(Work still in progress. Please, do not quote or circulate)

INTERNET REGULATION AND THE ROLE OF INTERNATIONAL LAW

Antonio Segura-Serrano

1. INTRODUCTION

Given the "virtual" nature of its existence, the first important legal discussion about the Internet focused on its natural resistance to regulation. Despite this supposed resistance, national laws have been erected throughout the world with the aim and effect of subjecting the Internet to "real" regulation. Considering the global character of the Internet, however, International Law should be a more suitable tool for regulation. This paper, therefore, aims to study the current and future roles of International Law regarding the regulation of the Internet.

In the first part of this paper, we shall see the current role of International Law with respect to the regulation of the Internet. That exercise will allow us to identify the main different national approaches to Internet regulation, as well as the existing International Law instruments stemming from those approaches. There is an array of questions related to this new technology that national laws have addressed in various forms. I would like to focus only on some substantial issues, such as freedom of speech and the fight against harmful content; intellectual property and the promotion of public domain information; and privacy rights and the protection of personal data *vis-à-vis* the commercial use of collected data. Although there are other possible questions to be discussed (education, cybersecurity, taxation, electronic commerce ad contracts, etc.), these issues will give the measure of the differences between national laws, and will reveal the present role of International Law with respect to the Internet.

In the second part of this paper, we shall consider some traditional International Law questions or issues relating to the Internet that have not attracted enough attention until now. First, it seems clear that the integrity of Internet facilities is a matter of national security for any country. As such, we shall determine whether a cyber-attack, in the form of a virus or otherwise, may be considered an armed attack; and if so, whether such an attack may legally trigger a nation's legitimate self-defense response, or even the collective action of the United Nations ("the UN"). Second, because the Internet is important not only for each and every country in the world, but also because it is so crucial for the well-being of people in developed and developing countries alike, it seems fair to ask about the future governing of the Internet. In this regard, International Law may add to the discussion by introducing a very interesting concept, the concept of the "common heritage of mankind". This concept may be useful in answering questions such as who rules the Internet, or who is entitled to appropriate the Internet, and how should the Internet be governed. Third, we will consider whether access to the Internet may be regarded as a human right. It is clear that freedom of expression is a human right. Access to the Internet means much more in that respect than, say, access to telephone lines and handsets. Nevertheless, some steps have been taken in order to outline what could be described as a right to "universal access", which may include a right to Internet access.

To this end, the World Summit on the Information Society held in Geneva in 2003 and sponsored by the UN and the International Telecommunication Union ("the ITU")[1] will also be taken into account as the most recent international effort to bring together all issues connected with the Internet and to establish the principles on which democracy can be introduced in this area.

2. REGULABILITY OF THE INTERNET

From the inception of the Internet, there has been a debate that may be labeled regulation v. deregulation regarding this new field of activity.[2] Is it possible and feasible to regulate the Internet, or to the contrary, is the Internet an essentially free place?

The libertarian position was embraced by a few academics, especially in the U.S., during the nineties as the Internet was spreading from small communities to larger population layers. According to the libertarians, the Internet cannot and should not be regulated.[3] Cyberspace sovereignty is the core idea in seminal writings like those of Johnson and Post.[4] In their view, not only is it impossible or futile for the State to regulate the Internet, but it is also desirable for the Net to be free of State regulation.[5] In addition, the State faces legitimacy problems in its efforts to govern activities happening on the Internet;[6] whereas, cyberspace self-governance would more fully realize liberal democratic ideas.[7] A further analysis would require us to establish a difference between the extremist cyber-separatists and those who merely advocate for self-regulation as the appropriate way to handle cyberspace. In any case, libertarians intend to create a space for "netizens"[8] (Net citizens) which would be free from traditional nation-state rules.

The arguments used by these cyber-separatists are numerous, covering a wide range of issues. On the descriptive side, libertarians maintain that, as there are no borders in cyberspace (an intrinsically global

---

[1] *See* Declaration of Principles, Building the Information Society: a Global Challenge in the New Millenium, World Summit on the Information Society, Geneva 2003-Tunis 2005, December 12, 2003, at 1, Doc. WSIS-03/GENEVA/DOC/4-E, whose item number 1 states "the common desire and commitment to build a people-centred, inclusive and development-oriented Information Society".

[2] *See* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contractin*g for Governance in Cyberspace, 6 Cornell J.L. & Pub. Pol'y 475, 499 (1997) (stating that "[T]he regulation of cyberspace may take one of three forms. Cyberia will be government regulated, self-regulated, or even unregulated.").

[3] It has become common place to quote as a leading proponent of cyberspace independency to JOHN PERRY BARLOW, A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE, *at* http://www.eff.org/~barlow/Declaration-Final.html (last visited Sep. 9, 2005); *See also* John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207, 208 (1997) (emphasizing that the arguments for complete non-regulation are compelling).

[4] *See* David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, *at* http://www.wm.edu/law/publications/jol/articles/post.shtml [hereinafter Post, *Anarchy, State*] (last visited Sep. 9, 2005). *See also* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, U. PITT. L. REV. 993 (1994) (promoting the use of norms of "self-regulation", including mechanisms like self-help, contracts, private associations and custom); Henry H. Perritt, Jr., *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?*, BERKELEY TECH. L.J., 413, 419 (1997) (stating that "self-governance is desirable for electronic communities").

[5] *See* Johnson & Post, *supra* note 4, at 1391-95 and 1370-76, respectively.

[6] *See* Aron Mefford, *Lex Informatica: Foundations of Law on the Internet*, 5 IND. J. GLOBAL LEGAL STUD. 211, 217 (1997).

[7] *See* David G. Post, *Governing Cyberspace*, WAYNE L. REV. 155, 170-171 (1996); David G. Post, *The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD., 521, 535-42 (1998). *But see* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 488 (2000) (contending that the liberal state would likely be a more effective guarantor of liberal rights).

[8] *See* David R Jonhson & David G. Post, *The New "Civic Virtue" of the Internet*, 11 *at* http://www.cli.org/paper4.htm (last visited Sep. 9, 2005).

phenomenon),[9] any efforts made by territorially based sovereigns to regulate it will be unsuccessful.[10] On the other hand, if the Net is everywhere and nowhere in particular, in other words, if it is "a-jurisdictional,"[11] then no sovereign state has a more compelling claim than any other to subject these events exclusively to its laws.[12] They argue, then, that it would be unjustifiable to subject acts abroad to domestic regulation,[13] because it would unfairly disturb individual activities in other jurisdictions and unacceptably affect regulatory choices of other nations in this field.[14] Surprisingly, cyberspace may reproduce those very boundaries[15] (called electronic boundaries) of the physical world that it was meant to abolish, though that result would supposedly correspond to a better way of organizing Internet governance.[16] The libertarian discourse maintains that there is also a problem of notice within such a system, due to the fact that cyberspace users would be unable to know before hand when and what jurisdiction they could be facing when navigating over the Net.[17]

In their view, the alternative to state-based governance is self-governance.[18] Building on the idea of "delegation", they say that informal rules, called Netiquette (Internet etiquette), developed over time by cyberspace participants,[19] and rules designed and accepted by businessmen (a kind of new Lex Mercatoria),[20] would more appropriately fit the needs of this new community. Governance of cyberspace must be construed not on the basis of remote, unaffected national legislators, but by cyberspace users themselves, "netizens", who are the true and legitimate constituents of this new societal space.[21] This kind of discourse is to some extent rooted in specific population layers, and is akin to the ideological trends of today's politics, particularly in the U.S.[22]

One of the most intricate problems posed by self-regulation is how far such regulation is to go. Even accepting the libertarian premise that self-rule is good for cyberspace, would that mean that every regulatory area related to the Internet would be left to self-regulation? Would the entire Net community be

---

[9] *See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 915 (1996) [hereinafter Reidenberg, *Governing Networks*] (underscoring that the Internet provokes the disintegration of territorial borders and undermines substantive legal sovereignty).

[10] They also suggest that, regarding enforcement, States may be unable to make cyber users abide by their laws, as they may very well be out of the State's reach and control, *see* Perrit, *supra* note 4, at 423; Mefford, *supra* note 6, at 214.

[11] *See* Post, *Anarchy, State*, *supra* note 4, *at* par. 36.

[12] This argument is also based on the idea of "comity" in International Relations, *see* Johnson & Post, *supra* note 4, at 1376 and 1391.

[13] *Cf.* Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1129-1131 (1996) (describing competitive federalism, he recalls how states may not attempt to "export" their local laws into another jurisdiction).

[14] *See* Johnson & Post, *supra* note 8, at 4-5; Burk, *supra* note 13, at 1129-1134.

[15] *Cf.* Reidenberg, *Governing Networks*, *supra* note 9, at 917 (speaking of visible network borders).

[16] *See* Johnson & Post, *supra* note 4, at1395; Johnson & Post, *supra* note 8, at 11.

