ESSAY

False Alarm?

Henry H. Perritt, Jr.*
Margaret G. Stewart**

Privacy law in the United States has been unsettled by a directive from the European Commission requiring every Member Nation of the European Union to enact comprehensive privacy legislation regulating databases with information about individuals.[1] The Directive requires that national legislation in the European Union prohibit the exchange of data between European database operators and persons in other countries that do not have adequate data privacy protection.[2]

* Dean and Professor of Law, Illinois Institute of Technology, Chicago-Kent College of Law.

** Professor of Law, Illinois Institute of Technology, Chicago-Kent College of Law.

1. Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 32, 1995 O.J. (L 281) 31, 49 (requiring Member States to adopt legislation conforming to terms of Directive) [hereinafter European Privacy Directive].

2. *Id*. art. 25(1). "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." *Id*. art. 1(1). "Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful." *Id*. art. 5.

The Directive imposes duties with respect to data quality (article 6). The Directive allows processing of data only when (1) the data subject has unambiguously consented, (2) processing is necessary to protect vital interests of the data subject, (3) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority," or (4) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)." *Id.* art. 7.

The United States historically has not had comprehensive privacy law at the federal level. While federal law regulates federal government databases and imposes duties on credit reporting agencies, it leaves to the state most other areas of privacy. A few states have regulated insurance and healthcare databases, but none has enacted regulation as comprehensive as the European Directive.

A reality of the Information Superhighway is that computerized data, including data pertaining to individuals, flows freely across national boundaries. It is not uncommon for multinational enterprises to collect data in one country, store it, and manipulate it halfway around the world. In addition, modern mass marketing depends, to an increasing degree, on rich lodes of data about consumer interests and purchasing patterns. If an enterprise wants to succeed in global markets, it must have global information about consumer behavior. Typically, it buys that information from entities that collect it in particular geographic markets.

These aspects of electronic commerce are shaken by data privacy regulation that differs sharply from one part of the world to another. When one country or region is significantly more restrictive in its data privacy regulation, economic and technological pressures are strong for data-handling activities in other parts of the world to come into conformity with the most restrictive requirements. This practical tendency for uniform data

---

The Directive permits information to be given to the data subject (articles 10-11), and allows the data subject a right of access to data (article 12) and a right to object to certain data contents (articles 14-15). It obligates data "controllers" to assure confidentiality and security of processing (articles 16-17) and obligates them to notify the supervisory authority when engaging in processing outside blanket authorization obtained through registration (articles 18-21).

It establishes a Working Party on the Protection of Individuals (article 30) and a Committee (article 31) to assist Member States and the European Commission on harmonization and adaptation of the Directive.

The geographic scope of the Directive is specified as follows:

> Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

Id. art. 4(1).

policies means that privacy law in one part of the world tends to have *de facto* extraterritorial effect.

This Essay analyzes the extraterritorial effect of the European Data Privacy Directive. Drawing upon excellent work by Professors Peter Swire,[3] Joel Reidenberg,[4] and Paul Schwartz,[5] and upon the ongoing activities of the ABA Internet Jurisdiction Project,[6] it considers whether application of the European Data Privacy Directive to various kinds of conduct occurring on the Internet offends the customary international law of jurisdiction. Three kinds of jurisdiction are relevant to this inquiry:[7] jurisdiction to prescribe (to subject conduct to ones own rules), jurisdiction to adjudicate (what most American lawyers call "personal jurisdiction"), and jurisdiction to enforce (application of physical power by the judicial or executive branches of government to compel compliance with legislative or judicial pronouncements).

This Essay concludes that most likely applications of the European Privacy Directive do not offend the international law of jurisdiction as a formal matter. The Essay also concludes, however, that purely regional approaches to data privacy, exemplified by the European Directive, jeopardize

3. Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998).

4. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995); Joel Reidenberg et al., *The Privacy Debate: To What Extent Should Traditionally "Private" Communications Remain Private on the Internet?*, 5 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 329 (1995); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992); Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137 (1992).

5. Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997); Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995); Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295 (1995).

6. *See generally* Chicago-Kent College of Law at the Illinois Institute of Technology, *Transnational Issues in Cyberspace: A Project on the Law Relating to Jurisdiction* (visited Mar. 15, 1999) <http://www.kentlaw.edu/cyberlaw/index.html>. The ABA Internet Jurisdiction Project originated with the Cyberspace Law Committee of the Business Law Section of the American Bar Association (ABA) and now is co-sponsored by the Sections on International Law, Science and Technology, and Public Utilities. It is located at Chicago-Kent College of Law at the Illinois Institute of Technology. Co-author Stewart is the Reporter.

7. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (1987) (explaining the three aspects of jurisdiction) [hereinafter RESTATEMENT].

the aspirations of free trade as codified in the World Trade Organization Agreement (WTO Agreement). It also concludes that the practical pressure for harmonization should be dealt with through multilateral negotiations rather than through unilateral imposition of norms by one important trading region. Discussions between the European Union and the U.S. government on contract-based self-regulatory approaches in the United States creating safe harbors for transfer of data outside the European Union offer promising new approaches for such multilateral adjustment.

Support for these conclusions is built upon two basic scenarios. Consider first a U.S. corporation with offices in France, a Member State of the European Union. Employee databases in France with respect to French employees of the U.S. corporation would clearly be protected by the Privacy Directive and the law of France implementing that Directive. To transfer the data to the U.S. corporate headquarters, assuming the U.S. law does not provide what the European Union considers adequate privacy safeguards, would be to violate French law. Yet rational employment policy presumably dictates that all such data be centrally stored and available to the final policy-making organs of the corporation located in the United States. If France can assert both adjudicatory and prescriptive jurisdiction and enforce its judgment, the U.S. corporation has a strong incentive to pressure the federal government to bring U.S. law into harmony with that of the European Union, whether or not as a matter of policy either the corporation or Congress is in agreement with the European Directive.[8]

As a matter of its own acknowledged power over persons and things within its borders,[9] France certainly may exercise both adjudicatory and pre-

8. Of course, from the point of view of privacy advocates in the United States, this is no bad thing. When one government is unwilling to act, pressure placed upon it by another government can be most valuable. Thus, for example, much of current "cooperative federalism" law is the result of individual states' original unwillingness to act until forced to choose between the direct imposition of federal law and self-regulation in accordance with federal guidelines.

9. This fundamental principle of international law was the early foundation of U.S. adjudicatory jurisdiction and presumably retains its legitimacy. *See* Pennoyer v. Neff, 95 U.S. 714 (1877), *overruled in part by* Shaffer v. Heitner, 433 U.S. 186 (1977). *Shaffer v. Heitner* raised a due process difficulty with an assertion by Delaware of jurisdiction over intangible property located within the state by virtue of a unique Delaware law, but two justices at the time questioned the holding's application to jurisdiction based on the presence of real property in the forum seized at the commencement of the lawsuit. Since then, Justice Scalia in *Burnham v. Superior Court*, 495 U.S. 604 (1990), writing for himself and three others, approved a state's assertion of jurisdiction over a defendant who was personally served with process in the forum, based on the long and continuing assertion of jurisdiction throughout the United States on this basis. While he purported to distinguish *Shaffer*'s requirement of minimum contacts from the assumed lack of such contacts in *Burnham*, his jurisdictional justification works equally well for jurisdiction based on the seizure of real estate. In both instances, jurisdiction is supported by tradition, and in both

scriptive jurisdiction over offices and employees of the U.S. corporation in France. Their physical location also, of course, most likely moots any issue of enforceability. Employee data, therefore, may be kept from U.S. headquarters. Whether application of the law is wise, in light of the potential incentive it gives the corporation to relocate, is a separate issue.

This kind of French control simply does not constitute the feared "extraterritorial" application of another nation's law within the United States. To the contrary, it is the classic example of the law's territorial application. While international law places some restraints on what a nation-state may do within its own borders to those located there, this kind of social-economic legislation and its enforcement obviously does not constitute a violation of the norms of the international order.

Of course, France's assertion of prescriptive jurisdiction here has an effect in the United States, where the "other" party to the transaction (the corporate headquarters) is located. Such extraterritorial ramifications, however, do not convert the exercise of jurisdiction over the French office into an exercise of jurisdiction over the U.S. headquarters.[10] They are what Jack Goldsmith and others call "spillover effects."

If the corporate assets in France are insufficient to satisfy a judgment there against the corporation, a request by the plaintiff to a U.S. court to enforce the judgment against U.S. assets ought to be granted pursuant to the doctrine of comity. As noted, exercises of adjudicatory and prescriptive jurisdiction were in accordance with international and local law.

