**Brooklyn Journal of International Law**

Volume 26 | Issue 2 Article 9

12-1-2000

# State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate

Joshua S. Bauchner

# NOTES AND COMMENTS

## STATE SOVEREIGNTY AND THE GLOBALIZING EFFECTS OF THE INTERNET: A CASE STUDY OF THE PRIVACY DEBATE

### I. INTRODUCTION

The concept of sovereignty long has held center-stage in the field of international law. Nations define themselves by their territoriality and fight to protect their sovereign interests. Within this realm, the Internet has served as a unique globalizing force.[1] In doing so, it has broken down traditional, physical boundaries, and, by extension, dismissed, or at least substantially modified, traditional views of state sovereignty.[2] "Telepower in its various forms–telecommunications, electronic entertainment, computer and information services, robotics, artificial intelligence, and expert systems–is already reshaping the global economy, internationalizing labor, and shifting jobs in space, time, and concept. Some would argue it is rendering the nation state obsolete."[3] In the modern day, states can rare-

---

1. *See* Fred H. Cate, *Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States: The E.U. Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 441-442 (1995) [hereinafter Cate, *Data Protection Law*]. *See also* Fred H. Cate, *Symposium: Sovereignty and the Globalization of Intellectual Property: Introduction Sovereignty and the Globalization of Intellectual Property*, 6 IND. J. GLOBAL LEGAL STUD. 1 (1998).

2. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS 65 (1998) (Quoting Timothy C. May, signature file end quote for numerous listserve postings which states, "[n]ational borders aren't even speed bumps on the information superhighway."). *See* Fred H. Cate, *Symposium: The Globalization of Law, Politics, And Markets: Implications For Domestic Law Reform*, 1 IND. J. GLOBAL LEGAL STUD. 467 (1994) [hereinafter Cate, *The Globalization of Law*]; David R. Johnson and David Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

3. *See* Cate, *The Globalization of Law*, *supra* note 2, at 467 (quoting Joseph

ly act domestically without causing significant effects elsewhere. In an amplified example of this, nations attempting to regulate the Internet are faced with the realization that their regulations have global impact[4] and must confront the reality that their laws may have a direct and significant impact on other states. Clearly then, regulation of the Internet is often not limited by territorial borders, and, therefore, risks encroaching upon the sovereignty of other states.

The European Union[5] Data Protection Directive ["Directive"] is one example of Internet legislation that has direct and possibly severe consequences on third-party sovereign nations.[6] The Directive was passed on October 24, 1995[7] in an effort to protect E.U. citizens' fundamental right to privacy.[8] The Directive requires all Member States to implement national legislation to conform with its terms within three years of its passage.[9] While Member States are given a degree of latitude to determine the scope and nature of national law drafted to conform with the Directive,[10] certain essential components are required. Specifically, the Directive aims to achieve equivalency among Member States to ensure similar, if not uniform, data protection laws.[11] Furthermore, the Directive requires Member States to limit the transmission of data only to third

---

N. Pelton, *The Globalization of Universal Telecommunications Services, in* ANN. REV. OF THE INSTIT. FOR INFO. STUDIES, 141, 143 (1991)).

4. *See infra* examples at p. 8.

5. The European Union is comprised of fifteen Member States including: Austria, Belgium, Denmark, Germany, Greece, Finland, Italy, Ireland, Luxembourg, Portugal, Spain, Sweden, the Netherlands, and the United Kingdom.

6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data, O.J. (L 281) Nov. 23, 1995 [hereinafter Directive]. *See infra* Section II.A.

7. *See* Convention for the protection of individuals with regard to automatic processing of personal data, Jan. 28, 1981, Eur. T.S. No. 108 (1980) [hereinafter Convention]. *See also* SWIRE, *supra* note 2, at 47, stating, "the Directive is designed to protect fundamental human rights to privacy."

8. Directive, *supra* note 6.

9. A European Union *directive* requires implementing legislation on behalf of the Member States. In contrast, a European Union *regulation* directly governs the activities of Member States.

10. Directive, *supra* note 6, art. 5. *See infra* discussion in Section III.B.

11. For a good discussion of the equivalency of the data protection laws of the Member States, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 474-477 (1995) [hereinafter *European Data Protection Law*].

countries[12] who demonstrate adequate data protection.[13] While adequacy is not as strict as equivalency,[14] it nevertheless demands a certain level of acquiescence to European Union law by third-party countries if they are to continue those relations with Member States. As a result, the Directive, by requiring third countries to implement adequate data protection, has encroached upon the sovereignty of these nations.

This note will address the globalizing effects of the Internet as it relates to the sovereignty of states. The European Union Data Protection Directive will be analyzed as a case study to illustrate the effects of the Internet, and regulation thereof, upon state sovereignty. The first section briefly discusses the concept of sovereignty and its role in the international realm. Second, the European Union Data Protection Directive will be explained, specifically, those provisions which impact upon third countries. Third, the note will address how the Directive impacts upon the sovereignty of third countries. Fourth, relying on the case study, the concept of sovereignty as it applies to the Internet will be further extrapolated to illustrate the shortcomings of traditional governmental regimes. Ultimately, the note will conclude that conventional regulatory regimes will have to be reassessed as a result of the Internet's globalizing force if they are to conform with fundamental tenets of international law.

## II. SOVEREIGNTY AMONG NATIONS

### A. *Sovereign Rights*

Sovereignty is a fundamental principle of international law.[15] "The success of international law as a political and intellectual discipline over the past four centuries has had much

12. "Third countries," and "third-party countries," as referred to in this note, are not members of the European Union.

13. Directive, *supra* note 6, art. 25.

14. Schwartz, *European Data Protection Law, supra* note 11, at 473.

15. For example, the UN "is based on the principle of the sovereign equality of all its Members." Charter of the United Nations, art. 2. MARC W. JANIS, AN INTRODUCTION TO INTERNATIONAL LAW 6, 10 (1988) (Explaining, "[t]he special character of international legal process, like the special nature of international legal rules, is explicable in terms of state sovereignty . . . The idea is that states by virtue of their sovereignty may authoritatively regulate not only their own internal affairs, but also their international relations.").

to do with international law's utility in regulating and cementing a world political system based more or less on sovereign states."[16] "Under international law, a sovereign state is an entity that has defined territory and permanent population, under the control of its own government, and that engages in, or has the capacity to engage in, formal relations with other such entities."[17] Under certain circumstances states may choose to act to protect and defend their domain, beyond their defined physical boundaries.[18] This may result in an encroachment upon another state's sovereignty, and often, takes the form of war.[19]

In the field of international relations, states are treated as persons and interact with one another accordingly.[20] As such, an individual state has the right, "to defend its integrity and independence, to provide for its conservation and prosperity, and consequently to organize itself as it sees fit, to legislate upon its interests, administer its services, and to define the jurisdiction and competence of its courts."[21] The only limitation upon these rights is the "exercise of the rights of other states according to international law."[22] The scope of a state's

---

16. JANIS, *supra* note 15, at 123. MARC W. JANIS & JOHN E. NOYES, INTERNATIONAL LAW 27 (1997) ("By virtue of their sovereign status, states are entitled to an important number of international legal rights and are concomitantly obliged by international legal duties. Central among these is the right of any sovereign state to a status of international legal equality vís-a-vís other states.").

17. A.L.I. *Restatement (Third) of the Foreign Relations Law of the United States* § 201 (1985) [hereinafter *Restatement*]. *See also* Convention on Rights and Duties of States, art. 1, 49 Stat. 3097, T.S. No. 881, 3 Bevans 145, 165 L.N.T.S. 19; Montevideo Convention, December 26, 1933, entered into force December 26, 1934 [hereinafter Montevideo Convention]; Kadic v. Karadzic, 70 F.3d 232 (2d Cir. 1995) (for a discussion concerning the recognition and succession of states and governments). *See generally* JANIS, *supra* note 15.

18. *See* Montevideo Convention, *supra* note 17, at art. 3. *See also Cyberspace Regulation and the Discourse of State Sovereignty*, 112 Harv. L. Rev. 1680 (May 1999) [hereinafter *Cyberspace Regulation*] (Determining "an examination of the Internet regulatory debate reveals three positive conceptions of state sovereignty: the realist, the representational, and the postmodern." Specifically, it is the "realist" conception which focuses on territorial boundaries as delimiting sovereignty.).

19. HOBBES, LEVIATHAN (John Plamenatz ed., The Fontana Library 1967) (1651) (Arguing that without a "Common Power" humankind, living in a state of nature, would be forever in conflict, either at war or preparing for war. A state operates as a common power over its citizens, but, without a common power over the world's states, they act in conflict with one another in a constant state of war.).

20. *See* Montevideo Convention, *supra* note 17, at art. 2.

21. *Id.* at art. 3.

22. *Id. See* Hartford Fire Ins. Co. v. Cal., 509 U.S. 764 (1993) (Scalia, J.,

sovereignty is, therefore, limited and defined by the reaches of another state's sovereignty.[23] Importantly, however, "[n]o state has the right to intervene in the internal or external affairs of another."[24]

The result is a delicate balance wherein states must act to the extent of their sovereign power without crossing an indeterminate line into the sovereignty of another state.[25] Since one state's sovereignty, and its rights thereunder, is defined by the reaches of another state's sovereignty in relation to it,[26] only by acting to the peripheral limits of that power can a state maximize the scope of its sovereign rights. Conversely, a state also will act to protect the outer boundaries of its sover-

---

dissent):

> Under the Restatement, a nation having some 'basis' for jurisdiction to prescribe law should nonetheless refrain from exercising that jurisdiction 'with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable. . . . The 'reasonableness' inquiry turns on a number of factors, including, but not limited to: 'the extent to which the activity takes place within the territory [of the regulating state],' *id.*, § 403(2)(a); 'the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated,' *id.*, § 403(2)(b); 'the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which desirability of such regulation is generally accepted,' *id.*, § 403(2)(c); 'the extent to which another state may have an interest in regulating the activity,' *id.*, § 403(2)(g); and 'the likelihood of conflict with regulation by another state,' *id.*, § 403(2)(h).