[17] *See* Johnson & Post, *supra* note 4, at 1379 and accompanying note n. 33; *But see* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1243-1244 (1998) (explaining the concept of "reasonable foreseeability"); Sanjay S. Mody, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365, 379-381 (2001).

[18] *See* Perritt, *supra* note 4, at 477-78 (stating that self-governance for the Internet is, not only legally feasible, but also "desirable for several reasons: self-governance may be more efficient; electronic network communities need different rules and procedures; open networks escape enforcement of conventional rules; and self-governance promotes voluntary compliance").

[19] *See* Johnson & Post, *supra* note 4, at 1389; Reidenberg, *Governing Networks*, *supra* note 9, at 920.

[20] *See* Johnson & Post, *supra* note 4, at 1389;

[21] *See* David G. Post, 43 WAYNE L. REV. 155, 163-165 (1996) (recalling on this point Jefferson's ideas on the decentralization of law-making to support cyberspace self-regulation).

[22] *See* Viktor Mayer-Schönberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 621 (2003) (stating that "self-rule and self-regulation […] sound very American and thus resonate with many of the largely American, suburban, middle-class people on the Net today"). *See also* Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261, 262 (2002) (confirming that "[S]eparatist philosophy derives largely from the American value placed on the unfettered flow of information").

regulated by self-regulating regimes, or only some specific subsets within it?[23] Another complex problem that cyber-libertarians face is enforcement. If there is no physical force in place, what means does the Net community have to enforce its own-built rules?[24] Some commentators state that the cost of expulsion from the community would be a valid tool of deterrence,[25] but this issue is far from being solved.

The libertarian claims have been contested, both on the descriptive[26] and normative fronts.[27] First of all, it is debatable whether in fact cyberspace constitutes a free place, a sovereign jurisdiction, far from state's reach.[28] Secondly, even taking for granted that assumption, what the Internet actually is may differ from what it should be, as leading scholars like Lessig have argued.[29] Goldsmith, in an already seminal work, has used the word "cyberanarchy" to describe (and fight back against) that kind of discourse which defends a space separate from the real world and devoid of any rules.[30] In sharp contrast with the separatist view, those who may be called traditionalists affirm that the political and legal institution known as the State is the proper regulatory organization to carry out the task of regulating the Internet.[31] The State, based on elected governments combined with the rule of law, exhibits a proven democratic legitimacy[32] and encompasses the institutional mechanisms to enforce the regulations needed to manage cyberspace.[33]

Traditionalists deal with the spillover effect, that is, the problems related to having as many regulations affecting Internet activities as there are states, many of which may be overly contradictory or conflicting, [34] by pointing out that this problem is hardly exclusive to cyberspace. [35] Moreover, conflict-of-laws doctrines have evolved to solve this problem effectively.[36] In sharp contrast with the spillover effect, the issue of regulatory evasion or regulatory arbitrage remains,[37] but this would be no more problematic

---

[23] *See* Mayer-Schonberger, *supra* note 22, at 622-623; Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT. L. REV. 1257, 1268-69 (1998).
[24] *See* Mefford, *supra* note 6, at 213 and 235.
[25] *See* Gibbons, *supra* note 2, at 523.
[26] *See* Timothy S. Wu, *Cyberspace Sovereignty? – The Internet and the International System*, 10 HARV. J.L. & TECH. 647 (1997).
[27] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, 25 (1999).
[28] *See* Wu, *supra* note 26, at 649-56; *Cf.* Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561, 562 (1998) (stating that "[T]he argument that technological changes occurring today require the death of the state and its regulatory function proves too much").
[29] *See* LESSIG, *supra* note 27, at 25.
[30] *See* Goldsmith, *supra* note 17; Netanel, *supra* note 7, at 443.
[31] *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEG. STUD. 475, 476 (1998); Charles Fried, *Perfect Freedom or Perfect Control?*, 114 HARV, L. REV., 606, 621 (2000) ; *See also* Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW., 1167, 1174 (1998) (stating, with regard to Cyber Law, that "[W]hatever connections the Internet facilitates among its users, it has no claim of authority over them. Whatever difficulties territorial states have in regulating elusive Internet behavior, there is no Internet sovereignty with which they must reckon").
[32] *See* Steven T. Ratner, *New Democracies, Old Atrocities: An Inquiry in International Law*, 87 GEO. L.J. 707, 740 (1999).
[33] *See* Mayer-Schönberger, *supra* note 22, at 612.
[34] *See* Johnson & Post, *supra* note 4, at 1374.
[35] *See* Goldsmith, *supra* note 17, at 1240-42; Trachtman, *supra* note 28, at 568-569; Mody, *supra* note 17, at 382-84. On the normative side, it has been also pointed out that states have the legitimate right to subject to their jurisdiction transnational activity having local effects even if it causes spillover effects (that is, it affects activities and regulation in other countries), *see* Goldsmith, *supra* note 17, at 1240-41.
[36] *See* Goldsmith, *supra* note 17, at 1205-12 (arguing that the current approach to choice of law is no longer based on a traditional and territorialist conception of how conflicts of law are resolved as the "skeptics", in Goldsmith terms, intend to show).
[37] *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, in BORDERS IN CYBERSPACE, INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 129, 140-150 (Brian Kahin & Charles Nesson eds., 1997); Mayer-Schönberger, *supra* note 22, 616 (describing it as the situation in which users of cyberspace, "seeking information that is illegal in their own jurisdiction, can go out on the Internet, disguise themselves, take another identity -and thus simulate their presence in another jurisdiction- and obtain the information they desire").

within the field of Internet regulation than with regard to other areas of the real world.[38] Thus, at least recently, there seems to be a growing consensus that the Internet does not constitute a distinct physical space or even a different jurisdiction,[39] and that it is starting to be viewed as the product of an advanced telecommunications technology.[40] National regulation of cyberspace transactions is legitimate and feasible.[41] The law must only adjust to this new reality,[42] and, as technology proceeds, we should expect to experience an increase in state regulation of cyberspace.[43]

There is a third way to tackle the Internet issue, namely, mixed regulation or governance.[44] This approach is not very different from a more classical view that distinguishes between default rules and mandatory rules.[45] Most commentators taking this approach think that cyberspace regulation should be the result of a mixture of national laws and self-community rules. This hybrid regulation would assure the legitimacy, flexibility and enforceability needed for Internet regulation to become a working legal system.[46] As Mayer-Schönberger has shown, it is possible to regulate the Internet avoiding the extremes (that is, relying exclusively on either national regulation or self-regulation) by way of blending together national law, self-regulation and even International Law.[47] To be sure, international lawyers have always reminded us that International Law and harmonization could be, and indeed are, the natural solution for global problems. Regarding the Internet, however, International Law alone is not always recommended,[48] and as a result, a sort of mixed governance has evolved with the Internet Corporation for Assigned Names and Numbers ("the ICANN"), a fascinating combination of the three mentioned regulatory layers.[49] We shall consider this situation and the question of Internet governance more deeply below.

Finally, that national regulation on the Internet is possible and is a reality can be confirmed very

---

[38] *See* Goldsmith, *supra* note 17, at 1222.
[39] *See* Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, in WHO RULES THE NET? 22 (Adam Thierer & Clyde Wayne Crews Jr. eds., 2003) (stating that early accounts "are now thoroughly dated, premised on a digital divide between offline and online that less and less exists"). *Cf.* Fried, *supra* note 31, at 621.
[40] *Cf.* Stein, *supra* note 31, at 1174.
[41] *See* Goldsmith, *supra* note 17, at 1244, 1249 (pointing out that national and international regulations on the Internet are not only legitimate and feasible, but also necessary, because they provide the enforcement mechanisms and flexibility needed by private parties).
[42] *See* Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C.L. REV. 359, 364 (2003) (pointing out that "[C]yberlaw has turned out to be a project of 'cyberizing' law, translating familiar legal concepts and the rough balance of interests created by the legal system into the Internet environment").
[43] *See* Wu, *supra* note 28, at 660; James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors* 66 U. CIN. L. REV. 177, 184 (1997) (forecasting the reaction of law and the state).
[44] *See* Reidenberg, *Governing Networks*, *supra* note 8, 929-30 (suggesting a "system of state-provided incentives through encouragement, as well as allocation of liability, that will induce networks themselves to adopt desirable public policies […] yet state governments cannot and should not attempt to expropriate all regulatory power from network communities").
[45] *See* Goldsmith, *supra* note 17, at 1216 and 1245.
[46] *See* Henry H. Perritt, Jr., *The Internet is Changing the Public International Legal System*, KY. L.J. 885, 930 (1999-2000) (stating that "[T]hese hybrid structures offer the advantages of greater flexibility and decentralization available through private ordering, while tying private ordering to public law to enhance legitimacy, political acceptability, and enforcement through state-based coercion when necessary").
[47] *See* Mayer-Schönberger, *supra* note 19, at 639-664 (giving examples, such as the case of obscenity laws -based on self governance and state governance, EU Directives -a mix of international and state governance, and others, to demonstrate the feasibility and the real existence of this kind of mixed regulation).
[48] *See* Perritt, *supra* note 46, at 930-931.
[49] *See* Mayer-Schönberger, *supra* note 22, at 656. *See also* Perritt, *supra* note 46, at 954 (confirming that the EU/US Data Privacy Agreement and ICANN regulation on Internet domain names are new models for international hybrid regulation). Mayer-Schönberger recognizes, however, that this kind of best regulatory option comes at a cost: "Governance blends potentially are less transparent to people than existing governance regimes [and] in some instances might lead to an increase in overlaps of governance regimes", *see* Mayer-Schönberger, *supra* note 22, at 669.

easily if we take a look at just any country's existing regulations in this field. For example, the US legislation on the Internet includes, among the best known, the Communications Decency Act (CDA), Child Online Protection Act (COPA), Children's Internet Protection Act (CIPA), Digital Millennium Copyright Act (DMCA), Uniform Electronic Transaction Act (UETA), Anti-Cybersquatting Consumer Protection Act (ACPA), E-Sign, and Uniform Computer Information Transaction Act (UCITA). So abundant national regulations on different issues related to the Internet exist along with various approaches to those issues. What we want to further advance now is the current role of International Law regarding this existing and mainly national regulation of the Internet.

