, supra note 11, § 24. According to this statute, the “transmission between France and another country . . . may call for prior authorization or be regulated by decree made in the Conseil d'Etat.” Id. To this day, the Conseil d'Etat has not issued such a regulation. Ellger, supra note 1, at 371.
The data transfer in question concerned information about Fiat-France employees that was to be transmitted to its main company in Italy. Because Italy has no national data protection law, the CNIL required the company’s main branch to sign a contract with its French branch. The resulting contract obligated Fiat-Italy to offer the protection of French law to the information once it was transferred to Italy.

This is a classic example of a contractual solution; the national data protection authority avoided the issuance of a data embargo order by requiring the domestic data exporter and foreign importer to reach a formal agreement mandating domestic levels of protection. The action also illustrates several of the weaknesses of this approach to data transfers. First, a domestic data protection authority lacks the power to enforce such agreements once the personal data leaves the land of its origin. In this case, the CNIL lacked authority to police the contract once the personal data left France. Second, Fiat-France or any domestic exporter may prove unwilling to furnish information regarding contract violations to a domestic data protection agency. A domestic exporter is even less likely to sue its home office or foreign partner to enforce the terms of an agreement. Thus, contractual solutions will, at best, be fated to under-enforcement.

Finally, although this was not the case with Fiat, a contract may rely excessively upon a company’s “code of conduct,” or other written policy defining internal practices regarding data processing. These policies have some potential to improve data protection in the private sector. But, since these business practices are subject to unilateral change, they cannot be seen as commensurate with a foreign nation’s statutory data protection law.

B. The Role of Data Protection Commissions and Commissioners

Despite the differences in the authority to issue the data embargo

---

146. French Privacy Commission, supra note 13, at 125.
147. Id.
148. Id.
149. See Nugter, supra note 17, at 309 (suggesting that the contractual approach should be used only as a temporary solution until the European Community can harmonize national privacy legislation); Simitis, § 1, in Simitis et al., Data Protection Treatise, supra note 22, at 87-88.
150. French data protection law attempts to create incentives for data exporters to provide its national data protection authority with knowledge of at least the initial export of personal information. Article 19 of France’s Data Protection Law requires all registrations of private organizations with the CNIL to state “whether the processing is intended for the dispatch of personal data between France and another country.” French Data Protection Law, supra note 11, art. 19. The use of personal data for reasons other than those set out in the CNIL registration is punishable by criminal penalties. Id. arts. 41, 44.
151. See supra notes 105-107 and accompanying text (discussing the formation of codes of conduct).
orders found in various countries' data protection laws, the data protection authorities enjoy a similarly powerful administrative action. However, thus far these agencies appear to have made scant use of the data embargo order.\textsuperscript{152} Such rarity of application does not, however, diminish the importance of this device. The significance of the data embargo order should not be assessed according to the frequency of its use, but by its relationship to data protection agencies' different functions.

Of the many institutional roles that a data protection agency can fulfill, three are particularly important. First, the data protection commission develops expertise in a critical area that is subject to dazzling technological developments. The commission's knowledge is to be made available to government, business, and private citizens. An area in which this first role has been particularly important is in the collection of medical information. In France, for example, the CNIL has issued strong criticism of an important project designed to increase the computerization of medical information in public and private health care institutions.\textsuperscript{153} Because of its specialization in informational privacy issues, the CNIL was able to identify weaknesses in the project's structure.\textsuperscript{154} In Germany, numerous proposals have been made to replace the current health identification card with a personal "chip card."\textsuperscript{155} Unlike the current identification device which is equipped with a simple magnetic strip, the proposed card contains a small silicon chip that is capable of storing large amounts of data.\textsuperscript{156} German federal and state data protection commissioners currently are carrying out a critical role by leading a public discussion concerning the kinds of health identification cards to be used in the German national health insurance program.\textsuperscript{157}

The data protection commission's second duty is to develop and monitor international agreements and foreign laws affecting data imports and exports. The data protection commissioners of the world now have substantial formal and informal contacts with one another.\textsuperscript{158} Indeed, as
we have seen, the commissioners of European nations have placed
significant pressure on the European Union that contributed to the
development of the Directive on Data Protection. The commissioners have
also engaged in important policy debates regarding data protection law's
international dimension. The United States' lack of any equivalent
agency handicaps its participation in this debate.

These first two roles contribute to the third task of the data
protection agency. Through its knowledge of technological developments
and oversight of international legal developments, this institution can be a
focal point for an ongoing national and international debate regarding the
application of information processing devices. In the United States, a
wide variety of administrative agencies have played a roughly analogous
role in other areas. These agencies have provided an important forum for
stimulating the kind of social discussions necessary in a deliberative
democracy.