A potentially more interesting jurisdictional question arises in the second scenario. A Web-based enterprise located in the United States makes available its services to a citizen of a Member of the European Union. As that citizen uses the Web site, the U.S. enterprise collects data from and about the citizen, including information on what pages the citizen views. The U.S. enterprise combines the data with other data available about that individual and sells it to direct marketing enterprises as well as using it for its own marketing and product development purposes. The U.S. enterprise does not register with any European data protection authority; it does not seek permission from the user for combination and transfer and subsequent use of

instances the state has the physical power to enforce its judgment (by the sale of the property or the holding of the defendant from the time of service until the time any judgment against him is paid). Additionally, if a defendant owns real property in a state, he has a permanent connection to the state (and may well be a resident of the state) such that the state may exercise general jurisdiction over him. *See* Helicopteros Nacionales, S.A. v. Hall, 466 U.S. 408, 414-15 (1984).

10. *See, e.g.*, Cable & Wireless P.L.C. v. FCC, 166 F.3d 1224 (D.C. Cir. 1999) (upholding an FCC *Order* capping the fees U.S. telephone companies are permitted to pay foreign companies for the completion of international long-distance telephone service).

data from that user; and it does not limit transfers of its personal data in conformity with European national law or the European Data Privacy Directive.

This scenario presents jurisdictional problems depending on the answers to three questions: First, do the activities described violate European law? Second, if they do violate European law, is there anything that any European legal institution can do about it? In other words, need the American enterprise worry about compliance with European law? Third, if it does have cause for "worry," is that the result of spillover effects from European regulation of its own citizens, as in scenario one, or is it the result of a qualitatively different imposition of duties on the American actor?

The answer to the first question depends on whether the Web-based enterprise "makes use of equipment, automated or otherwise, situated on the territory of the said Member State."[11] Arguably, the computer belonging to the European citizen is, when the citizen is using the U.S.-based Web server, such "equipment" (English version of section 4(c)) or a "means" (French language version of section 4(c)) of the Web enterprise.[12] This conclusion would subject the Web enterprise to national laws of the Member State pursuant to the European Data Directive under article 4.

The answers to the second and third questions depend upon whether any of the remedies specified in articles 22 and 23 (judicial remedies and monetary compensation) meaningfully can be imposed on the U.S.-based enterprise. Whether they can depends on whether the enterprise has facilities in Europe as to which the remedies would be meaningful.[13] A large enterprise—one of Professor Swire's "elephants"—probably would have facilities or personnel in Europe, and it could be subjected to enforcement procedures of a criminal or civil money penalty sort, much as American facilities of foreign firms are potentially subject to contempt and other procedures to force their off-shore facilities to allow discovery under the U.S. Federal Rules of Civil Procedure.[14] If the enterprise is an elephant, scenario two approaches scenario one.

11. European Privacy Directive, *supra* note 1, art. 4(c).

12. *See* Swire, *supra* note 3, at 1009 & n.104 (discussing difference between English and French versions of "Directive"; French term "*des moyens*" ("any means") is broader).

13. The user's computers could be targeted by enforcement authorities, but that would be impracticable and actually would have relatively little effect on the U.S.-based enterprise.

14. *See* Société Nationale Industrielle Aérospatiale v. United States Dist. Ct., 482 U.S. 522, 539-43 (1987) (permitting U.S. court to compel production of documents located in a foreign country, under Federal Rules, even though it may violate foreign blocking statute); *In re* Air Crash Disaster Near Roselawn, Ind., 172 F.R.D. 295, 309 (N.D. Ill. 1997) (applying *Aérospatiele*'s three factors: (1) intrusiveness of discovery requests given facts of particular case, (2) sovereign interests involved, and (3) likelihood that resort to Hague

If, on the other hand, the U.S. enterprise is one of Professor Swire's "mice," a European nation's ability to control it depends upon the willingness of U.S. courts either to apply European law to decide liability in a case brought against the U.S. company in the United States or to enforce a European judgment against assets located in the United States.

In general, when confronting the parallel question of whether to apply U.S. law to activities that occurred abroad, U.S. courts focus on whether the activity causes effects in the United States.[15] However, in light of the obvious potential interest of other sovereigns, at least some courts, notwithstanding U.S. effects, balance the interests of each sovereign in regulating the conduct, and often conclude that U.S. law should not be applied.[16] If the same approach is used to determine the applicability of European privacy law,[17] resolution is debatable at best. United States actors acting in the United States are obviously subject to U.S. law. However, that does not foreclose the possibility that they are also subject to European law when their U.S. activities cause substantial, foreseeable, and intentional effects in Europe. The entire point of the Privacy Directive is to prevent the dissemination of personal information concerning European citizens, which is the precise mission of the U.S. enterprise. On the one hand, not to utilize European law would place those allegedly protected by it in a position much like the one that predated the Directive. On the other hand, U.S. policy favoring the free flow of information would be substantially hampered if European

Convention would be effective, and allowing discovery of documents located in foreign country pursuant to Federal Rules, although protected from disclosure under French administrative law).