3. CURRENT ROLE OF INTERNATIONAL LAW ON THE REGULABILITY OF THE INTERNET

In this section we will analyze several issues in which there is some room for International Law. First, the willingness on the part of some States (European included) to control and eliminate harmful content within the Internet has collided with the firm and constitutionally protected right of freedom of expression in the USA. Questions of jurisdiction and choice of law between sovereigns have attracted much attention in this regard. Second, there is the question of the protection of intellectual property rights. Copyrights and other intellectual property rights seem to be massively violated by software allowing piracy. In this case, International Law instruments have been used by States desiring to combat this ever-growing activity. Third, the protection of data privacy against illegitimate uses on the part of companies operating through the Internet has prompted agreement between the main dissenting parties, i.e. the U.S. and the EU.

3.1. FREE SPEECH AND HARMFUL CONTENT

One of the most compelling issues related to the Internet is the protection of free speech versus the legal hunting of harmful content. Whereas in the US there is a strong sentiment, constitutionally protected, favoring freedom of speech, we see that European countries and Australia are more favorable in this balance towards controlling the distribution of harmful content. The *Compu Serve* and *Yahoo! France* cases demonstrate the European approach followed by Germany and France regarding this issue. International Law has a major role to play with respect to this substantive problem because this is also a jurisdictional issue. Regulatory conflicts in cyberspace are now frequently linked to the interplay between the worldwide availability on the web of data perceived to be harmful or offensive to fundamental values in the regulating State, and the constitutional protections for freedom of expression existing in the State in which the data is made accessible, i.e. the USA, where many of content providers are located.

The *CompuServe* case was one the first renowned cases of what could be called a "true" regulatory conflict.[50] The alleged offence to German law, the Criminal Code, consisted of the provision by CompuServe Deutschland (a 100% subsidiary of CompuServe USA) of access to publicly available violence, child pornography and bestiality. The content was stored on CompuServe USA's newsgroups servers. After blocking access worldwide to that content, CompuServe made available parental control software to its subscribers and unblocked the newsgroups. Nevertheless, a sentence was imposed by the Munich court on Felix Somm, managing director of CompuServe Deutschland.[51] Although the case was later overturned by a German higher court,[52] this sentence attracted much criticism, particularly in the USA.

Such criticism has been scant, however, compared to the almost universal condemnation received by the *Yahoo!* case in the USA. This case arose when two French public interest groups, La Ligue Contre le Racisme et L'Antisemitisme (LICRA) and L'Union des Etudiants Juifs de France (UEFJ), sued Yahoo! Inc., a Delaware corporation located in California. The alleged criminal offence was the offering for sale of Nazi memorabilia by the Yahoo! auction website accessible in France, which was deemed illegal under French law. Indeed, French legislation, along with many other nations' laws, may be considered to be in accordance with the Convention on the Elimination of All Forms of Racial Discrimination (IECRD).[53] The plaintiffs sought an order prohibiting Yahoo! from displaying the memorabilia in France. The French court, which found it had personal jurisdiction because the harm was caused in France, sought an expert opinion on the possibility for Yahoo! to block access to French users, instead of completely eliminating the website content worldwide. After being advised that this could be achieved with a 90 % success rate (besides, French users were greeted by the website with advertisements in French, which means some kind of geographical identification was already available), it ordered Yahoo! "to take all measures at their availability, to dissuade and render impossible all visitation on Yahoo.com to participate in the auction service of Nazi objects".[54] After that, Yahoo! sought a declaratory judgment that the French decision could not be recognized in the USA. Besides finding it had jurisdiction,[55] the US District Court granted summary judgment on the merits in favor of Yahoo![56] Nevertheless, the US Court of Appeals has recently reversed

---

[50] Horatia Muir Watt, *Yahoo! Cyber-Collision of Cultures: Who Regulates?*, 24 MICH. J. INT'L L. 673, 676 (2003) ("Typically, an assertion of freedom of expression in the State in which the website is located clashes with restrictive legislation in the receiving State, designed to protect such values as the right of privacy, to restrict hate speech or libel, or to prohibit indecency or pornography. The free availability of information collides with the negative right of the receiving State to protect itself against outside interference").

[51] *See* Gareth Grainger, *Freedom of Expression and Regulation of Information in Cyberspace: Issues concerning Potential International Cooperation Principles*, in THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 90-91 (Teresa Fuentes Camacho ed., 2000).

[52] Apparently, most commentators agree that the judge in the *CompuServe* trial simply did not apply the Internet legislation properly to the case, *see* Franz A. Mayer, *Europe and the Internet: The Old World and the New Medium*, 11 EUROPEAN JOURNAL OF INTERNATIONAL LAW 149, 151 (2000).

[53] International Convention on the Elimination of All Forms of Racial Discrimination, Mar. 7, 1966, 660 U.N.T.S. 195.

[54] *See* LICRA & UEJF v. Yahoo! Inc., T.G.I. Paris, May 22, 2000, available at http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (last visited September 23, 2005), reprinted in LEA BRILMAYER & JACK GOLDSMITH, CONFLICT OF LAWS: CASES AND MATERIALS 851-53 (5th ed. 2002).

[55] Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168 (N.D. Cal. 2001).

[56] Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

that decision,[57] and held that the California Court had no personal jurisdiction over the French parties and that France had every right to hold Yahoo! accountable in France.[58]

Despite the overwhelming criticism that the French ruling received in the USA,[59] the Yahoo! case has shown that traditional conflict of laws instruments may apply to cyberspace, and that France was thus entitled to apply its national law because the harmful effects had occurred in its territory.[60] The case has also confirmed that in trans-boundary disputes in which issues of freedom of speech arise,[61] it is not the place of the country of the information provider but the place of the country of the recipient to govern the situation.[62] The *Gutnick* case, decided by the Australian Supreme Court,[63] has recently come to corroborate this approach, and reflects therefore the emerging majority opinion.[64] The German, French and Australian democracies have chosen rules for free expression that are consistent with international human rights but that do not mirror the protection afforded by the First Amendment to the United States Constitution.[65]

It may be said that this kind of solution ultimately goes against the basic freedom of speech and freedom of information in cyberspace, but, as leading scholars like Lessig have demonstrated, the fact that the Internet has been developed as a free place does not say anything about how it should be.[66] The technological designs developed by code writers, the web architecture, carries a sort of ideological or philosophical choice, very much reflecting the values expressed in the First Amendment.[67] Code is law, but this kind of *lex informatica*[68] need not entail normative implications for solutions of regulatory conflicts. The Internet is what we make of it; there is nothing essentially given and unchangeable. Technological