(quoting *A.L.I. Restatement (Third) of the Foreign Relations Law of the United States* (1985)). As will be shown, none of these factors will be either 1) readily applicable to an inherently international medium or, if found to be applicable, 2) permit the conclusion that regulation by a single state is reasonable.

23. *See Restatement, supra* note 17, at § 201(h), 74 ("Whether an entity satisfies the requirements for statehood is ordinarily determined by other states when they decide whether to treat that entity as a state.").

24. Montevideo Convention, *supra* note 17, at art. 8. *See* 1 OPPENHEIM'S INTERNATIONAL LAW 295, and note 1 (H. Lauterpacht 8th ed. 1955) ("A State must not perform acts of sovereignty in the territory of another state.").

25. *See* Hartford Fire Ins. Co., 509 U.S. at 764 ("'[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains'. . . . It is relevant to determining the substantive reach of statutes because "the law of nations," or customary international law, includes limitations on a nation's exercise of its jurisdiction to prescribe." (quoting Murray v. Charming Betsy, 2 Cranch 64, 118 (1804)).

26. *See* JANIS, *supra* note 15.

eignty from encroachment by another state.[27] By doing so, a state can ensure the greatest breadth of sovereign rights.

Historically, states have attempted to clearly delineate their sovereign domain.[28] However, as explained above, sovereignty is conceptually defined[29] and not always congruent with a state's physical, territorial borders.[30] Adding to this uncertainty, a state's sovereignty interests in one area within the international arena may be more expansive than its interests in another; again preventing clearly defined parameters.[31] The Internet's global reach further clouds these considerations.

### *B. The "Effects Test"*

Efforts by states to regulate the Internet also must take into consideration a state's obligation under international law not to intervene in the internal affairs of another nation.[32] In the United States, states often rely upon the "effects test"[33] to

---

27. *See* Timberlane Lumber Co. v. Bank of Am., 549 F.2d 597 (9th Cir. 1976) (declaring "nations have sometimes resented and protested, as excessive intrusions into their own spheres, broad assertions of authority by American courts."). *See, e.g.,* U.S. v. Thomas, 74 F.3d 701 (6th Cir. 1996) (Providing an example of two U.S. states competing to maintain their sovereign interest in the enforcement of normative beliefs. Defendants, located in California, operated an electronic bulletin board service containing pornography. They were convicted under a Tennessee obscenity statute. On appeal, defendants contended that the trial court incorrectly applied a Memphis community standard to determine obscenity rather than a Californian standard, where the defendants were located, or, in the alternative, an Internet community standard.). *See also Cyberspace Regulation, supra* note 18.

28. *See, e.g.,* Hartford Fire Ins., 509 U.S. at 764 (defining "prescriptive comity" as "the respect sovereign nations afford each other by limiting the reach of their laws).

29. *See* Laker Airways v. Sabena, Belgian World Airlines, 731 F.2d 909, 937 (D.C.Cir. 1984) (defining comity as "a complex and elusive concept–the degree of deference that a domestic forum must pay to the act of a foreign government not otherwise binding on the forum").

30. Permitting, under the Restatement's reasonableness test, for example, instances where a state's laws may appropriately reach beyond its physical borders. *Restatement, supra* note 22. *See* U.S. v. Aluminum Co. of Am., 148 F.2d 221 (2d Cir. 1945).

31. *See* Laker Airways v. Sabena, Belgian World Airlines, 731 F.2d 909 (D.C. Cir. 1984) ("Since comity varies according to the factual circumstances surrounding each claim for its recognition, the absolute boundaries of the duties it imposes are uncertain.").

32. *See* Montevideo Convention, *supra* note 17, at art. 8. *See also* Hartford Ins. Co., 509 U.S. at 764.

33. Calder v. Jones, 465 U.S. 783 (1984) (establishing the "effects test" as a

determine the appropriateness of the application of their state's law upon Internet activity occurring in another state.[34] Simply, when a party's activity causes a result to occur in another state, that party may be subject to the laws and jurisdiction of that state.[35] The Internet's globalizing force uniquely results in an exponential increase in incidents requiring the application of such principles. In fact, all Internet users can, by virtue of their activity, find themselves subjected to the jurisdiction of a foreign government.[36]

By extension, the "effects test" also can be used to gauge the effects of a foreign state's laws upon another state;[37] as opposed to an entity's activity causing effects within a forum warranting jurisdiction. In this capacity, the "effects test" is used to determine infringements upon a state's sovereignty vís a vís another state's actions.[38] The Internet represents a heretofore unparalleled medium in which one state's regulatory efforts can influence the "internal affairs" of another. It is almost impossible for a state to regulate the Internet without

---

means of determining personal jurisdiction).

34. *See Cyberspace Regulation, supra* note 18.

35. *See* Bensusan Rest. Corp. v. King, 126 F.3d 25 (2d Cir. 1997); Panavision Int'l v. Toeppen, 938 F. Supp. 616 (CD Cal. 1996); NY CPLR § 302(a)(3). The section permits a court to exercise:

> personal jurisdiction over any non-domiciliary, or his executor or administrator, who in person or through an agent
>
> . . .
>
> 3. commits a tortious act without the state causing injury to person or property within the state
>
> . . .
>
> (ii) expects or should reasonably expect the act to have consequences in the state and derives substantial revenue from interstate or international commerce.

*Id.* However, courts have attached a foreseeability requirement holding that the defendant foresee, "the consequences generally and not to the specific event which produced injury within the state." Fantis Foods, Inc. v. Standard Imp. Co., 49 N.Y.2d 317 (1980).).

36. *See infra* discussion in Section IV.

37. *See* Aluminum Co. of Am., 148 F.2d at 228 (In which Hand, J. stated it is settled "that any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its border which the state reprehends.").

38. *See* Timberlane Lumber Co. v. Bank of Am., 549 F.2d 597 (9th Cir. 1976) (declaring "it is evident that at some point the interests of the United States are too weak and the foreign harmony incentive for restrain too strong to justify an extraterritorial assertion of jurisdiction.").

causing a rippling extraterritorial effect resulting in impact upon other states.

For example, a French law requires that all solicitations of French citizens be made in the French language.[39] Accordingly, all Web sites targeting French citizens for the sale of goods and services must be in French.[40] The law resulted in a suit brought by the French government against Georgia Tech Lorraine, a division of the Georgia Institute of Technology, because its educational site, targeting French citizens, was drafted only in English.[41] Similarly, prosecution by German officials for violation of a German anti-obscenity law forced CompuServe, a multinational online service provider, to block 250 allegedly obscene newsgroups from all of its users worldwide.[42] Germany also has caused (tidal) waves in response to Amazon.com's offering of fascist literature, in violation of German law, on its U.S. directed Web site.[43] While Amazon.com has a site specifically targeting German citizens, which does not offer such material, Germans nevertheless can access the U.S. Amazon site over the Internet; thereby circumventing Amazon.com's attempt at compliance and resulting in its criminal liability.[44]

### *C. The European Union and Sovereignty*

The Directive serves as a prime example of an Internet regulatory scheme that has a far reaching and significant impact beyond the borders of the regulating entity.[45] Interesting-

---

39. *See* Ian C. Ballon, *The Law of the Internet: Developing A Framework for Making New Law (Part II)*, Cyberspace Lawyer, 2 No. 10, CYBERSPACE LAW, 16, 1, January 1998.

40. *See* Ballon, *supra* note 39; Mark Owen, *International Ramifications of Doing Business Online: Europe*, 564 PLI/Pat 263, 285 (1999)

41. *See* Ballon, *supra* note 39; Owen, *supra* note 40, at 285.

42. *See* Ballon, *supra* note 39; Owen, *supra* note 40, at 285. Additionally, the former managing director of CompuServe Germany was sentenced to two years in prison because the court found that CompuServe's servers disseminated the obscene material. However, the sentence was suspended upon payment of a fine. *Id.* at 285.

43. *See Free Speech and Other Dilemmas for Web Retailers*, N.Y.L.J., Vol. 222, No. 39, August 24, 1999. The article quoted Michael S. Mensik, a partner at Baker & McKenzie, explaining that, "German courts generally don't care where you are, or how many clicks it takes to get to you. If you're providing illegal content to people in Germany, you're liable under German law."

44. *See id.*; Ballon, *supra* note 39.

45. *See infra* discussion in Section IV.

ly, the Directive is the result of an international union, rather than a single nation-state. However, the European Union acts in many ways like a sovereign state within the international arena.[46] While the history and dimensions of the E.U. are beyond the scope of this article, certain components of the Union's role within the international community are important to this discussion.