15. United States v. Aluminum Co. of Am., 148 F.2d 416, 443 (2d Cir. 1945).

16. Lauritzen v. Larsen, 345 U.S. 571 (1953). *See also* Timberlane Lumber Co. v. Bank of Am., N.T. & S.A., 549 F.2d 597 (9th Cir. 1976). *But see* Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909, 948-49 (D.C. Cir. 1984). The *Laker* court argued that *Timberlane*'s balancing approach in part only repeats factors already considered in a classic prescriptive jurisdiction analysis (nationality, allegiance, and principal place of business of the parties, the ability of the court to enforce its judgment, and the substantiality, foreseeability, and intentional nature of U.S. effects) and in part refers to factors not within the judicial competence to evaluate (the degree to which the desirability of the regulation is generally accepted, the existence of justified expectations of the parties, and the importance of the regulation to the regulating state). A court could, however, assume the competing governmental interests were of equal theoretical value and determine the extent to which application of each law would foster or hinder each interest—an approach suggested a number of years ago. *See* Margaret G. Stewart, *Forum Non Conveniens: A Doctrine in Search of a Role*, 74 CAL. L. REV. 1259 (1986).

17. United States courts might be put in the position of deciding the applicability of European law in the theoretically possible, but unlikely, event of an action brought in the United States by a European government to enforce its law. Somewhat more likely is an action for damages brought in the United States by a European victim of a U.S. entity's data practices.

law applies. Furthermore, the harm caused to European citizens when information concerning them is in the hands of U.S. marketing concerns may, as a practical matter, be less than if the same information were available to European concerns with more direct access to them.[18]

Should the plaintiff in this situation proceed against the U.S. defendant in a European court and obtain a default judgment against it, enforcement of that judgment is dependent on a U.S. court's recognition of the judgment. Assuming it determines that application of European law is supported by the existence of effects felt there, the question of adjudicatory jurisdiction remains, when the European governments elect to proceed in their own tribunals rather than litigating in American courts. The U.S. defendant has not acted physically outside the United States, and the maintenance of a Web site that can be accessed from Europe alone does not establish the minimum contacts due process and international law required for personal jurisdiction.[19] Nevertheless, jurisdiction in *Calder v. Jones* was premised on out-of-state activities by the defendants intentionally aimed at a California plaintiff.[20] The claim there was defamation; the injury was to reputation and occurred in the plaintiff's home state. By analogy, the claim here, invasion of privacy, is, like defamation, an intentional tort; the injury to that privacy, like the injury to reputation, necessarily occurs where the plaintiff lives. At least in a state-state context, jurisdiction would appear to be properly asserted. The international context of the dispute, however, makes its assertion more burdensome and, the defendant could plausibly argue, unreasonable and, therefore, unconstitutional and/or violative of international law.[21]

Quite apart from litigating in U.S. or European courts against American firms, European governments could impose border controls that would preclude persons within their territory from interacting with U.S. or Internet enterprises that violate European privacy law. Such enforcement and application of local European law, both confined to the territory of the European state, probably would comply with traditional customary international law notions of adjudicatory, prescriptive, and enforcement jurisdiction,[22] because

18. European firms are more likely to target European citizens in their marketing activities than U.S. firms.

19. *See, e.g.*, IDS Life Ins. Co. v. SunAmerica, Inc., 958 F. Supp. 1258, 1268 (N.D. Ill. 1997), *aff'd in part, vacated in part*, 136 F.3d 537 (7th Cir. 1998).

20. *Calder*, 465 U.S. 783 (1984).