---

[57] Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 379 F. 3d 1120, 1126 (9th Cir. 2004).
[58] Joel R. Reidenberger, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1952 (2005).
[59] *See* Ben Laurie, *An Expert's Apology* (Nov. 21, 2000), available at http://www.apache-ssl.org/apology.html (last visited September 23, 2005) (describing the solution imposed by the French ruling as "half-assed and trivially avoidable").
[60] Reidenberg has been a *rara avis* in the USA when he has sided with the French ruling in several articles, *see e. g.* Joel R. Reidenberg, *supra* note 22, at 42 (stating that "no one could seriously challenge that France has jurisdiction to prescribe rules for activities within French territory. Yahoo, however, thought it was above the law"; "[T]he Internet does not, however, displace the well-established principle in international law that allows states to exercise prescriptive jurisdiction of conduct having effects occurring within the national territory").
[61] There has been however self-criticism in the USA about the failure to explain the "differences between promulgation of speech-restrictive rules and mere enforcement of them" and "why speech directed abroad necessarily deserves First Amendment protection", *see* Molly S. Van Houwelling, *Enforcement of Foreign Judgments, the First Amendment, and Internet Speech: Notes for the Next Yahoo! v. Licra*, 24 MICH. J. INT'L L. 697, 698 (2003).
[62] Mathias Reimann, *Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage*, 24 MICH. J. INT'L L. 663, 667-668 (2003).
[63] *See* Dow Jones & Company Inc. v. Gutnick [2002] HCA 56 (10 December 2002), available at http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html (the Australian Supreme Court has found jurisdiction in a libel case brought by an Australian plaintiff against Dow Jones & Co. on the basis of an article published in New Jersey but accessible and downloaded in Australia). This decision has been nevertheless criticized *see* Uta Kohl, *Defamation on the Internet—Nice Decision, Shame about the Reasoning: Dow Jones & Co. Inc. v. Gutnick*, 52 INT'L & COMP. L. Q. 1049 (2003); Nathan W. Garnett, *Dow Jones & Co. v. Gutnick: Will Australia's Long Jurisdictional Reach Chill Internet Speech World-Wide?*, 13 PAC. RIM. L. & POL'Y J. 61 (2004); Shawn A. Bone, *Private Hars in the Cyber-World: The Conundrum of Choice of Law for Defamation Posed by Gutnick v. Dow Jones & Co.*, 62 WASH. & LEE L. REV. 279 (2005).
[64] *See* Zittrain, *supra* note 39, at 19.
[65] *See* the Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 2 (item 5) which, taking into account art. 29 of the Universal Declaration of Human Rights, states that "in the exercise of their rights and freedoms, everyone shall be subject only to the such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society".
[66] *See* LESSIG, *supra* note 27, at 207-208.
[67] *See* Reidenberg, *supra* note 58, at 262-63 (confirming that the so called "separatist" philosophy "derives largely from the American value placed on the unfettered flow of information"; but noting also that "the American position is becoming a minority view").
[68] Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, TEX. L. REV. 553 (1998).

innovation is now empowering sovereign states to assert their rules on Internet activity.[69] Filtering and zoning technologies allow for location, and claims of the ubiquity of information on the web no longer hold.[70] The *Yahoo!* case has just shifted the rule-making power from technologists back to political representatives.[71] When considering regulatory conflicts in the international arena, then, "there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it. Analysis of such a claim has shown that it reverses the proper relationship between law and technology. Technology being purely manmade, and thus subject to ideological choice, should not dictate the way in which law manages conflicting interests arising through its medium".[72]

Extraterritoriality and jurisdiction in cyberspace have then been the focus of an intense debate, and the dichotomy between freedom of speech and the protection against harmful content has simply been the issue articulating this conflict, despite the existence of other kinds of extraterritoriality cases within the Internet, i.e. when the USA has required compliance with its copyright laws abroad.[73] As Goldsmith maintains, extraterritorial regulation within the internet field is justified on the basis that cyberspace is not functionally different from transnational activities carried out through other means and because every state has the right to regulate those extraterritorial acts that may produce harm or other local effects within the national jurisdiction. This kind of approach is commonplace in national legal systems and is legitimate until a nation has acquiesced to an international law rule that specifies otherwise.[74]

It can be said then that extraterritorial regulation in the Internet field is feasible, although it need not be perfect in order to be effective.[75] Also, choice of law rules do work within the Internet realm as much as within other real world fields.[76] The *CompuServe, Yahoo!* and *Gutnick* cases just show us that International Law and doctrines like prescriptive jurisdiction, effects-based jurisdiction, and the technical solution of filtering and zoning are helping to solve transnational disputes in a fair way until there is a solution based on international harmonization or otherwise.[77] If international harmonization is difficult to

---

[69] *See* Reidenberg, *supra* note 56, at 1960. Some authors have nevertheless expressed caveats with respect to the possibility that technology becomes the means of transmitting and implementing the values of the regulating nation, *see* Yochai Benkler, *Internet Regulation: A Case Study in the Problem of Unilateralism*, 11 EUROPEAN JOURNAL OF INTERNATIONAL LAW 171, 178 (2000).

[70] *But see* Robert Corn-Revere, *Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?* in WHO RULES THE NET? 225-226 (Adam Thierer & Clyde Wayne Crews Jr. eds., 2003) (stating that the Internet can not be carefully calibrated by using technology to keep information out of restrictive jurisdictions).

[71] *See* Reidenberg, *supra* note 58, at 272.

[72] *See* Muir Watt, *supra* note 49, at 695. *See also* Reidenberg, *supra* note 56, at 1970-72 (maintaining that "when technologies exist and are deployed for commercial purposes, they are typically not configured to support public policies […] States have, as a result, a normative incentive to assert the supremacy of law over technological determinism").

[73] A very well known case was Twenty Century Fox Film Corp. v. iCraveTV.com, 53 U.S.P.Q. 2d (BNA) 1831 (W.D.Pa. 2000), where the US district court applies an analysis similar to the French Yahoo! ruling. *See* Cherie Dawson, *Creating Borders on the Internet: Free Speech, the United States, and International Jurisdiction*, 44 VA. J. INT'L L. 637, 657 (2004). *See* Reidenberg, *supra* note 58, at 274 (stating that "[t]he U.S. values are inconsistent by favoring the free flow of information against data privacy and speech restrictions, but not against intellectual property".

[74] *See* Goldsmith, *supra* note 17, at 1239-40.

[75] Indeed, the contrary appears to be true, because zoning and filtering technologies may make prescription and enforcement to coincide, ensuring perfect compliance, *see* Muir Watt, *supra* note 50, at 688-689.

[76] *See* Goldsmith, *supra* note 17, at 1223 and 1233-34, respectively.

[77] *See* Mark F. Kightlinger, *A Solution to the Yahoo! Problem? The EC E-Commerce Directive as a Model for International Cooperation on Internet Choice of Law*, 24 MICH. J. INT'L L. 719 (2003) (stating that the EC E-Commerce Directive and its "country

achieve,[78] it may be the time for the U.S. to take some steps in order to avoid being the so-called hate speech haven.[79]

3.2 INTELLECTUAL PROPERTY

With the coming on of the Internet, the protection of intellectual property rights has been challenged by new technologies and software (like MP3 and Napster)[80] allowing the free distribution of copyrighted digital works. These technologies permit Internet users to download perfect copies of songs, movies and other works[81] previously protected by existing national laws and international treaties.[82] This problem has only been aggravated by the advent of peer-to-peer (P2P) technologies,[83] a new type of software which allows Internet users to download files between individual hard drives without a central server doing any job.[84] Apparently, these kinds of Internet technologies have paved the way to massive piracy, with the ensuing losses for authors and the industry in general.[85] The responses to this new situation have been twofold.

On the one hand, after the first efforts were carried out by the US Commerce Department in 1995 with the aim to restore the "balance" in intellectual property law,[86] the immediate legal answer has translated into new national laws seeking to reinforce the protection afforded by traditional copyright laws. In the USA, the No Electronic Theft Act (NETA) in 1997 and the Digital Millennium Copyright Act (DMCA) in 1998 were passed to that end,[87] although the DMCA has been accused of shifting the balance in favor of private entities.[88] Similarly, the Copyright Directive has been adopted in the EU.[89] Also,

---

of origin" and "home country control" rules would be a good starting point for an international agreement on internet content which would ease transnational disputes); Viktor Mayer-Schonberger & Teree E. Foster, *A Regulatory Web: Free Speech and the Global Information Infrastructure*, in BORDERS IN CYBERSPACE, INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 244 (Brian Kahin & Charles Nesson eds., 1997) (arguing that the international concept of *ius cogens* might provide a basis for regulating speech content on the Net).

[78] On the impossibility of developing universally accepted Internet content regulation, *see* Julie L. Henn, *Targeting Transnational Internet Content Regulation*, 21 B.U. INT'L L.J. 157, 172 (2003).

[79] *See* Christopher D. Van Blarcum, *Internet Hate Speech: The European Framework and the Emerging American Haven* 62 WASH. & LEE L. REV. 781, 826 (2005).

[80] Jeffrey L. Dodes, *Beyond Napster, Beyond the United States: The Technological and International Legal Barriers to On-line Copyright Enforcement*, N.Y.L. SCH. L. REV. 279 (2002-2003).

[81] *See* NICHOLAS NEGROPONTE, BEING DIGITAL, 58 (1995).

[82] For a short history on the legal protection of intellectual property, *see* KLAUS W. GREWLICH, GOVERNANCE IN "CYBERSPACE", ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS, 219 (1999).

[83] Scholars have recently proposed some solutions to the yet unsolvable question of P2P technologies, instead of suing users or facilitators of these technologies, *see* Mark A. Lemley and R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345 (2004); Jessica Litman, *Sharing and Stealing*, 27 HASTINGS COMM. & ENT. L.J. 1 (2004); Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-To-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003).

[84] On the prominent examples of this kind of file sharing such as Gnutella and Freenet, *see* STUART BIEGEL, BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE, 287 (2001).

[85] However, it is said that the losses for the industry are not that big, *see*

[86] *See* U.S. Department of Commerce, Task Force – Working Group on Intellectual Property Rights, "Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights", available at http://www.uspto.gov/web/offices/com/doc/ipnii (last visited October 1, 2005).