Substantial divergence exists in the form and institutional power of
the world's data protection commissions. Such differences are not
surprising since each agency is an integral part of a different social,
political, and legal order. Yet, the most successful data protection agencies
are those most adept at seeking and maintaining the necessary national
and international discussions concerning the application of information
technology. These data protection commissions have engaged citizens,
businesses, and their governments in a shared effort to resolve difficult
issues about the promise and dangers of certain kinds of technology. They
have stimulated deliberation about information processing by all
potentially affected groups.

One striking example of data protection commissions playing such a
critical national role occurred in Germany during the early 1980s. This
incident also indicated the merits of federalism in data protection. At the
time, a law authorizing a national census, which passed the Parliament with
little debate, led to an unexpected storm of protest. Citizens objected

---

159. Priscilla M. Regan, The Globalization of Privacy: Implications of Recent Changes in
Europe, 52 Am. J. Econ. & Soc. 257, 263-65 (1993).
160. Id. at 265.
161. Evangelia Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes
162. For a general discussion of the role of administrative agencies in stimulating
deliberative democracy, see Mark Seidenfeld, A Civic Republican Justification for the
163. Mitrou, supra note 161, at 277.
164. For a discussion of the Census law, the protest against it in Germany, and the
decision of the Constitutional Court, see Paul M. Schwartz, The Computer in German and
American Constitutional Law: Towards an American Right of Informational Self-Determi-
RESTRICTIONS - INTERNATIONAL DATA FLOWS

to the intrusive nature of some of the questions and the comparisons planned between census information and the official inhabitant register, which is maintained in all German cities and villages.165 During the heated national reaction to the census, at a time when the Federal Data Protection Commissioner defended the census, state data protection commissioners not only raised their own voices in protest but expressed their criticisms in expert testimony before the German Constitutional Court.166 The Court struck down the most objectional parts of the census law.167 At the time of the next census, which occurred in 1987, the data protection commissioners, state and federal, played an important role in advising the parliament and structuring legal safeguards for the collected information.168

Data embargo orders should be understood within the context of the functions of data protection agencies. Because of their expert knowledge and their international role, these institutions have a unique ability to stimulate domestic and international discussion about the processing of personal information. Moreover, the potential severity of the data embargo order gives European data protection authorities a persuasive voice in these discussions. The agencies' ability to issue these orders means that they can be ignored only at great risk. Europe's data protection commissioners will have a part in setting the terms for the international discussion of global issues in data protection.

CONCLUSION

Considerable diversity exists in Europe in both the substantive standards for judging the permissibility of international data transfers and the process by which these judgments are made. This diversity suggests not only the difficulty of general judgments regarding the permissibility of planned data transfers from Europe, but also points to difficulties in an underlying task of the European Union: the harmonization of laws of the Member States.

This Article has shown that national laws in Europe already regulate transfers of personal data to third countries such as the United States. Most of these nations' data protection statutes permit transfers only when a third country has an equivalent level of data protection. On the Europe-wide level, the Council of Europe's Convention also sets out an equivalency standard. Under the European Union's Directive, which represents the most recent element in European law's response to international issues in data protection, international transfers of personal data to non-Member

---
165. Id.
166. Id. at 688.
167. 65 BVerfGE 1, 43 (1983).
168. See Schwartz, supra note 164, at 700.
Nations require only adequate protection in a third country. It is not yet clear, however, whether European domestic law may set a higher standard than the Directive's adequacy standard and continue to require equivalent protection.

Some observations regarding the nature of European evaluation of the adequacy or equivalency of foreign data protection are possible. The substantive task will not be to rate foreign law based on the overall extent of its equivalency or adequacy but, rather, to analyze the norms of a specific European nation with reference to a planned data transfer and the protection that will be available to the data in question. According to the Directive, this comparison is to "all the circumstances surrounding a data transfer operation." 169

As regards the process of regulating international transfers of personal information, European law has created the data embargo order. European countries adopt different approaches when issuing data embargo orders. In Germany, the government enjoys only a limited power to issue data embargo orders, and it confers that power on the "supervisory authority." 170 Danish and British law explicitly grant their respective data protection authorities the power to issue data embargo orders. The Netherlands assigns this power to the Minister of Justice. In the United Kingdom, the Netherlands, and France, authorities can issue data embargo orders to both public and private organizations. 171 In Denmark, authorities can extend data embargo orders only to information processing activities in the private sector. 172 Until now, agencies have made scant use of data embargo provisions. Yet, the power to issue data embargo orders insures that data protection agencies will participate significantly in the international debate regarding the application of information technology.

169. Directive, supra note 4, art. 25(2).
170. See supra notes 133-38 and accompanying text (discussing German law as it relates to the authority to issue data embargo orders).
171. See supra notes 129-32, 139-43, 145-49 and accompanying text (discussing the data protection laws of the United Kingdom, the Netherlands, and France, respectively, as they relate to the authority to issue data embargo orders).
172. See supra notes 125-28 and accompanying text (describing the power of Danish data protection authorities to block private, but not public, data transfers via data embargo orders).