Arguably, the European Union is a sovereign entity in and unto itself.[47] "Member countries have agreed to pool some of their sovereign powers for the sake of unity, just as American states did to create a federal republic."[48] The E.U. is, therefore, the result of that "pool" and has the ability to exercise certain sovereign powers relinquished to it by the Member States.[49] "The Member States work together, in their collective interest, through the joint administration of their sovereign powers."[50] However, Member States also retain their own, individual sovereignty,[51] specifically in the areas of na-

---

46. *See* EUROPEAN UNION: A GUIDE FOR AMERICANS 3 (1998) [hereinafter E.U. GUIDE]; *Restatement, supra* note 17, at § 201, Reporter's Notes n.6, p.75 ("The creation of the European Community did not terminate the statehood of its constituent members, although the Community assumed international responsibility for a number of matters previously in the control of the individual states. The Community is not a state, but it has become party to some international agreements in its own right."). An example of this is the E.U.'s membership in the World Trade Organization singly, as well as by virtue of the membership of its Member States, again illustrating its quasi-sovereign status within the international arena. *About the WTO* (February 9, 1998), *at* http://www.wto.org/wto/about/organsn3.htm.

47. *See supra* note 46.

48. E.U. GUIDE, *supra* note 46, at 4, 6.

49. *Id.* at 4.

50. *Id.* at 6.

51. The concept of segmented sovereignty can be viewed as a paradox. For example, if a state relinquishes its sovereign power, it is no longer sovereign since it has surrendered a degree of control over itself, negating its sovereignty. Hobbes maintains sovereignty is absolute. Therefore, when an entity relinquishes any of its sovereignty to a higher power, it surrenders *all* of its sovereignty.

The E.U. attempts to circumvent this paradox though the principle of "subsidiarity" which permits it to act only in those matters, "that cannot be handled effectively at lower levels of government, i.e., national, regional, or local." E.U. GUIDE, *supra* note 46, at 7. In one of the first adjudicated cases to address this paradox, the British House of Lords held that the U.K. was a sovereign state within the E.U. However, the court also held that an Act of Parliament could be stayed by virtue of an injunction granted by the European Court of Justice. The House reasoned that the U.K. was merely consenting to the injunction, a choice only a sovereign entity could make, even though a foreign body was imposing itself upon the sovereign will of Parliament. This permitted Parliament to retain

tional security and defense, and criminal prosecution.[52]

The E.U.'s role in the international community was further solidified through passage of the Maastricht Treaty[53] which "made it constitutionally possible to achieve Economic and Monetary Union (EMU), and to develop the Union's inherent political dimension through the new Common Foreign and Security Policy,"[54] thus conforming with the principal determinant of a sovereign state - the establishment of a political will recognized by other states.[55] Furthermore, recent passage of the Amsterdam Treaty[56] represents an attempt by the E.U. to harmonize its foreign policy activity permitting it to act in foreign relations on behalf of the Member States.[57] The European Union is clearly positioning itself, if it has not done so already, to assume the rights and obligations of a sovereign state (in the form of a sovereign region) within the international community; particularly as it now chooses to interact with other sovereign states.[58] Accordingly, the E.U. is now in a position to assume the rights and obligations of an international actor.[59] It must adhere to principles of international law and must restrict its actions so as not to interfere in the internal affairs of third-party sovereign states.[60]

Within this capacity, U.S. representatives have been negotiating with E.U. representatives regarding the Directive, rather than the individual Member States.[61] This is particularly

---

its sovereignty while acquiescing to a foreign authority. Regina v. Sec'y of State for Transp., *ex parte* Factortame Ltd., [1991] 1 A.C. 603, [1989] 2 W.L.R. 998.

52. *See* E.U. GUIDE, *supra* note 46, at 4; Directive, *supra* note 6, art. 3, para 2, art. 13(1)(a)-(d); E.U. Commission Directorate General 15, *Data Protection: Background Information* (Nov. 3, 1998), *at* http://www.europa.eu.int/comm/dg15/en/media/dataprot/law/ [hereinafter *Background Information*]; Cate, *Data Protection Law*, *supra* note 1, at 434.

53. *See* TREATY ON EUROPEAN UNION, 1992 O.J. (C 224) (entered into force Nov. 1, 1993).

54. E.U. GUIDE, *supra* note 46, at 5.

55. *See supra* Section II.A.

56. Amsterdam Treaty, 1997 O.J. (C 340) (Nov. 10, 1997) [hereinafter Amsterdam Treaty].

57. *See id. See also* E.U. GUIDE, *supra* note 46, at 5.

58. *See* Amsterdam Treaty, *supra* note 56. *See also* E.U. GUIDE, *supra* note 46, at 5.

59. *See supra* Section II.A.

60. *See* Montevideo Convention, *supra* note 17, at art. 8. *See also supra* Section II.A.

61. *See* U.S. International Trade Administration Electronic Commerce Task Force, "Safe Harbor Principles," *at* http://www.ita.doc.gov/ecom/menu.htm (last visit-

interesting since it is the Member States that unilaterally implement national legislation in conformance with the Directive[62] and determine whether third countries evidence adequate data protection.[63] The Union's involvement is legislatively limited to instances wherein a conflict arises and the matter is appealed to the Commission.[64] The question then arises as to what extent the E.U. will be able to represent the individual Member States' varying, albeit harmonized, data protection policies.[65] Nevertheless, these negotiations have arisen out of concern for certain provisions of the Directive,[66] specifically, its requirement that Member States block data transmissions to third countries without adequate data protection.[67]

Beyond the provisions requiring the blocking of data,[68] the Directive also results in the imposition upon third countries of a de facto requirement to create new policies and implement new technologies to ensure adequacy.[69] The Directive's scope extends to "grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."[70] Accordingly, third countries will have to adopt additional

---

ed Nov. 15, 1999).

62. Directive, *supra* note 6, art. 4, para 1.

63. *Id.* art. 25, paras 1-3.

64. *See id.* art. 25, paras. 3-6.

65. *See infra* Section III.A. The E.U. representatives are members of the Article 29 Working Group which consists of national data protection commissioners.

66. *See* Cate, *supra* note 1, at 437-439. *See also* SWIRE, *supra* note 2, at 3; Owen, *supra* note 40, at 281; Henry H. Perritt, Jr. & Margaret G. Stewart, *False Alarm?*, 51 Fed. Comm. L.J. 811, 812 (1999).

67. Directive, *supra* note 6, art. 25.

68. *See id.*

69. *Id.* art. 15(1). This is further evidenced by European officials efforts, "to encourage the United States and other third countries to adopt comprehensive privacy legislation. By deemphasizing the use of [private] contracts and other [self-regulatory models], the Europeans can try to apply more pressure on other countries to adopt privacy-protection legislation." *See also* SWIRE, *supra* note 2, at 56; Cate, *Data Protection Law*, *supra* note 1, at 438 ("The European data protectors view the current situation as an excellent opportunity to put pressure on Canada and the United States for improved data protection.").

70. Directive, *supra* note 6, art. 15(1).

protections in order to adequately comply with the breadth of the Directive.[71] The reach of the Directive, therefore, extends beyond the territorial boundaries of the Union and causes significant, if not severe, effects in third-party sovereign states forcing their adherence to the will of a foreign authority.

## III. EUROPEAN UNION DATA PROTECTION DIRECTIVE

### *A. Directive Background*

The Directive does not mark Europe's first step at ensuring privacy protection for data. In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ["Convention"].[72] The purpose of the Convention was, "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."[73] The Directive clearly represents an extension upon the Convention particularized to the nuances of the Information Age.[74] Accordingly, the object of the Directive is to, "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[75]

The Directive requires Member States to enact legislation implementing its terms.[76] The harmonization[77] of Member

---

71. *See* Owen, *supra* note 40, at 283.

72. Convention, *supra* note 7.

73. *Id.* art. 1.

74. The Directive also represents a focused effort by the E.U. toward political unity. Whereas the Convention was intended to permit open markets within the E.U., the transition from the Convention to the Directive mirrors the E.U.'s own transition from a market focused community toward a political union. *See* Simitis, *From the Market to the Polis: The E.U. Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446-447; Cate, *Data Protection Law*, *supra* note 1, at 432.

75. Directive, *supra* note 6, art. 1, para. 1.

76. *Id.* art. 4, para. 1.

77. *See* Schwartz, *European Data Protection Law*, *supra* note 11, at 481 ("Harmonization is a technical term of European Community law that refers to formal attempts to increase the similarity of legal measures in Member Nations. 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.'") (quoting GEORGE A. BERMANN ET AL., CASES AND MATERI-

State laws will ensure equivalent data protection throughout the European Union.[78] The "person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data,"[79] the data controller, is responsible for compliance with domestic law, rather than the end user.[80] The data controller is governed by the laws of the Member State in which it is established.[81] "Establishment" means the data controller physically exists within the territory of a Member State[82] and "implies the effective and real exercise of activity through stable arrangements."[83] However, the Directive continues to afford protection even if the data controller is established in a third country.[84] In such a scenario, the "processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice."[85]

Specifically, the Directive imposes four obligations upon the data controller, and grants five rights to the data subject. To promote the principles of the Directive, the data controller must ensure the: 1) data quality; 2) technical security; 3) notification to the supervisory authority; and, 4) circumstances under which processing can be carried out.[86] Conversely, the data subject is entitled: 1) to the data of which they are the subject of processing; 2) to be informed that processing is tak

---

ALS ON EUROPEAN COMMUNITY LAW 430 (1993)).

78. Directive, *supra* note 6, at Preamble, para. 8; *Background Information, supra* note 52, *at* http://www.europa.eu.int/comm/dg15/en/media/dataprot/law/ (last visited Oct. 18, 2000).

79. Directive, *supra* note 6, art. 2(d).

80. *See id.* at Preamble, para 18.

81. *See id.* N.Y. L.J., Proposed Directive is an Important Step, vol. 222, no. 17, July 26, 1999, at col. 2. This also is known as the "country of origin" rule. *See also* Owen, *supra* note 40, at 270.