[87] No Electronic Theft Act, *17 U.S.C. (2000)*; Digital Millennium Copyright Act (DMCA), *Pub. L. No. 105-304*, 112 Stat. 2860 (1998).

[88] *See* Hughes, *supra* note 42, at 371.

[89] Council Directive 2001/29/EC of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10, modified by the Corrigendum to Directive 2001/29/EC, 2002 *O.J.* (L 6) 70. *See* Thomas

national courts have made a great effort to elucidate the question of how to protect those copyrights and to what extent, in order not to limit excessively the information available in the public domain, with the results tilting in favor of copyright protection.[90]

On the other hand, the answer (allowed by national laws) has also been technical, because the industry (subsidized by government)[91] has used technology as well to create copyright management schemes called "trusted systems", that is software that makes it easier for information providers to control access to and use of copyrighted content. In this way, enforcement by the code is "ex-ante", free from legal scrutiny and efficient to a degree that does not exist in the non-virtual world.[92] This technical response, which substitutes private empowerment for public law,[93] has lead to an important criticism on the part of authors, because this perfect control carried out by private companies providing internet content may have consequences with respect to the right to privacy and freedom of expression, which in turn concerns other issues like fair use and public domain doctrines.[94]

Efforts to craft international regulation in the intellectual property field have led to the WIPO Copyright Treaties, i.e. the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.[95] It may be said that these agreements are the only indisputable example of international treaty-based, top-down, development of legal norms regarding the Internet.[96] These recent WIPO Treaties have been added to the existing and already ancient international treaties, i.e. the Paris Convention for the Protection of Industrial Property and the Berne Convention for the Protection of Literary and Artistic Works,[97] with the stated aim of strengthening the protection afforded to copyright owners. There is some controversy as to the results achieved by these new treaties. Whereas for some it is not at all clear whether these treaties have really developed the protection previously existing,[98] for others the WIPO treaties may be regarded as a

---

Hoeren, *The European Union Commission and Recent Trends in European Information Law*, RUTGERS COMPUTER & TECH. L.J. 1 (2003).

[90] *See* A & M Records, Inc. v. Napster, Inc. *114 F. Supp. 2d 896 (N.D. Cal. 2000)*, affirmed in part, reversed in part, *239 F. 3d 1004* (9th Cir. 2001); Universal City Studios, Inc. V. Corley *111 F. Supp. 2d 294 (S.D.N.Y. 2000)*, aff'd sub nom. *Universal City Studios, Inc. V. Corley, 273 F 3d. 429 (2d Cir. 2001)*.

[91] *See* LESSIG, *supra* note 27, at 126.

[92] Niva Elkin-Koren, *Copyright in Cyberspace: The Rule of the Law and the Rule of the Code*, in LAW, INFORMATION AND INFORMATION TECHNOLOGY 135-136 (Eli Lederman & Ron Shapira, eds. 2001).

[93] *See* LESSIG, *supra* note 27, at 135.

[94] *See e.g.* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999); Julie E. Cohen, *A Right to Read Anonimously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) and *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345 (1995); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1999); LAWRENCE LESSIG, THE FUTURE OF IDEAS 4-16 (2001); Neil W. Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1 (2001) and *Locating Copyright Within the First Amendment Skein*, STAN. L. REV. 1 (2001); *But see* Pamela Samuelson, *Copyright and Freedom of Expression in Historical Perspective*, 10 J. INTELL. PROP. L. 319 (2003).

[95] WIPO Copyright Treaty, adopted Dec. 20, 1996, *36 I.L.M. 65 (1997)*; WIPO Performances and Phonograms Treaty, adopted Dec. 20, 1996, *36 I.L.M. 76 (1997)*.

[96] *See* Hughes, *supra* note 42, at 373-374.

[97] Paris Convention for the Protection of Industrial Property, opened for signature Mar. 20, 1883, as revised at Stockholm on July 14, 1967, *21 U.S.T. 1630, 828 U.N.T.S. 305*; Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised at Paris on July 24, 1971, *25 U.S.T. 1341, 828 U.N.T.S. 221*.

[98] *See* MARCUS FRANDA, GOVERNING THE INTERNET, THE EMERGENCE OF AN INTERNATIONAL REGIME 126 (2001) (describing the recent WIPO treaties as conservative).

positive outcome, even if the "high-protectionist" agenda of the USA did not succeed.[99] It would also be good to note here that the EU agenda in this regard was not less protectionist.[100] Nevertheless, it seems that national implementation of these treaties has gone far beyond what they require,[101] and what they require is no less contentious.[102]

Furthermore, the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights[103] of 1995 has been a benchmark international agreement for the protection of copyrights globally,[104] and it may very well be so in the Internet field. This agreement not only sets out minimum rules and standards of protection and harmonizes domestic procedures and remedies for the enforcement of intellectual property rights, but above all, it extends the dispute settlement mechanism of the WTO to this particular field.[105] This extension of the dispute settlement system was meant to improve the enforcement mechanisms applicable to copyright violations that were almost absent before the coming of the TRIPS.[106] The benefits internationally of this treaty are now being coupled with other national benefits; that is, some representatives of copyright industries have already advanced the idea of using the TRIPS agreement to dispute existing exceptions to national copyright laws.[107]

As we see, International Law has played and will likely continue to play a very important role in the protection of intellectual property rights in the Internet field. It is not only that there is some regulation, but that this regulation is also of the best kind. International treaties and agreements, that is, "hard law" as opposed to "soft law", are used here by the States in order to cooperate and establish minimum standards, mandate the setting up of domestic enforcement mechanisms, and use a system to settle international disputes arising in this context. Why is it that we find this strong approach here, but only here?[108] The convergence of interests between nation-states and copyright holders with vast intellectual property assets has made it possible for International Law to play an important role in the regulation of this specific area of

---

[99] *See* Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 435 (1997).

[100] The EU wanted to have protected the ephemeral copies or temporary reproductions, together with a copyright on databases, *see* Grewlich, *supra* note 80, at 238 and 244.

[101] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH, L.J. 519, 521 (1999); Grewlich, *supra* note 82, at 257 and 261.

[102] These treaties require signatories to provide "effective legal remedies against the circumvention of effective technological measures that are used by authors" in the exercise of their copyrights (art. 11 of the WIPO Copyright Treaty and art. 18 of the WIPO Performances and Phonograms Treaty), that is, states must take legislative measures to safeguard "technical protection systems" adopted by copyright owners. This kind of anti-circumvention legislation may lead to the privatization of information policy in cyberspace, *see* Elkin-Koren, *supra* note 92, at 141.

[103] Agreement on Trade-Related Aspects of Intellectual Property Rights in WTO, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 321 (1999).

[104] It was not at all a cherished agreement for developing countries, which accepted it as a part of the Uruguay Round package deal, *see* MICHAEL TREBILCOCK AND ROBERT HOWSE, THE REGULATION OF INTERNATIONAL TRADE 320-321 (2nd ed., 1999).

[105] On the significance of this Dispute Settlement System *see* MITSUO MATSUSHITA, THOMAS J. SCHOENBAUM & PETROS C. MAVROIDIS, THE WORLD TRADE ORGANIZATION, LAW, PRACTICE AND POLICY 18 (2003).

[106] In fact, the TRIPS has not been fully effective yet, as non-violation complaints were agreed not to be brought under it until 2000 (TRIPS Agreement Art. 64.2 and 3), and then the Doha Ministerial Conference has delayed it to the following ministerial conference in Cancun (which failed to reach any agreement), *see* WTO, Ministerial Conference, Fourth Session, Doha, 9-14 November 2001, *Implementation-Related Issues and Concerns*, WT/MIN (01)/DEC/17, 20 November 2001, para. 11.1.

[107] *See* Samuelson, *supra* note 88, at 332.

[108] It is true that the hunting of crime in cyberspace has also led to another international treaty, the Cybercrime Treaty (European Convention on Cybercrime, Nov. 23, 2001, 185 *E.T.S.*). However, the effort displayed to achieve and implement this treaty's goals has not been so muscular, *see e.g.* Sara L. Marler, *The Convention on Cybercrime: Should the United States Ratify?*, 37 NEW ENG. L. REV. 183 (2002); Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead* 2 J. HIGH TECH L. 101 (2003); Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, BERKELEY TECH. L.J. 425 (2003).

the Internet. So it seems that only if International Law completely fulfils the expectations of business within the Internet field will it be a preferred tool for States to regulate this area of human activity. In this regard, it seems quite difficult to implement one of the action lines of the World Summit on the Information Society sponsored by the U.N. and the I.T.U., which provides for the "development and promotion of public domain information as an important instrument promoting public access to information".[109] The question remains whether the UN is as effective an international structure as, say, the WTO in attempting to regulate this field of human activity and in implementing that regulation.