21. Asahi Metal Indus. Co., Ltd. v. Superior Ct., 480 U.S. 102 (1987). It should be noted, however, that in *Asahi* the claim against the foreign defendant had no relation to the defendant's allegedly purposeful act directed at the forum. *Id.*

22. RESTATEMENT, *supra* note 7, § 431.

> (1) A state may employ judicial or nonjudicial measures to induce or compel compliance or punish noncompliance with its laws or regulations, provided it has jurisdiction to prescribe in accordance with §§ 402 and 403.

only the local effects of extraterritorial conduct are being regulated and targeted for enforcement. As noted above, prohibiting an individual found within the state from interacting with a Web server located outside the state does not raise significant jurisdictional problems. A state is clearly competent to regulate the conduct of the person found within the state's boundaries.[23] This is no different in terms of international law from the United States prohibiting an American "person" from trading with the country subject to economic sanctions.[24] It is rather like imposing export or import con-

> (2) Enforcement measures must be reasonably related to the laws or regulations to which they are directed; punishment for noncompliance must be preceded by an appropriate determination of violation and must be proportional to the gravity of the violation.
>
> (3) A state may employ enforcement measures against a person located outside its territory
>
> (a) if the person is given notice of the claims or charges against him that is reasonable in the circumstances;
>
> (b) if the person is given an opportunity to be heard, ordinarily in advance of enforcement, whether in person or by counsel or other representative; and
>
> (c) when enforcement is through the courts, if the state has jurisdiction to adjudicate.

Id.

23. *Id.* § 402.

> Subject to § 403 [(prohibiting "unreasonable" exercise of jurisdiction)], a state has jurisdiction to prescribe law with respect to
>
> (1) (a) conduct that, wholly or in substantial part, takes place within its territory;
>
> (b) the status of persons, or interests in things, present within its territory;
>
> (c) conduct outside its territory that has or is intended to have substantial effect within its territory;
>
> (2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and
>
> (3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

Id.

24. *Id*. § 431 cmt. c. Nonjudicial enforcement measures include "denial of the right to engage in export or import transactions; removal from a list of persons eligible to bid on government contracts; suspension, revocation, or denial of a permit to engage in particular business activity; prohibition of the transfer of assets." *Id.* Even export controls must be reasonable, however. *See id.* cmt. d (contrasting presumably permissible export sanctions against country that reexported strategic items to prohibited country from presumably impermissible export sanctions against country for trading with third country, because United States lacks prescriptive jurisdiction over third country).

The Helms-Burton Act is the target of significant criticism that it violates international law. *Compare* Antroy A. Arreola, Comment, *Who's Isolating Whom?: Title III of the Helms-Burton Act and Compliance with International Law*, 20 HOUS. J. INT'L L. 353, 368 (1998) (mobilizing customary international law arguments in favor of legality but expressing doubt as to consistency with treaty obligations of the United States), *and* J. Brett Busby, Note, *Jurisdiction to Limit Third-Country Interaction with Sanctioned States: The Iran and Libya Sanctions and Helms-Burton Acts*, 36 COLUM. J. TRANSNAT'L L. 621, 636

trols in support of economic boycotts such as those mandated by the Helms-Burton Act,[25] restricting transfer of funds located in the United States to foreign creditors,[26] excluding foreign firms from regulated U.S. markets,[27] or compelling domestic litigants to allow discovery of materials located in foreign countries.[28]

Even if there is no violation of the customary international law of jurisdiction, one can ask whether such border controls violate the WTO Agreement[29] because they are tantamount to discrimination against trade in goods or services with foreign countries. Also, from a policy perspective, this kind of isolation, and its probable effect indirectly on extraterritorial

(1998) (finding no persuasive jurisdictional basis for Act). Implemented primarily through sanctions imposed on entry of exports and personnel from entities that trade in certain Cuban assets, the Act draws legitimacy from the United States' conceded power under international law to regulate its borders. On the other hand, this use of enforcement jurisdiction effectively extends American prescriptive jurisdiction over trade between Cuba and third countries. It is this indirect extension of prescriptive jurisdiction that attracts criticism. Enforcement of the EU Privacy Directive is on stronger ground; therefore, enforcement jurisdiction over the export of data is used not to regulate trade between the United States and third countries, but to regulate trade between the United States and the European countries using their enforcement jurisdiction. While the ultimate target is arguably domestic privacy policy in the United States there is the argument that it is the interest of European citizens that would be adversely affected by the exports. Under Helms-Burton, it is the interest of U.S. citizens whose property was expropriated by Cuba that is being protected, but the protection is one step removed by imposing penalties on intermediaries—those trading with Cuba.