82. Directive, *supra* note 6, art. 3(1)(a).

83. *Id.* at art. 3(1)(a), Preamble, para 19. If a single controller is established in many states, "it must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities." *Id.*

84. *Id.* at art. 3(1)(c).

85. Directive, *supra* note 6, at Preamble, para 20 and art. 4.

86. *See id.* at Preamble, para. 25.

ing place; 3) to consult the data; 4) to request corrections; and, 5) to object to processing in certain circumstances.[87]

*B. Transfer of Data to Third Countries: The Adequacy Requirement*

Article 25 of the Directive requires third countries to establish an "adequate level of protection" for data to permit transfers from a Member State.

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, *the third country in question ensures an adequate level of protection.*[88]

Each Member State is responsible for determining, "in light of all the circumstances surrounding a data transfer operation,"[89] whether a third country has such protections. The Member States and the E.U. Commission are then to pool their knowledge regarding the protections afforded in third countries and, "shall take the measures necessary to prevent any transfer of data of the same type to the third country in question."[90] Consequently, "[t]he Directive establishes rules designed to ensure that data is only transferred to countries outside the E.U. when its continued protection is guaranteed or when certain exceptions apply."[91]

---

87. *See id.* at Preamble, para. 25 and art. 7(a)-(f).

88. *Id.* at art. 25, para. 1 (emphasis added.).

89. *Id.* at para 2.

90. *Id.*

91. *Background Information, supra* note 52. The exceptions include transfers: 1) with the data subject's consent; 2) relating to the performance of a contract involving the data subject; 3) relating to the performance of a contract in the interest of the data subject; 4) in furtherance of an important public interest; and, 5) from a register intended to provide such information to the public. Directive, *supra* note 6, at art. 26, paras. 1(a)-(f). *See* Greenleaf, *Global Protection of Privacy in Cyberspace, at* http://www2.austlii.edu.au/itlaw/articles/TaiwanSTLC-3.html (last visited Jan. 8, 2000). The Directive's outright prohibition against data transfers to certain states "is in stark contrast . . . to the two previous major international privacy instruments, the OECD privacy Guidelines and the Council of Europe privacy Convention . . . Neither of these agreements *require* their signatories to impose export restrictions on non-signatory countries, or on countries which do not provide an equivalent degree of protection." *Id.*

To allay concerns regarding a blacklist scenario, the E.U. has been careful to explicate that "[a] decision to block a transfer would only apply to other transfers of the same type, not to all transfers to the country concerned."[92] However, European countries have a history of preventing transfers of information both in and out of the Union,[93] making the threat of data blockages a genuine concern for third countries[94] who have not adhered to the E.U.'s adequacy requirement.[95] Furthermore, threats to third countries may lead to reverse blackouts wherein foreign countries choose not to conduct business within the E.U. for fear of sanction and civil liability.

In the European Union, privacy is considered a fundamental human right.[96] Therefore, the Directive seeks not only to protect E.U. citizens' privacy generally, but does so within the context of protecting a fundamental right requiring "protection of a high degree, which in the Union's language means the maximum possible."[97] The adequacy requirement is, therefore, quite demanding and extensive when applied to the limitless reaches of the Internet. "The duty to safeguard the fundamental rights of the Union's citizens does not end at the frontiers of the Union. On the contrary, the Union is no less bound to achieve a high degree of protection for all transborder flows of

---

92. *Background Information, supra* note 52 (Emphasis added.).

93. *See* discussion, *supra* at 17.

94. At present, the U.S., for example, does not have adequate data protection in accordance with the E.U.'s standards. *See* Tom S. Onyshko & Lesia A. Stangret, *Privacy and the Internet: Recent Developments in Canada, the U.S. and Europe*, 4 N.2 Cyberspace Law 2 (1999); Ballon, *supra* note 39. However, the recently agreed upon "Safe Harbor Principles" were developed to circumvent this problem. *See infra*, Section IV.B.3.

95. *See* Cate, *Data Protection Law*, *supra* note 1, at 439.

96. *See* Directive, *supra* note 6, at Preamble, paras. 1, 2 and art. 1, para. 1. Treaty on the European Union, Title I - Common Provisions - art. F, para. 2 ("The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms . . . and as they result from the Constitutional traditions common to Member States, as general principles of Community Law."); European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, para. 1, Nov. 4, 1950 [hereinafter Human Rights Convention] ("Everyone has the right to respect for his private and family life, his home and his correspondence."). *See also* The Universal Declaration of Human Rights, art. 12, G.A. Resolution 217A (III), U.N. Doc. A/810, at 71 (1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such attacks.").

97. Simitis, *supra* note 74, at 448.

data."[98]

Further, even in view of the effort toward harmonization,[99] states are nevertheless permitted to implement legislation affording greater protection than required by the Directive[100] or by other Members.[101] For example, France, a Member State, acted under domestic law to prohibit a "French subsidiary of an Italian parent company from transferring data to Italy [another Member State] because Italy did not have an omnibus data protection law" to ensure equivalency.[102] France also has "required that identifying information be removed from patient records before they could be transferred to Belgium, Switzerland and the United States."[103]

Since each Member State is responsible for determining a third country's adequacy, such unavoidable "disparities"[104] in regulation among Member States means the adequacy requirement could be raised to meet the highest bar established by any single Member State.[105] Potentially then, the degree of

---

98. *Id.*

99. In fact, contrary to the E.U.'s continued efforts toward economic and political unity, Member states continue to cling to their unique identities and resist assimilation into a European nation-state. *See, e.g.,* Marlise Simons, *In New Europe, a Lingual Hodgepodge: Old Tongues Are Flourishing in a Revival of Regional Cultures*, N.Y. TIMES, Oct. 17, 1999, at D2.

100. Directive, *supra* note 6, at art. 5 stating, "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."

Because some Member States have delayed complying with the Directive's three year time frame for implementation, the Commission placed nine Member States on notice urging conformance with the Directive and indicating individuals who suffer losses due to a State's failure to implement may seek compensation in the national courts. *Data protection: Commission decides to send reasoned opinions to nine Member States* (July 29, 1999), *at* http://europa.eu.int/comm/dg15/en/media/dataprot/news/99-592.htm [hereinafter *Commission decides*]. The Directive requires Member States to enact laws to provide for civil remedies against data controllers pursuant to article 24. *See* SWIRE, *supra* note 2.

101. *See* Cate, *The Globalization of Law, supra* note 2.

102. *See id.* at 483.

103. *Id.* at 483.

104. *Commission decides, supra* note 100. *See also* Simitis, *supra* note 74, at 464 ("Experience has shown that the primary interest of the Member States is not to achieve new, union-wide principles, but rather to preserve their own, familiar rules."); Schwartz, *European Data Protection Law, supra* note 11, at 473.

105. *See Commission decides, supra* note 100 ("The Directive also establishes rules to ensure that personal data is only transferred to countries outside the E.U. when its continued protection is guaranteed, so as to ensure that the *high standards of protection introduced by the Directive within the E.U. are not undermined.*") (emphasis added). *See also* Simitis, *supra* note 74, at 464; Schwartz, *Eu-*

protection sought is without limits and the corresponding adequacy requirement may be similarly expansive. As individual Member States demand greater protections, other Members will be forced to conform to ensure equivalency. Again, the bar is raised and the adequacy requirement made more stringent. Accordingly, individual Member States, in their heightened demand for greater protections, could impose greater obligations upon third countries, increasing the degree of interference into those countries' internal, sovereign affairs.

Discounting the disparities in regulation among E.U. Member States for a moment, similar disparities among different third countries also are likely to result in the establishment of the most restrictive regulatory scheme.[106] Political, economic and technological pressures, combined with a desire to achieve uniformity, suggest such regulations tend "to have a de facto extra-territorial effect,"[107] intruding upon the will of sovereign states. Ultimately, therefore, the Directive could result in a race to the top in which various states compete to ensure greater degrees of data protection, without regard for the ramifications of their actions upon foreign states, or for the resulting stifling of information flow.[108]

## IV. THE DIRECTIVE'S EFFECT ON THE SOVEREIGNTY OF THIRD COUNTRIES

### *A. The "Establishment" Provision*

As illustrated above,[109] the Directive's "establishment" provision[110] claims governance over data controllers pursuant to the national laws in the country in which they are physically located.[111] Additionally, the Directive also claims authority over data controllers in third countries who "make use of equipment"[112] in a Member State. For example, depending

---

*ropean Data Protection Law, supra* note 11, at 487 (Explaining that many Member States initially expressed concern that the Directive might lower their already high standards for data protection.).

106. *See* Perritt and Stewart, *supra* note 66, at 812-813.

107. *Id.*

108. *See infra* Section IV.B.

109. *See supra* Section III.A.

110. Directive, *supra* note 6, at Preamble, para. 18 and art. 4.

111. *Id.*

112. Directive, *supra* note 6, at art. 4(1)(c) ("Each Member State shall apply

upon interpretation, "a U.S. Web site 'makes use of equipment' in France or Germany when a user accesses the site from one of those countries."[113] This clause potentially extends the Directive's influence over any entity in any location. Accordingly, the Directive's regulatory reach into third countries is conceivably without limits.[114]

Application of the "effects test" exemplifies the degree to which the Directive may influence the internal affairs of sovereign nations.[115] The potential extraterritorial effect of the E.U.'s Directive is to halt data transfers[116] and promote or even require the implementation of data protection policies, legislation, and technologies within third countries.[117] The test, therefore, effectively illustrates the Directive's encroachment upon the sovereignty of third countries.[118]

Simply, the Internet is a global network.[119] By seeking to regulate an international medium,[120] the E.U. necessarily must unilaterally impose its will upon the medium as a whole–it cannot simply regulate that portion of the Internet which exists within its physical territory since data transfers do not recognize boundaries established in the bricks and mortar world.[121] Regardless of the blurred lines demarcating a state's sovereign interests,[122] the Directive's scope necessarily extends beyond the E.U.'s defined territorial boundaries.[123]

---

the national provisions it adopts pursuant to this Directive to the processing of personal data where: . . . 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 . . . ") (emphasis added).