3.3 PRIVACY

Large scale processing of personal data was initially reserved to institutions with centralized databases. The advent of the PC and the Internet has changed that situation, and now there are many more participants using personal information. Almost anyone with a PC and access to the Internet may collect and process personal information, which has led to a dramatic change with regard to the privacy issue.[110] Specially, profiling and data mining activities on the part of marketing companies have been the focus of privacy scholars for some time now.[111] Therefore, the protection of personal data and privacy in the Internet era has become a critical public policy concern,[112] and States have started to realize how important this question is in itself for democracy,[113] let alone its role in fostering e-commerce. The World Summit on the Information Society has just recalled how vital this issue is for the development of the Internet.[114]

The protection of personal information is not the same in every country but varies prominently between different states, and this disparity is striking when we compare the approaches taken by the USA and the EU.[115] Although the USA was probably the first country regulating privacy,[116] the protection afforded to personal information here has always been based on a market-dominated policy[117] coupled with

---

[109] *See* World Summit on the Information Society, Geneva 2003-Tunis 2005, Plan of Action, December 12, 2003, at 4, Doc. WSIS-03/GENEVA/DOC/5-E. The Plan of Action states that the action lines are aimed "to advance the achievement of the internationally-agreed development goals, including those in the Millenium Declaration, the Monterrey Consensus and the Johannesburg Declaration and Plan of Implementation, by promoting the use of ICT-based products, networks, services and applications, and to help countries overcome the digital divide", *id.* at 1.

[110] *See* Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 557-61 (1998) (commenting on the quantitative and qualitative change in privacy).

[111] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1238-41 (1998); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 530 (1995).

[112] *See* Robert Gellman, *Conflict and Overlap in Privacy Regulation: National, International, and Private*, in BORDERS IN CYBERSPACE, INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 255 (Brian Kahin & Charles Nesson eds., 1997); Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 Wake Forest L. Rev. 105, 106 (1995).

[113] *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 557 (1995).

[114] *See* the Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 5, whose principle number 5 states that "[S]trengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs […] it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade".

[115] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1319 (2000).

[116] *See* Gellman, *supra* note 112, at 255.

[117] *See* Reidenberg, *supra* note 115, at 1318; Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 770-773 (1999); DANIEL J. SOLOVE, THE DIGITAL PERSON, TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 91 (2004) (arguing that the market currently fails to provide mechanisms to enable individuals to

the strong influence of First Amendment principles that favor the free flow of information.[118] Within this model, the role of the state is limited: legal rules and statutory rights are aimed to protect narrowly defined sectors so that privacy protection is mainly to be achieved by industry self-regulation and codes of conduct.[119]

This has been highly criticized by some scholars[120] who have seen international and, especially, European regulations as a formula to be followed. Schwartz and Reidenberg have persistently repeated that the European, as opposed to the U.S., approach regarding privacy is the most appropriate because it rightly considers data protection as a civil rights issue.[121] They highlight the normative role of privacy in democratic governance,[122] arguing that a model based in self-regulation and the market may harmfully affect deliberative democracy.[123] Nevertheless, U.S. information culture may be changing.[124] To some extent, there is a growing concern among the American population with the extensive use of information technologies to build profiles of individuals.[125] That concern explains why the Federal Trade Commission (FTC) and the U.S. Congress have tried to improve the substantive and procedural rights of individuals regarding their right to privacy,[126] although it is true that this regulation is still limited by its sector-based approach.[127]

The other predominant approach, the European approach (which is also the model existing in countries such as Canada, Australia, New Zealand and Hong Kong),[128] consists of a comprehensive data protection law.[129] In this model, a kind of omnibus legislation creates a wide-ranging set of rights and obligations for the processing of personal information and, as opposed to a market-based policy, entails a human rights perspective where users are not "consumers" but "citizens".[130]

As a result of being party to the European Convention of Human Rights (ECHR) and other

---

exercise informed meaningful choices).

[118] *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 153 (1998).

[119] *See* Reidenberg, *supra* note 115, at 1331.

[120] *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999).

[121] *Cf.* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 39-42 (1996).

[122] *See* Reidenberg, *supra* note 115, at 1340.

[123] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1615 (1999) (considering that no other option but the imposition of standards through law will serve to the aim of developing effective privacy norms); Paul M. Schwartz, *Internet Privacy and the State*, CONN. L. REV. 815 (2000) (analyzing the flaws in the dominant rhetoric that favors the market, bottom-up regulation, and industry self-regulation); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373 (2000) (arguing that both legal and technological tools will foster data privacy protection).

[124] *See* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy* 87 CAL. L. REV. 751, 770 (1999).

[125] *See* Kang, *supra* note 111, at 1196-97.

[126] Even those who consider the traditional U.S. approach to privacy regulation as appropriate, have conceded that there is a movement in this country towards a more intense protection in this field, *see* Fred H. Cate, *Privacy Protection and the Quest for Information Control*, in WHO RULES THE NET? 311 (Adam Thierer & Clyde Wayne Crews Jr. eds., 2003) (stating that the recent U.S. enactments "reflect a much broader concept of privacy protection than previously recognized by U.S. law").

[127] *See* SOLOVE, *supra* note 113, at 67; Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-first Century*, 4 N.Y.U J. LEGIS. & PUB. POL'Y 439, 452-453 (2000-01).

[128] Beth Givens, *Privacy Expectations in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 347, 348 (2000).

[129] *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REVIEW 471 (1995) (exploring the content of substantive European standards).

[130] *See* Reidenberg, *supra* note 115, at 1331.

international agreements,[131] countries in the European region are under certain obligations, such as ensuring the respect for private and family life, home and correspondence (Art. 8 ECHR).[132] Specifically, in the digital context, there exist several international legal instruments relating to privacy and data protection with undeniable European origin or flavor. The 1980 Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[133] have been followed by the Ottawa *Ministerial Declaration on the Protection of Privacy on Global Networks* held in 1998.[134] The latter reaffirms the objectives set forth in the 1980 Privacy Guidelines and "the commitment to the protection of privacy on global networks in order to ensure the respect of important rights," and both texts come to set what has been called "technological neutral principles" for the protection of personal data at the international level.[135] The OECD, however, continues to stress the economic implications of data protection; that is, it focuses on individuals as "users" and "consumers" instead of treating them as "citizens".[136] A slightly different approach is found within the Council of Europe in which two important legal texts have been adopted: the 1980 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[137] and the 1999 Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on the Information Highways.[138]

Finally, the 1995 EC Directive on the protection of personal data[139] is the "world's most ambitious and far-reaching data privacy initiative of the high-technology era".[140] One distinctive feature of this piece of legislation is its extraterritorial effect, made effective through the data transfer ban of Art. 25, that prohibits the transfer of data to States that do not provide "an adequate level of protection" of personal information.[141] This was clearly a threat to data flows coming from the EU to the U.S., because European

---

[131] *See* Grewlich, *supra* note 82, at 280.
[132] *See* Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, October 4, 1950, art. 8, 5 E.T.S.
[133] Organization for Economic Cooperation and Development (OECD), Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, September 23, 1980, 20 *I.L.M.* 422 (1981), at http://www.oecd.org/document/18/0,2340,en_2649_34223_1815186_1_1_1_1,00.html.
[134] *See* OECD, Ministerial Declaration on The Protection of Privacy on Global Networks, October 7-9, 1998, Doc. DSTI/ICCP/REG(98)10/FINAL, at http://www.oecd.org/dataoecd/39/13/1840065.pdf.
[135] *See* Franda, *supra* note 98, at 165.
[136] *See* Reidenberg, *supra* note 115, at 1353.
[137] *See* Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 108 *E.T.S.*, 20 *I.L.M.* 377 (1981) (entered into force on October 1, 1985). Nevertheless, the U.S. is not a signatory of the Council of Europe Treaty.
[138] *See* Council of Europe, Committee of Ministers, Recommendation No. R (99) 5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet, Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on the Information Highways, 660th meeting, February 23, 1999.
[139] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 *O.J.* (L 281) 31, which has been partially superseded by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), *O.J.* (L 201) 37. *See* Aparna Viswanathan, *On Cookies That Don't Crumble: Will the Electronic Privacy Directive 2002 Make Cyberspace Safe?*, COMPUTER & TELECOMMUNICATIONS LAW REVIEW 63 (2003).
[140] Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, VAND. J. TRANSNAT'L L. 655 (2002). *See also* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L. J. 461 (2000) (stating that EU governments have moved aggressively to regulate the use of personal data).
[141] This ban would have prevail should the U.S. have challenged that measure within the WTO Dispute Settlement System under the GATS, *see* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 50-51 (2000).

officials deemed the U.S. legislation as not sufficiently protective of personal data.[142] With this Directive on Data Protection, the EU has set both the international standard and the agenda in this field for the years to come.