25. *See generally* Bret A. Sumner, Comment, *Due Process and True Conflicts: The Constitutional Limits on Extraterritorial Federal Legislation and the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996*, 46 CATH. U. L. REV. 907, 912-13 (1997). This comment discusses the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996, Pub. L. No. 104-114, 110 Stat. 785 (codified at 22 U.S.C. §§ 6021-6091 (Supp. III 1997)), noting foreign country claims that it violates international law. Title I of Helms-Burton authorizes civil penalties for U.S. firms, U.S. nationals, and resident aliens that engage in financing transactions related to confiscated property in Cuba. *Id.* §§ 6032-6033. Title IV allows the State Department to deny U.S. visas to any person who traffics in expropriated property. *Id.* § 6091(a). Most people agree that these titles are well within the prescriptive jurisdiction of the United States. Title III, which authorizes lawsuits in U.S. courts against foreign entities that trade with Cuba, is the controversial portion of the statute. *See* Sumner, *supra* (analyzing Title III in detail, but not other titles).

26. RESTATEMENT, *supra* note 7, § 431 reporter's note 4 (citing United States v. First Nat'l City Bank, 379 U.S. 378 (1965)).

27. *Id.* § 431 reporter's note 5 (citing cases of exclusion from securities and commodities markets).

28. *See* Société Nationale Industrielle Aérospatiale v. United States Dist. Ct., 482 U.S. 522, 539-40 (1986).

29. *Cf.* WTO, *United States - Standards for Reformulated and Conventional Gasoline*, WT/DS2/AB/R 29 (Appellate Body Apr. 29, 1996) (visited Mar. 15, 1999) <http://www.wto.org/wto/ddf/ep/public.html>. United States environmental regulations that focused on imported gasoline violated the WTO Agreement.

conduct, may be inconsistent with an international legal system that seeks to limit states in their exercise of jurisdiction.[30]

Moreover, and probably of greater practical significance, such interruption of commerce imposes a higher and higher price on the state imposing the prohibitions as the stream of commerce interrupted becomes a proportionally greater share of the total commerce conducted by that state.

The Authors believe that the Internet's potential as a marketplace will cause Internet commerce to be a rapidly growing portion of world trade. Regulating Internet commerce according to traditional concepts of prescriptive, adjudicatory, and enforcement jurisdiction may present states of the world with the same kind of unpleasant choice as the states now comprising the European Union faced after the end of the Second World War. They were legally competent to keep their trade barriers high and their borders secure, but doing so threatened to erode their economic welfare because it interfered with natural trade patterns.

The Authors expect that jurisdictional issues such as those raised by application of the European Privacy Directive will put pressure on thinkers and policymakers to harmonize substantive legal rules and to develop legal institutions so that new kinds of trade, flowing through virtual electronic pipelines, are not corrupted. Just as ocean commerce gave rise to *Lex Mercatoria*, and the Industrial Revolution gave rise to the United States and eventually to the European Union; just as concepts of free trade gave rise to the WTO, so also will electronic commerce give rise to new international institutions seeking to harmonize privacy, consumer protection, defamatory and hate speech, money laundering, and gambling.[31]

The self-regulatory approach envisioned by the 1998 U.S. Department of Commerce policy statement[32] may represent such a new international institution. Its viability depends on it being backed up by effective enforcement under local law, and its being accepted by the European authorities as an adequately protective privacy regime.[33]

30. *Cf.* Timberlane Lumber Co. v. Bank of Am. Nat'l Trust & Sav. Ass'n, 749 F.2d 1378, 1383-86 (9th Cir. 1984) (declining extraterritorial application of U.S. antitrust law because of effect on sovereign prerogatives of Honduras). *See generally* Edieth Yvette Wu, *Evolutionary Trends in the United States Application of Extraterritorial Jurisdiction*, 10 TRANSNAT'L LAW. 1 (1997).

31. *See* NTIA, Dep't of Commerce, *Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy* (visited Mar. 15, 1999) <http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm>.

32. *See* International Trade Admin., Dep't of Commerce, *Safe Harbor Principles* (Nov. 4, 1998) (visited Mar. 15, 1999) <http://www.ita.doc.gov/ecom/menu.htm>.

33. European Commission, Directorate General XV, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (July 24, 1998); European Commission, Directorate General XV, *Judging Industry Self-*

Regulation: When Does It Make a Meaningful Contribution to the Level of Data Protection in a Third Country? (Jan. 14 1998); European Commission, Directorate General XV, *Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries* (Apr. 22, 1998). The preceding documents can be found at the PrivacyExchange.org Web site, <http://www.privacyexchange.org/> (visited Mar. 15, 1999).