113. *See* SWIRE, *supra* note 2, at 69.

114. Owen, *supra* note 40, at 283 ("The restriction may have a huge impact in circumstances where it is necessary to transfer any data to the U.S. and this of course includes any provision of personal data by an E.U. user via a U.S. Web site.").

115. *See supra* Section II.A.

116. Directive, *supra* note 6, at art. 35, para. 4.

117. *See* SWIRE, *supra* note 2, at 56.

118. *See* Timberlane Lumber Co. v. Bank of Am., 549 F.2d 597 (9th Cir. 1976); U.S. v. Aluminum Co. of Am., 148 F.2d 241 (2d Cir. 1945).

119. *See* Cate, *Data Protection Law, supra* note 1, at 441-442.

120. *See* Cate, *The Globalization of Law, supra* note 2, at 467-468.

121. *See* Cate, *Data Protection Law, supra* note 1, at 441. *See also* Cate, *The Globalization of Law, supra* note 2.

122. *See supra* Section II.A.

123. An enduring principle of American law dictates "that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territo-

Therefore, to ensure the maximum protection of privacy,[124] as warranted by what the E.U. perceives to be a fundamental right,[125] it must prescribe and enforce the Directive's protectionary measures wherever the Internet extends.

Does the European Union's sovereign interest similarly extend beyond its physical borders? As explained above,[126] pursuant to international law one, state's sovereign interest is defined by that of another state.[127] Therefore, the point at which a third country has exercised its own right to legislate within the privacy sphere represents the point at which the Directive must cease to control.[128] The problem is that at this rather penumbral barrier a polarized conflict of interests arises between various states.[129]

### *B. Privacy v. The Free Flow of Information*

#### 1. The Delicate Balance

At the heart of this issue is an attempted balance between individuals' privacy and the need to transmit data relating to individuals,[130] particularly in the Information Age.[131] As

---

rial jurisdiction of the United States." Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285 (1949); Hartford Fire Ins. Co., 509 U.S. at 764. In fact, Justice Holmes explained that a canon of statutory interpretation "would lead, in case of doubt, to a construction of any statute as intended to be confined in its operation and effect to the territorial limits over which the lawmaker has general and legitimate power. 'All legislation is *prima facie* territorial'." Am. Banana Co. v. United Fruit Co., 213 U.S. 347, 407 (1921) (citing Ex parte Blain, L. R. 12 Ch. Div. 522, 528). While Holmes' general proposition has been substantially limited, the territorial principle remains a viable determinant, among several, for a state's proper assertion of its jurisdiction. W.S. Kirkpatrick & Co. v. Envtl. Tectonics Corp. Int'l, 493 U.S. 400, 406-408 (1990).

124. *See supra* Section III.B.

125. *Id.*

126. *See supra* Section II.A.

127. *Id.*

128. *See, e.g.*, Timberlane Lumber Co. v. Bank of Am., 549 F.2d 597 (9th Cir. 1976).

129. This conflict also exists within the E.U. as various Member States individually seek to determine the level of protection necessary to achieve harmonization with the Directive. Member States define jurisdiction differently and how each interprets the extent of their data protection regulations likely will result in dissension. *See* Joel R. Reidenberg and Paul M. Schwartz, *Data Protection Law and On-Line Services: Regulatory Responses*, *at* http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.htm (last visited Jan. 8, 2000).

130. The OECD, which has been addressing the protection of privacy and

discussed, privacy is at best a fundamental right,[132] and perhaps, only slightly less so, a dominant concern of most industrialized societies.[133] On the Internet, the lack of privacy[134] has created unique interests among governments and private groups to obtain, transmit, sell and otherwise disseminate personal information.[135] "In fact, an entire industry has emerged to market a variety of software products designed to assist Web sites in collecting and analyzing visitor data and in serving targeted advertising."[136] Furthermore, the Internet's

---

transborder flows of data since at least 1980, also has recognized these competing principles in its efforts to "affirm the commitment to protect individual privacy in the increasingly networked environment, both to uphold human rights and to prevent interruptions in transborder data flows." Workshop on "Privacy Protection in a Global Networked Society" Feb. 1998, excerpted *at* http://www.oecd.org/dsti/sti/it/secur/act/privnote.htm (last visited Jan. 8, 2000) [hereinafter OECD Workshop].

Interestingly, the European Convention for the Protection of Human Rights and Fundamental Freedoms, which protects privacy, also affords protection to the sharing of information. Human Rights Convention, *supra* note 96, at art. 10, para 1, Rome, 4, Nov. 1950 ("Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."). Even the Universal Declaration of Human Rights, provides protection for both privacy and the dissemination of information. Article 19 states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and *to seek, receive and impart information and ideas through any media and regardless of frontiers.*" Universal Declaration of Human Rights, *supra* note 96, at art. 19 (emphasis added).

131. "The Internet has made it easier for anyone to collect personal information about others." SWIRE, *supra* note 2, at vii.

132. *See supra* Section III.B.

133. *Id.*

134. *See* Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission, June 1999, *at* http://www.msb.edu/faculty/culnanm/gippshome.htm (last visited Nov. 12, 1999) (determining that of the 361 Web sites surveyed, 93% collected user information); Privacy and the Top 100 Web Sites: Report to the Federal Trade Commission, June 1999, *at* http://www.msb.edu/faculty/culnanm/gippshome.htm (last visited Nov. 12, 1999) (determining that of the top 100 most frequently visited Web sites, 99% collect user information).

135. *See Little Brother*, Thomas L. Friedman, N.Y. TIMES, Sept. 26, 1999. "The architecture of cyberspace is highly influenced by commerce and government, 'both of which have an interest in knowing as much as they can about what people are doing and where . . . So it's not an accident that the emerging Internet architecture makes it easier to track people and collect private data, because tracking people is what governments like and collecting private data is what commerce likes.'" *Id.* (quoting Professor Lawrence Lessig).

136. SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS, FTC, July 1999, at 2, *at* http://www.ftc.gov (last visited on Nov. 12, 1999) [hereinafter

architecture has evolved around electronic commerce which serves as the bedrock of much Internet activity and represents the source of the attraction toward personal data.[137] Companies engaging in electronic commerce have a significant interest in personal data, and its transfer online.[138] "Transborder data flow has become indispensable to the very existence of transnational enterprise and to the currently flourishing global marketplace . . . Information is the lifeblood that sustains political, social, and business decisions."[139] Interestingly then, electronic commerce depends upon consumers who unfortunately approach the Internet with trepidation[140] from the harvesting of their personal data to further electronic commerce.[141]

The E.U. recognizes the need to achieve a balance between these competing interests, and strives, within the context of the Directive, to do so. As discussed above, the first objective of the Directive is to protect the fundamental right of privacy.[142] However, the second object of the Directive cautions that

---

FTC REPORT].

137. *See* Friedman, *supra* note 135; FTC REPORT, *supra* note 136 (citing a U.S. Dept. of Commerce report that online sales tripled from approximately $3 billion in 1997, to approximately $9 billion in 1998.).

138. *See id.* Cate, *Data Protection Law*, *supra* note 1, at 439 ("Although figures vary, information services and products are either the first or second largest sector of the U.S. economy, accounting for between ten and twelve percent of Gross Domestic Product" and representing "more then 4.5 million U.S. jobs."). *Note:* These figures are from 1994 and likely have dramatically increased since then. It is safe to presume that the importance and value of electronic commerce has experienced a corresponding increase.

139. Cate, *The Globalization of Law*, *supra* note 2, at 471-472 (quoting Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 Vand. L. Rev. 985, 989 (1991)).

140. *A Little Privacy Please*, BUS. WK., March 16, 1998, at 98.

141. *See* OECD Workshop, *supra* note 130, at 5. Privacy Protection in a Global Networked Society, OECD, Feb. 1998 ("[P]rivacy protection is one of the critical elements of consumer and user trust in the online environment and a sine quo non for the development of electronic commerce."). *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (1998) (Survey found 85% of Web sites collect personal data about consumers, 14% disclose their information collection practices, and 2% provide a privacy policy.).

For an interesting discussion on European efforts to protect consumer interests, see Samantha Mitchell, *Cross Border Disputes: To Sue or Not to Sue?*, CONSUMER POLICY REVIEWS, Vol. 9, Issue 3, May 1, 1999.

142. Directive, *supra* note 6, at art. 1, para. 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.*

"Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection" of personal privacy.[143] The question at hand is whether the European Union, in an attempt to effectuate such a delicate balance, is unilaterally imposing its own regulatory scheme upon sovereign nations, due to an innate inability to regulate the technology without such an encroachment.