Some kind of understanding between the U.S. and the EU was therefore necessary in order to avoid disrupting data flows, and that is how the major international cooperation effort[143] to date with real effects in this area has been achieved by a Safe Harbor Agreement between the U.S. and the EU. As the EC Directive on Data Protection became effective in 1998 and its data transfer ban was immediately applicable, the Department of Commerce and the European Commission tried to reach some kind of common understanding on data protection. The U.S. proposal for a Safe Harbor Agreement was finally accepted after two years of negotiations by the European Commission in July 2000.[144] This Safe Harbor Agreement establishes core data privacy principles for the industry to follow. Those companies joining the Safe Harbor principles on privacy protection would be placed by the Department of Commerce on its web site list of certifying firms and, conversely, EC Member States would not challenge them or otherwise condition any data transfers to them.[145] Although some scholars consider this Safe Harbor Agreement as insufficient[146] or even a surrender act on the part of the EU,[147] it is nevertheless regarded as a "compromise through institutional development pursuant to which free transatlantic information flows may be preserved while satisfying legitimate EC concerns".[148] It seems, however, that this kind of negotiated settlement is not likely to serve as a permanent solution to the disparity between U.S. and European data privacy protection.[149]

From the International Law perspective, this Safe Harbor agreement is clearly not an International Treaty. It has not been signed nor ratified by the parties, and so it is not subject to the Vienna Convention on the Law of Treaties. At most, it could be maintained that this is a "Gentlemen's Agreement," or political agreement, but not even an "Executive Agreement".[150] Some scholars consider it as an example of a new kind of international regulation.[151] This Safe Harbor agreement would then be an example of a "soft-law", as opposed to a "hard-law" instrument, although regarding its effects it may very well achieve a *de facto*

---

[142]

[143] Some scholars still consider that a General Agreement on Information Privacy would be the best solution to attain international cooperation and harmonization in data protection. This treaty would need an institutional setting strong enough and the WTO would offer the best choice in that regard, *see* Reidenberg, *supra* note 115, at 1359-62.

[144] Commission Decision 2000/520/EC, of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce, 2000 *O.J.* (L 215) 7.

[145] *See* US Department of Commerce, Safe Harbor at www.export.gov/safeharbor (last visited October 5, 2005).

[146] *See* Joann M. Wakana, *The Future of Online Privacy: A Proposal for International Legislation*, 26 LOY. L.A. INT'L & COMP. L. REV. 151, 168 and 176 (2003) (stating that the Safe Harbor does not weigh consumer privacy concerns heavily enough and demanding a more active role for the U.S. government).

[147] *See* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 744 (2001) (arguing that the Safe Harbor poses a weakening of European standards) ; Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, Vand. J. Transnat'l L. 655, 681 (2000) (asking whether the U.S. is making real concessions with the Safe Harbor Agreement).

[148] *See* Gregory Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limites of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29, 58 (2002).

[149] *See* Fromholz, *supra* note 140, at 483.

[150] *See* ANTONIO CASSESE, INTERNATIONAL LAW 172 (2nd ed. 2005).

[151] *See* Perrit, *supra* note 46, at 940 (referring to this agreement as an example of international hybrid regimes involving public and self-regulation).

harmonization of data privacy protection. Compared to the intellectual property protection afforded by hard-law, i.e. International Treaties, it is again striking (or may be not) that Internet regulation in this area of data privacy rights has only been achieved by a soft-law instrument. Vigorous international cooperation in this field is necessary, but when business interests within the U.S are at stake,[152] even given support from the population, international legal texts with more teeth are difficult to achieve.

4. FUTURE ROLE OF INTERNATIONAL LAW ON THE REGULABILITY OF THE INTERNET

As we have seen, International Law has played the role of a catalyst between states, solving some issues that affect mainly e-commerce and that require cooperation, i.e. an international response articulated through the application of traditional doctrines of conflict of laws for the problem of free speech and content regulation, international treaties (international hard-law) for the protection of intellectual property rights, or some kind of Safe Harbor agreements (international soft-law) for the protection of privacy rights. International Law has yet another role to play with regard to the regulation of the Internet. International Law tools and institutions may answer some of the questions that have not been, or only timidly, been addressed to date. These questions are of an undisputed international flavor, and so only International Law can answer them. International Law should be ready to react mainly to the possibility of invoking self-defense in the case of a cyber-attack; the likelihood of considering the Internet as part of the Common Heritage of Mankind; and the prospect of regarding access to the Internet as an International Human Right.

4.1 THE USE OF FORCE AND SELF-DEFENSE IN CYBERSPACE

4.1.1 Introduction

As it is well known, the use of force between States is definitively forbidden in International Law since the advent of the U.N. Charter.[153] This prohibition is also a principle of customary International Law, as declared by the International Court of Justice in the *Nicaragua* case.[154] Nevertheless, there are two undisputed exceptions to this principle: the right of self-defense (Art. 51 of the U.N. Charter) and the collective action by the U.N. as decided by the Security Council (Art. 42 of the U.N. Charter). Other possible exceptions to this peremptory norm of International Law exist, but they are more disputed.[155]

The threat of a major attack to a State's Internet infrastructure is no doubt a primary question of national security. In the case of the North Atlantic Treaty Organization (NATO) strike against Yugoslavia, the Internet facilities existing in Belgrade were one of the military objectives specifically targeted by

---

[152] *See* Gellman, *supra* note 112, at 274 (arguing that there is no support in the U.S. business community to standardize privacy regulation).
[153] *See* U.N. CHARTER art. 2, para.4.
[154] *See* Military and Paramilitary Activities (Nicar. v. US), 1986 I.C.J. 14 (June 27). *See* MALCOLM N. SHAW, INTERNATIONAL LAW 91 (5th ed. 2003).
[155] *See* CASSESE, *supra* note 150, at 350.

NATO. An attack of this kind may easily be considered an armed attack, giving way to a response justified by self-defense. That military action also included "limited" computer warfare in what could be characterized as the "first cyber-war".[156] Apart from computer attacks in wartime, that is, governed by *ius in bello*, there is also the possibility of attacks in peacetime. What about an attack through viruses or otherwise directed to cause a major collapse in the functioning of a State's vital infrastructure? Does this kind of attack constitute a use of force in Cyberspace? Could it even be considered an armed attack? Will a State's reaction in the form of self-defense be justified? Could this self-defense reaction reasonably include the use of force? It seems that there is a need for answers based on International Law.

These sort of questions have already been posed by some scholars[157] who have foreseen the possibility of the Internet being used either as the battlefield of Century 21st (there are already possible enemies)[158] or as the preferred tool for terrorist action.[159] We will limit our analysis, though, to actions engaged in by states. The low-risk character of an Internet attack and the asymmetrical benefits that it offers to States (or non-state actors) which do not have the level of economic and military supremacy of developed states such as the U.S. makes it a very attractive tool.[160]

4.1.2 Computer Network Attacks (CNA) as Use of Force

From the point of view of International Law, the first question to be answered is whether or not a CNA can be considered a use of force, or even an armed attack. Before we try to develop any analysis, it would be good to bear in mind some previous assumptions. As we maintained before regarding the question of jurisdiction, location of the attack must be determined according to the "effects doctrine"; that is, what matters is not the physical location of the attacker but where the effects of the attack are felt.[161] Also, there is a broad spectrum of possible attacks, meaning not every CNA will meet the level comparable to a use of force. On the contrary, it would also be unreasonable to maintain that because a CNA does not physically destroy the object of the attack (although the effects are felt elsewhere), it can never amount to a use of force.[162] In order to illuminate this idea, we should consider some examples of possible computer attacks against vital interests like the New York Stock Exchange (NYSE), the NYC subway system or the U.S. Air Control System.

In this regard, it is clear that the prevailing interpretation of the Charter makes the prohibition of

---

[156] *See* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1081 (2000).
[157] *See* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 7 (1999); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense* STAN. J. INT'L L. 207, 208 (2002).
[158] *See* Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-attacks from China*, 17 AM. U. INT'L L. REV. 641 (2002).
[159] *See* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-attacks* U. ILL. J.L. TECH. & POL'Y 1, 12-13 (2002) (explaining how the permeability of cyberspace facilitates cyberterrorism and therefore makes cyberspace an attractive method for terrorists).
[160] *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 897 (1999).
[161] *See* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 286-287 (1996).
[162] *See* Jensen, *supra* note 157, at 222.

use of force applicable only to "military" force.[163] In the Nicaragua case, however, the ICJ affirmed that other activities, such as the arming and training of the Contras, were also prohibited.[164] So, it could be said that there are other activities also prohibited by Art 2 (4) even though they do not strictly consist of armed force, as long as they are "employed for the destruction of life and property".[165] In this vein, some scholars maintain that CNA's challenge the prevailing paradigm and have ventured that it should be possible to equate a CNA to a use of force, taking into account the results or consequences of the attack. If the attack causes physical destruction and human injury, then it could be considered a use of force prohibited by Art 2 (4).[166] As the ICJ stated, Art 51 does not refer to specific weapons.[167] There may even be some support for this interpretation in treaty law.[168]