### 2. The European Union's Response

The E.U. has recognized concerns expressed by third countries regarding its alleged intrusion upon their sovereignty.[144] In a response to these concerns, the E.U. has compiled a FAQ answering twelve questions solely regarding the Directive's adequacy requirement and its extraterritorial effect upon third countries.[145] The final question asks, "Why is the E.U. trying to impose its system on other countries? Is this not a case of 'extraterritoriality'?"[146] In response, the Union contends,

> There is no desire to "export" the E.U. system to other countries. There are clearly different ways of arriving at the same results, but we need to ensure that personal data of E.U. citizens transferred outside the E.U. is being processed with due respect for certain widely accepted principles, that citizens can enforce their rights and that they are entitled to redress if they suffer damage as a result of a breach of these principals. We are conscious of the need to avoid procedures for blocking data transfers which are exclusively unilateral. Non-E.U. countries concerned need to be informed and given the chance to express their views.[147]

Interestingly, the E.U. refers to "certain widely accepted prin-

---

143. Directive, *supra* note 6, at art. 1, para. 2. The Convention similarly highlights the E.U.'s historical recognition of this balancing effort, dating back to 1981. The Preamble states, "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in *particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data* undergoing automatic processing." Convention, *supra* note 7 (emphasis added).

144. *See* Owen, *supra* note 40, at 281.

145. *Background Information, supra* note 52. In this ten-page document, five pages address concerns regarding the E.U.'s limitations on the transfer of data to third countries.

146. *Id.*

147. *Id.*

ciples"[148] in support of the privacy right. Doubtless, however, these principles may not be as "widely accepted"[149] as the E.U. seems to indicate judging from the resulting controversy surrounding its protection of them.[150] Moreover, as detailed above,[151] another "widely accepted principle" prohibits interference in the internal affairs of a sovereign nation. Has the E.U. (unilaterally) determined that the right to privacy trumps this principle of international law?

Further, the E.U.'s willingness to give third countries the "chance to express their views"[152] may be limited to just that, an opportunity for expression without necessarily a willingness to compromise. For example, the Chair of the Council of Europe's Data Protection Experts Committee has stated:

> Contrary to most other documents and nearly for the first time in the history of the Community, the Commission in its draft said that the need for the Directive is based on the need to protect human rights within the Community. This is why, when we speak of data protection within the Union, we speak of the necessity to respect fundamental rights of the citizens. Therefore, data protection may be a subject on which you can have different answers to the various problems, but it is not a subject you can bargain about.[153]

Ostensibly, the E.U. recognizes the fine line the Directive treads and the difficulty, if not impossibility, of affording such protection on the Internet without interfering with in internal affairs of third countries. However, its concern for international law is apparently outweighed by its own sovereign interest in protecting its citizens' rights.

---

148. *Id.*

149. In the E.U.'s defense, similar privacy principles have, to a degree, been "widely accepted" in the form of the OECD's Privacy Policy, which has been "accepted" by numerous states. However, the mere acceptance of the policy is mitigated by the fact that far fewer states have actually acted pursuant to its recommendations. OECD Workshop, *supra* note 130.

150. *See* Cate, *Data Protection Law*, *supra* note 1. *See also infra* Section IV.B.3.

151. *See supra* Section II.

152. *Background Information*, *supra* note 52.

153. Cate, *Data Protection Law*, *supra* note 1, at 438 (emphasis added).

3. The European Union and the United States

The United States, for example, also has recognized the need to effectuate such a balance. The U.S. has acknowledged the need "to assure personal privacy in the networked environment if people are to feel comfortable doing business"[154] must be weighed against "fundamental and cherished principles like the First Amendment, which is an important hallmark of American democracy protect[ing] the free flow of information."[155] However, unlike the E.U., the U.S. has chosen to forgo a governmental regulatory scheme in favor of dependance upon private sector self-regulation.[156] Herein lies the genesis of dissension between the E.U. and U.S. approaches to this issue.[157] While the E.U. seeks proactive legislation, the U.S. is relying upon private industry to achieve this balance.[158] The

154. A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 10, *at* http://www.iitf.nist.gov/eleccomm/ecomm.htm (last visited Oct. 6, 1999) [hereinafter FRAMEWORK].

155. *Id.* The International Safe Harbor recommends that U.S. organizations voluntarily self-certify their adequacy in accordance with E.U./U.S. proposed privacy principles. While the negotiations were closed, agreement was difficult and delayed "because one or the other side is subject to legal constraints. This category includes, for example, several instances in which the [European] Commission's proposed changes conflicted with the First Amendment." *Cover Letter from Ambassador David L. Aaron to U.S. organizations requesting comments on the newly-posted draft documents - November 15, 1999, at* http://www.ita.doc.gov/ecom/aaronmemo1199.htm.

156. *See* FRAMEWORK, *supra* note 154, at 11; *Draft International Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce, at* http://www.ita.doc.gov/ecom/aaronmemo1199.htm (last visited on Nov. 15, 1999) ("While the United States and the European Union share the goal of enhancing privacy protection of their citizens, the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation."). *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 24-25 (1999) [hereinafter Schwartz, *Privacy and Democracy*].

157. *See Welcome to the Internet, The First Global Colony,* Steve Lohr, N.Y. TIMES, Jan. 9, 2000, at D5. *See generally supra* Section IV.B.1.

158. *See* Cate, *Data Protection Law*, *supra* note 1, at 438. The OECD has conducted workshops in an effort to harmonize government and self-regulatory approaches and achieve a degree of uniformity in online privacy protection methodologies. OECD Workshop, *supra* note 130.

The FTC issued a second report, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, FTC, May 2000, in which the Commission called for legislative action by a vote of 3-2. However, "[d]espite the publicity surrounding the FTC's new report, the 106th Congress is expected to do little, if anything, of substance regarding the issue before it adjourns for the November elections." *FTC Backs Its Online Privacy Report,* Keith Perine, THE STANDARD,

U.S. has recognized the potential for conflict, and has cautioned the private sector that if self-regulation does not work,[159] "the Administration will face increasing pressure to play a more direct role."[160] Accordingly, the U.S. has indicated it will continue discussions with the E.U. "to increase understanding about the U.S. approach to privacy and to assure that the criteria [the E.U. uses] for evaluating adequacy are sufficiently flexible to accommodate our approach."[161]

In the meantime, however, the governments have agreed upon "Safe Harbor Principles" to permit the free flow of data between the E.U. and U.S. without requiring U.S. entities to actually conform with the Directive's standard for protection.[162] The compromise upholds the United States' reliance

---

May 25, 2000, *at* http://www.thestandard.com/article/display/0,1151,15439,00.html. In fact, Forrester Research has predicted that Congress will pass "weak" legislation in 2001, and then drop the issue until 2005. *Id.*

159. *See* FTC REPORT, *supra* note 136. The report concluded that private sector self-regulation has "fallen far short of what is needed to protect consumers." *Id.* at iii. With the exception of very specific legislation, such as the Children's Online Privacy Act, 15 U.S.C.A. § 6501, the U.S. government has done little to protect privacy online. Even the courts have balked at affording such protections. *See* Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996). The court upheld the firing of an employee after she complained that the company refused to adhere to its promises of confidentiality in employee e-mail. The court held employees do not have a reasonable expectation of privacy in e-mail communications. *Id.*

160. FRAMEWORK, *supra* note 154, at 12. The United State's reliance upon industry self-regulation is likely politically motivated, as well as being based upon First Amendment ideals. Private industry has loudly championed a self-regulatory model and would obviously benefit from the opportunity to establish the protections–on behalf of consumers–to which it would have to adhere, without government intervention. The Administration's warning that it "will face increasing pressure to play a more direct role" is clearly a less-than-veiled incentive for industry to take appropriate measures. *See* FTC REPORT, *supra* note 136.

Not surprisingly, "American firms view the EU [D]irective as Draconian and unworkable, and object to the EU's ban on the export of data to countries with less-strict regulations because this threatens to erect a huge barrier to the transatlantic transmission of information." *Living in the global goldfish bowl*, THE ECONOMIST, Dec. 18, 1999, at 49. However, a holiday study by the Electronic Privacy Information Center ("EPIC"), of the 100 most popular online shopping sites determined that none met the "basic criteria for privacy protection" in conformance with fair information practices. The executive director of EPIC concluded that "self regulation has failed. 'We need legislation to enforce fair information practices.'" John Schwartz, *Internet Privacy Eroding Study Says*, WASH. POST, Dec. 17, 1999, at E4.

161. FRAMEWORK, *supra* note 154, at 12.

162. "Commerce Secretary William M. Daley Hails U.S.-EU "Safe Harbor" Privacy Arrangement," Commerce News, U.S. Dept. of Commerce (March 14, 2000), *at* http://www.ita.doc.gov/media/privacy314.html. Beyond privacy concerns, the compro-

upon self-regulation permitting companies to elect entrance into the harbor via self-certification.[163] After two-years of negotiations, the resulting Principles recognize the fundamental differences in the respective approaches to privacy protection.[164]

The European Union and the United States are each relying on their own unique approach to achieve the aforementioned balance.[165] With proactive regulation, however, the E.U.'s approach causes significant effects on third countries.[166] By contrast, a self-regulatory scheme within the private sector does not represent a unilateral effort by one entity, intentional or otherwise, to influence activity or dictate policy

---

mise serves to resolve significant economic and political dissonance as the Agreement protects $350 billion in E.U.-U.S. trade. *See European Union OKs 'Safe Harbor'*, Jason Spingarn-Koff, WIRED, May 31, 2000. However, consternation remains on both sides of the issue, and the Atlantic, as privacy advocates ridicule the pact as "toothless" and business interests claim it "in effect establishes a non-tariff trade barrier." *U.S., E.U. data privacy deal near*, CNET News, June 4, 2000, *at* http://news.cnet.com/news/0-1005-202-2016754.html; *U.S., EU Agree on Privacy Standard,* Robert O'Harrow Jr., WASH. POST, June 1, 2000, at E4.

163. SAFE HARBOR PRIVACY PRINCIPLES, issued by the U.S. Department of Commerce, *at* http://www.ita.doc.gov/td/ecom/USPrinciplesJune2000.htm (last visited June 24, 2000); *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles,"* adopted May 16, 2000, E.U. Media, Information Society and Data Protection, *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32en.htm (last visited June 25, 2000).

164. SAFE HARBOR PRIVACY PRINCIPLES, issued by the U.S. Department of Commerce, *at* http://www.ita.doc.gov/td/ecom/USPrinciplesJune2000.htm (last visited June 24, 2000). "While the United States and European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Community." *Id.*

165. The most apparent example of this difference is the E.U.'s treatment of privacy as a fundamental right, whereas the U.S. has no uniform privacy legislation. *See* Perritt and Stewart, *supra* note 66; *See also* N.Y. L.J., *supra* note 81, at 3 ("The U.S. does not have equivalent federal privacy statutes for privacy protection.").

In fact, in searching for a right to privacy within the U.S. Constitution, Justice Douglas was forced to look to the penumbras of certain amendments now made famous in his majority opinion in *Griswold v. Connecticut*, 381 U.S. 479 (1965), since no *prima facie* right was found to exist. The Court has proceeded to recognize a constitutional interest "in avoiding disclosures of personal matters" in *Whalen v. Roe*, 429 U.S. 589, 599 (1977), but that protection has never been tested against legislative action. Of course, such a Constitutional protection only would apply to the government's use of personal information, and not that of the private sector. *Compare with* Human Rights Convention, *supra* note 96, and the Treaty of the E.U. For a good discussion of the different regulatory approaches taken by the E.U. and the U.S., see SWIRE, *supra* note 2.

166. *See supra* Section II.A.

over another sovereign entity. The E.U. is recognizing and addressing a profound concern among the Internet community.[167] Perhaps due to its appreciation of privacy as a fundamental right,[168] and its greater willingness to rely on government regulation,[169] the E.U. has elected to take such a substantial step.

The appropriateness of its actions, however, is irrelevant within the context of this discussion. The salient point is that the E.U. is unable, due to the nature of the Internet, to act within its own sovereign interests without extraterritorial effect. Regardless of the European Union's motivations, there is no denying that the effect of the Directive transcends sovereign borders. By unilaterally establishing the standard for protection, the E.U. has unquestionably "intervene[d] in the internal or external affairs of"[170] third countries. These sovereign states must either comply with the will of a foreign power, or be effectively sanctioned via a blacklist.[171] Because the Internet transcends borders, the Directive, to be effective, must as well.

## V. SOVEREIGNTY AND THE INTERNET

### *A. Trouble Ahead, Trouble Behind*

What does the Internet do to traditional notions of sovereignty when states are faced with the unavoidable reality that most any regulation of the technology will necessarily impact upon other sovereign states in violation of international law?

---

167. *See A Little Privacy Please, supra* note 140. Poll found 78% of Internet users claim they "would use the Web more if privacy were guaranteed." *See also* Schwartz, *Privacy and Democracy, supra* note 156, at 1609 ("Indeed, information privacy concerns are the leading reason why individuals not on the Internet are choosing to stay off."); SWIRE, *supra* note 2, at 80.

"A study by the Center for Democracy and Technology found that less than 10 percent of all Web sites respected the O.E.C.D.'s privacy guidelines, which stipulate that people have the right to expect that any personal data they submit over the Internet will not be used without their consent, that they have a right to correct any errors and to assume the data will be protected from abuse." Friedman, *supra* note 135. *See also* Cate, *Data Protection Law, supra* note 1, at 441.

168. *See supra* Section II.B.

169. *See* SWIRE, *supra* note 2, at 159.

170. *See supra* Section I.

171. *See* Directive, *supra* note 6, at art. 25, para. 4.

The European Union is acting pursuant to its ideological beliefs and in a genuine effort to protect the interests of its citizenry.[172] However, by doing so, it affronts certain maxims of international law leading to conflict with other states.

New regulatory endeavors are on the horizon, akin to the Directive.[173] These include efforts to govern contract,[174] law enforcement and encryption,[175] digital signatures,[176] consumer protection and spamming,[177] and intellectual property.[178] These ventures are likely to result in dissension regarding their appropriateness, necessity, applicability and impact, as each attempts to harness the power of the Internet according to the regulating state's own self-interest.[179] There can be little doubt that other Internet regulatory efforts will have the same effect.[180] While in the instance of the Directive two basic principles are in conflict–the protection of privacy

172. Interestingly, however, the effectiveness of the Directive is quite questionable. The Economist commissioned a private investigator to retrieve information about the article's author, based in the U.K. Perhaps not surprisingly, the investigator easily obtained "protected" personal information, in contravention of U.K. privacy laws passed in accordance with the Directive. *Living in the global goldfish bowl*, THE ECONOMIST, Dec. 18, 1999, at 49.

173. *See* Owen, *supra* note 40.

174. *See* The European Commission's proposal for a Directive on certain legal aspects of electronic commerce in the on-line market, O.J. (C 139) (June 16, 1999); United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce, Dec. 16, 1996; Building Confidence in Electronic Commerce - a consultation document published by the U.K. Dept. of Trade and Industry. *See generally* David Mirchin, *Online Contracts*, 563 PLI/Pat 351 (1999); Owen, *supra* note 40, at 266 ("There is a growing realisation that there is little point in any one country (or even one trading block) announcing e-commerce legislation if this is not also extended to its major trading partners.").

175. *See* Fact Sheet on Cyberspace Electronic Security Act of 1999 ("CESA"), *at* http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/9/16/16.text.1 (last visited Jan. 8, 2000).

176. *See* The European Commission's proposal for a Directive on a Common Framework for Digital Signatures, O.J. (C 325) (Oct. 23, 1998).

177. *See* The European Distance Selling Directive, 97/7 O.J. 97/L144, May 20, 1997.

178. *See* The European Copyright Directive Proposal, O.J. 98/C/108/03; The European Trade Mark Directive, 89/104 O.J. 88 L/40, Dec. 21, 1998.

179. *See, e.g.*, Laker Airways, 731 F.2d at 937 ("No nation is under an unremitting obligation to enforce foreign interests which are fundamentally prejudicial to those of the domestic forum. Thus, from the earliest times, authorities have recognized that the obligation of comity expires when the strong public policies of the forum are vitiated by the foreign act.").

180. *See* Owen, *supra* note 40.

and the free flow of information[181]–other efforts may result in the promotion of numerous antagonistic ideals each advocated by a sovereign state interest. The resulting panoply of conflicting laws is not likely to further the technology's evolution or serve to benefit its users.

### *B. International Agreements*

In the future, Internet regulation may require international arrangements that transcend state borders and originate independent of traditional state governmental processes. These international conventions would be free from the tarnish of unilateral state action and would prevent acceding sovereign states from encroaching upon each other's sovereignty in violation of the principles of international law. States "must recognize that, because of the global characteristic of information and its centrality to the modern economy, their own self-interest lies in compatible legal regimes, workable international standards, and global cooperation."[182]

The mechanisms for the imposition for such international standards are varied. Some commentators suggest creating a distinct cyberlaw jurisdiction–separate from territorial spheres of law–based on established Internet rules and protocols.[183] These proponents argue that "by applying both the doctrine of comity and the idea of delegation to Cyberspace, a local sovereign is called upon to defer to self-regulatory judgments of a population partly, but not wholly, composed of its own subjects."[184] Others analogize the problems of regulating Cyberspace to those faced by sovereign states attempting to regulate the high seas, which, like the Internet, are located beyond a state's territorial reach[185] and are governed by in-

---

181. *See supra* Section IV.B.

182. Cate, *The Globalization of Law*, *supra* note 2, at 487.

183. *See* Johnson and Post, *supra* note 2. *See also* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, *at* http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration (last visited Oct. 23, 2000) (Proclaiming, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.").

184. Johnson and Post, *supra* note 2, at 1367.

185. *See* Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 103-104 (1996).

ternational convention.[186] Accordingly, they propose applying principles of admiralty law to control online activity.[187] Choice of law decisions would be made depending upon the type of interaction between the various parties.[188] A third methodology recommends "conditioning access [to the Internet] on consent to a governing legal regime . . . at the entry point of a cyberspace network."[189] By doing so, traditional, territorially based rules then could be readily applied.[190]

The imposition of one of these, or any other, governing regime first would require an international agreement to ensure acceding states universally conform to its application. A state's ability to regulate the Internet then would be dictated by the provisions of that agreement and conflicts of law would be resolved accordingly.[191]

### *C. Individual Self-Regulation and the Internet Community*

Another regulatory methodology could depend upon self-regulation. However, rather then relying upon traditional industry self-regulation, this model would rely upon individual self-regulation. The plurality of norms, ideas, customs, and politics within the Internet community itself escapes regulation by a single entity or acquiescence to a single jurisdiction. For example, at the heart of the European Union's Directive is a principled belief system stemming from a communal ideology regarding the protection of personal information.[192] The Internet represents an infinite number of ideologies and indi-

---

186. United Nations Convention on the Law of the Sea, Dec. 10, 1982, U.N. Doc. A/CONF.62.122.

187. *See* Burnstein, *supra* note 182, at 103-104.

188. *See id.* at 103-104. Specifically, three types of interaction are delineated: "(1) disputes involving parties in privity with each other who act in their cyberspatial capacities; (2) those involving two users not in privity but acting in their cyberspatial capacities; and, (3) those involving cyberspace with regard to the defendant, but not the plaintiff." *Id.* at 116.

189. Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1213-1217 (1998) (Concluding "that the governing law challenges presented by cyberspace are not significantly different from the ones presented by other transnational transactions.").

190. *See id.*

191. *See generally* Burnstein, *supra* note 182, at 103-104; Kai Schadbach, *The Benefits of Comparative Law: A Continental European View*, 16 B.U. INT'L L.J. 331 (1998).

192. *See supra* Section III.A.

viduals congregating around them. These individuals are also not delineated by geographic boundaries and are further removed from real space through their online activity.[193] Appropriately then, the enforcement of a single state's self-interested policies will inevitably run afoul of one or many within the Internet community.[194] Even negotiated international agreements necessarily would have to benefit certain ideals while forsaking others in an effort to achieve compromise and unity. The encroachment is no longer upon another state's sovereignty, but an infringement upon the sovereignty of the individual.

The sovereignty of the individual predates the sovereignty of nation-states,[195] which did not truly become an axiom of international law until the seventeenth century.[196] Perhaps the Internet represents, in some capacity, a return to a state of nature in which humans interact with each other out of their own self-interest[197] and out of the reach of a common governmental power.[198] However, even in the state of nature, norms develop.[199] Individuals seek to protect their own self-interest in relation to one another and a system of reciprocity evolves–communities develop.[200]

---

193. *See generally* Cate, *Data Protection Law*, *supra* note 1, at 441; Cate, *The Globalization of Law*, *supra* note 2.

194. *See supra* Section IV.B.3.

195. *See* JANIS, *supra* note 15, at ch. 6.

196. *Id.*

197. *See* HOBBES, *supra* note 19.

198. *See id. See also* Rousseau, Jean-Jacques, *Discourse on the Origin of Inequality* (1754) (trs. by Donald. A. Cress in BASIC POLITICAL WRITINGS OF JEAN-JACQUES ROUSSEAU 1987). Rousseau argued that the ills of the human condition result from the formation of society and that in the state of nature humans are free and happy "noble savages." In a famous passage Rousseau criticizes the civil society declaring, "[t]he first man who enclosed a plot of ground and thought of saying, 'This is mine,' and found others stupid enough to believe him, was the true founder of civil society." *Id.* at 60.

199. *See* J.S. MILL, UTILITARIANISM (1861). Mill's exegesis on the happiness principle argues that "the sole evidence it is possible to produce that anything is desirable is that people do actually desire it" and that, as a matter of fact, happiness is the one and only thing people desire.

For further exposition on norms supplementing (if not supplanting) public law on the Internet, see David G. Post & David R. Johnson, *Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998); Johnson and Post, *supra* note 2.

200. *See* MILL, ON LIBERTY (1848). Mill mitigates the happiness principle with the harm principle arguing that an individual's ability to act is limited at the point at which she causes harm to another. "In support of this principle, Mill cited the varied benefits of liberty in self-regarding actions. Such liberty, he argued,

The early stages of the Internet mirrored this condition.[201] Individuals acted not only for their own purposes, but also to develop and promote the technology.[202] The earliest uses of the Internet included the creation of online communities which established rules through consensus, trial and error.[203] These communities then provided support, guidance, instruction, information, and other collective benefits to their membership.[204]

Further, these online communities may, in fact, be better suited to enforce developed norms than governments are able to develop and enforce law. For example, an entity in one state who violates the laws of another may be easily spared the enforcing will of the regulating state if it is unable to force extradition or otherwise impose a sanction.[205] By contrast,

---

leads to the discovery of useful new truths and modes of life; confirms and strengthens the insights we already possess; *and promotes the happiness of each individual more surely than any enforced and uniform standard can.*" CLASSICS OF WESTERN PHILOSOPHY, 3RD ed. (Steven M. Cahn ed., Hackett Publishing Co., Inc. 1977) (emphasis added). *See also* Richard A. Epstein, *International News Service v. Associated Press: Custom and Law as Sources of Property in News*, 78 VA. L. REV. 85, 126 (1992) (Suggesting that norms should be enforced only when "there are repeat and reciprocal interactions between the same parties.").

201. *See* JOHN SEABROOK, DEEPER: ADVENTURES ON THE NET (1997); HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY, *at* http://www.rheingold.com/vc/book/ (last visited Nov. 17, 1999).

202. *See* SEABROOK, *supra* note 198; RHEINGOLD, *supra* note 198.

203. *See* SEABROOK, *supra* note 198. An example of one of the first online communities is The WELL, a Bay Area based network which early on developed its own rules and protocols for membership and use. Seabrook explains that "[t]he basic idea was that by providing citizens with the technology to do more things for themselves . . . you could free people from their dependence on mass consumer products and corporate marketing, which were the windows through which the soul leaked out of modern man." *Id.* at 147-148.

204. *See* RHEINGOLD, *supra* note 198. In fact, Internet communities have since become the subject of college lectures, *Internet Communities*, *at* http://www.westga.edu/~dboldt/BUSA1900/F/TopicF.html (last visited Nov. 17, 1999); and *Building Communities on the Internet*, *at* http://www.syslab.ceu.hu/~i-netcl/(last visited Nov. 17, 1999), and generated the creation of Web newsletters, *Community Report*, *at* http://www.OnlineCommunityReport.com (last visited Nov. 17, 1999).

205. *See Legislation threatens European e-commerce: Irish companies hoping to trade online to the world may face complex legal battles if new EU draft legislation comes into play*, John Kennedy, BUS. & FIN. WORLD REPT., Sept. 23, 1999 (Criticizing new, proposed legislation which would permit a lawsuit to be filed in the jurisdiction in which the buyer of sales and goods is located. "The prospect of having to defend cases in a foreign court could deter some businesses from making the most of e-commerce . . . [The E.U.] has to let the market decide. It would be impossible to investigate every single item sold on the Internet.").

the Internet's history is replete with instances wherein members of the online community acted to enforce community norms by punishing or "flaming" violators.[206]

Norms need not supplant current law governing Internet activity which similarly takes place offline.[207] The concern is for new law, crafted specifically to control the Internet, which threatens to encroach upon its continued evolution and violate established norms which have well served to govern those areas law does not control. Norms do not risk encroachment upon state sovereignty and serve to promote the communitarian nature of the Internet. In short, norms should govern where the law cannot.[208]

Therefore, while the principle of sovereignty as currently existent within the international legal regime is inapplicable to cyberspace due to competing ideologies advanced by singular, self-interested states, it nevertheless remains intact in its truer, original form, empowering the individual.[209] Norms and rules will evolve pursuant to the needs of the individuals

---

206. For example, spamming, or the sending of bulk, unsolicited e-mail, has long engaged the wrath of members of the Internet community. In response, members have united to boycott spammers, *BlackMail, at* http://www.bitgate.com/spam (last visited on Nov. 17, 1999), and educate each other concerning the threat of spam, how to avoid it, and fight back, *Fight Spam on the Internet!, at* http://www.spam.abuse.net/spam (last visited Nov. 17, 1999). Perhaps the most comprehensive source to combat spam is a twelve part C-NET story instructing users on all aspects of avoiding and combating spam. *Can anyone stop SPAM?, at* http://www.cnet.com/Content/Features/Howto/Stop/ssola.html (last visited Oct. 23, 2000). All are freely available and signify a communal effort to protect a norm and punish transgressors.

207. *See* Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998)("[T]here are three possible types of actors who might enforce Internet norms: self-appointed private individuals who determine the norms and enforce them, usually by excluding offenders from the Net altogether; judges deferring to norms in the particular cases in which the issues arise; or the architecture of the Internet itself, which might simply make certain types of conduct impossible."). *Id.* at 1292.

208. *See also* Richard A. Epstein, supra note 200, at 126. Epstein suggests that "decentralized customs may be generated without legal interference and control, but legal force may be necessary to maintain them against systematic defection." *Id.*

209. Howe, *Supreme Court, 1952 Term–Foreward: Political Theory and the Nature of Liberty*, HARV. L. REV. 91, (1953). "[G]overnment must recognize that it is not the sole possessor of sovereignty, and that private groups within the community are entitled to lead their own free lives and exercise within the area of their competence an authority so effective as to justify labeling it a sovereign authority." *Id.*

comprising the Internet community[210] distinct from any interference from real space governmental mechanisms which cannot translate to effectively control certain aspects of a non-territorially based technology.[211]

## VI. CONCLUSION

This note illustrates the failure of governments in their effort to regulate the Internet, specifically due to an adherence to conventional regulatory paradigms. The principles of real space do not always translate to cyberspace. The inherent degree to which states infringe upon other state's sovereignty in attempting to regulate the Internet, in violation of international law, is highlighted by the European Union's Directive. Accordingly, future regulatory efforts, in order to conform with the principles of international law and prevent conflicts among states, should depend upon international agreements or rely upon individual self-regulation toward the continued evolution of the Internet community.

*Joshua S. Bauchner*[*]

---

210. The sense of "community" on the Internet is quite strong. Historically, individuals have been willing to sacrifice their sovereignty for the benefit of community membership. The community then provides a degree of security and identity to the individual, perhaps unattainable alone in the state of nature. For example, in the *Crito*, Socrates refused to forsake the community of Athens, even to escape his own death. Socrates realized that part of his identity was shaped by Athens and he was no longer only a separate individual, but also, and more importantly, part of something larger.

Similarly, members of the Internet community have conformed to certain community ideals and now represent themselves accordingly. Encroachment upon that community, as much as an encroachment upon their individuality, is met with significant resistance. *See* SEABROOK, *supra* note 201; RHEINGOLD, *supra* note 198.

211. *See supra* Section IV.

* The author would like to thank Prof. Timothy Griffin, Prof. Paul Schwartz, Prof. James Maxeiner, and Rekha Ramani for their thoughtful comments throughout the writing process. The Note is dedicated to his parents.