This interpretation could be understood as a change in the normative construction of Art 2 (4)'s prohibition, which would focus not on whether or not the attack actually has an armed character (or amounts to strictly military action), but on the causation of similar damage.[169] This interpretive flexibility[170] may be justified in order to keep pace with the new technology. The problem that remains would be how to classify and clearly demarcate these attacks from those attacks not amounting to use of force.[171] As to the possible response to those other attacks that fall short of armed force, as the ICJ stated in the Nicaragua case,[172] the offended nation will only have recourse to countermeasures, limited by the applicable conditions as stated by the ICJ in the Gabcikovo case.[173]

4.1.3 CNA and Self-Defense

In the event of a CNA that could be equated to the use of force, then, as we know, there are only two possibilities. Either the Security Council decides to take collective action according to Chapter VII of the U.N. Charter, or, absent this reaction, the attacked state decides to make recourse to the right of self-defense. Art. 51 limits the right of self-defense to those situations where there is "armed attack", not merely use of force; nevertheless, the gap is not that big whenever a lethal result to human beings or serious destruction of property is engendered.[174] Therefore, it seems appropriate to include within the right of self-

---

[163] *See* Albrecht Randelzhofer, *Article 2(4)*, in THE CHARTER OF THE UNITED NATIONS. A COMMENTARY 106, 113 (Bruno Simma ed., 1994).
[164] *See* Military and Paramilitary Activities, *supra* note 154, at 119.
[165] IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (1963).
[166] *See* Schmitt, *supra* note 160, at 913 (arguing that "[A]rmed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused […] that computer network attack employs electrons to cause a result from which destruction or injury directly ensues is simply not relevant to characterization as armed force").
[167] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, 35 I.L.M. 809, 822 (1996).
[168] *See* Todd A. Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter* CASE W. RES. J. INT'L L. 591-592 (1998) (arguing that the analysis of information warfare as a weapons system is supported by the 1989 U.S.-U.R.S.S. Agreement on the Prevention of Dangerous Military Activities, whose Art. VI considers interference with command and control networks a "dangerous military activity").
[169] *See* Schmitt, *supra* note 160, at 914.
[170] *See* SHAW, *supra* note 154, at 843.
[171] *See* Schmitt, *supra* note 160, at 914 (offering criteria to distinguish between them according to their consequences).
[172] *See* Military and Paramilitary Activities, *supra* note 154, at 110.
[173] Gabcikobo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, 55-56 (Sep. 25).
[174] *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 100 (Schmitt & O'Donnell eds. 2002).

defense responses directed against a CNA constitutive of armed force as previously stated, that is, one provoking physical destruction and human injury.[175] Of course, the attacked State will have to comply with the requirements of self-defense, meaning the immediate response must be necessary and proportional[176] as well as subsidiary and provisional,[177] in addition to the obligation to report to the Security Council according to Art. 51. The question arises, then, whether the State attacked must react in the Internet field itself in order to comply with the proportionality requirement, in other words, with another CNA. It seems that, even if the response must be directed to halt and repel an attack, it is also clear that the defending state is not restricted to the same weapons used by the attacking state.[178] Furthermore, the defending state may not have the technological capacity and ability to defend itself in that particular field. For these reasons, an armed self-defense could be deemed appropriate in this case.

If the right to self-defense is available to States in this field, another important issue would be where and at what moment is it possible to invoke this right. If the Internet allows for instant lethal attacks that do no let State officials have much time to react, it would make no sense to speak of a self-defense response designed to repel and end the attack when this attack takes no more than a computer click to occur. In other words, the question here is whether it is even possible to talk about self-defense in the ultra-fast Internet field (that is, a late response may be considered a non-justified reaction because it is non-immediate, and thus a retaliation[179]) and, therefore, whether some kind of anticipatory self-defense would then be justified.

There seems to be some truth in the assertion that in the age of instant computer lethality, it makes no sense to speak about self-defense if this self-defense is not somehow anticipatory (there could be no point in taking defensive measures against a CNA that within seconds achieves its targets causing damages and death). In principle, anticipatory self-defense is ruled out by Art. 51 of the U.N. Charter, which requires an "armed attack" in order to exercise self-defense.[180] This has been a consistent state practice, established to avoid the risk of an abuse on the part of some states exercising wide discretion.[181] As some international lawyers have generally supported, under certain conditions, the doctrine of anticipatory self-defense,[182] or so called "interceptive" self-defense,[183] there are an equal number of scholars who defend its applicability to the Internet field. According to Sharp, the anticipatory right of self-defense should apply whenever there

---

[175] *See* Schmitt, *supra* note 160 at 929.
[176] *See* CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 120 (2nd ed. 2004) (stating that necessity and proportionality are requirements accepted by states since the 1837 Caroline incident).
[177] *See* NGUYEN QUOC DINH, PATRICK DAILLIER & ALAIN PELLET, DROIT INTERNATIONAL PUBLIC [PUBLIC INTERNATIONAL LAW] 901 (6th ed. 1999) (recalling that self-defense may be invoked and exercised until the Security Council gets involved and there is collective action).
[178] *See* GRAY, *supra* note 176, at 121.
[179] *But see* Dinstein, *supra* note 174, at 107-108 (considering "on-the-spot reaction" to CNA troublesome, and arguing in favor of armed reprisals at a different time and place as a legitimate response).
[180] *See* BROWNLIE, *supra* note 165, at 275-278 (1963); IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 700 (2003).
[181] *See* Albrecht Randelzhofer, *Article 51*, in THE CHARTER OF THE UNITED NATIONS. A COMMENTARY 661, 676 (Bruno Simma ed., 1994).
[182] *See e.g.* Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1634-1635 (1984); THOMAS M. FRANCK, RECOURSE TO FORCE, STATE ACTION AGAINST THREATS AND ARMED ATTACKS, 105 (2002); S. Schwebel, *Aggression, Intervention and Self-Defense*, 136 COLLECTED COURSES OF THE HAGUE ACADEMY OF INTERNATIONAL LAW 479-481 (1972-II).
[183] *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 172-173 (3rd ed. 2001).

is a "penetration of sensitive systems that are critical to a state's vital national interests".[184] Jensen is also in favor of a flexible anticipatory self-defense doctrine and supports legal measures listing or defining those critical infrastructures that should be defended even by active means.[185] Others, like Schmitt, are more cautious and provide some limited factors for the anticipatory self-defense to take place, but always within the framework of an overall armed attack and always by stressing that it is not the CNA but its context which should be used as the guiding principle.[186]

Bearing all these assertions in mind, it seems that, if CNA's cause damages similar to conventional uses of force, they should be considered uses of force, allowing for self-defense responses. Claims for an anticipatory right of self-defense in cyberspace should not, however, be accepted in principle. There is no reason at all to treat cyberspace attacks any differently from conventional armed force attacks or even nuclear missile attacks. In this sense, the Internet has not brought about any single innovation which should modify the traditional normative analysis of International Law on the use of force.

4.2 THE INTERNET AS A PART OF THE COMMON HERITAGE OF MANKIND

4.2.1 Introduction

The history of the Internet is an American history. Invented, funded and developed in the U.S.,[187] the Internet has an unquestionable American flavor when it comes to analyzing its features. As we have seen, freedom of information and free flows of data, as part of the First Amendment culture, are profoundly rooted characteristics of the Internet. They are part of its code. They are in fact the law of the Internet. Although there are recent efforts that try to change this state of things, as the judicial decisions reviewed above demonstrate,[188] it is still difficult to modify the current functioning of the Internet where there is a country, i.e. the U.S., that bluntly plays the major role in its governance. If we take the example of the domain name system, which is now run by the ICANN (Internet Corporation for Assigned Names and Numbers), we will see that, although the ICANN pretends to be a model of mixed or hybrid regulation[189] which should take into account the interests of all stakeholders, the truth is that the ICANN is an American private non-profit organization incorporated under Californian law, subject to U.S.' jurisdiction and authority, where commercial interests have a leading role,[190] but which on the other hand may violate

---

[184] *See* SHARP, *supra* note 157, at 129 (In fact his starting point is more wide-ranging as he affirms that all hostile intent constitute a threat to use of force which triggers the right to use force to respond in anticipatory self-defense *id.* at 95, but he seems to nuance his position in order to affirm the lawfulness of cyber espionage *id.* at 129).
[185] *See* Jensen, *supra* note 157, at 226-231.
[186] *See* Schmitt, *supra* note 160, at 932-933 (delimiting the three factors that may trigger anticipatory self-defense as "1) the CNA is part of an overall operation culminating in armed attack; 2) the CNA is a irrevocable step in an imminent (near-term) and probably unavoidable attack; and 3) the defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack").
[187] *See* Benkler, *supra* note 69, at 172.
[188] *See supra* note 72 and the parallel discussion in the main text.
[189] *See* Wolfgang Kleinwoechter, *From Self-governance to Public-private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources*, LOY. L.A. L. REV. 1103 (2003).
[190] *See* Jochen von Bernstorff, *Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of*

fundamental U.S. policies.[191] Other instances, such as the location of the main Internet root servers on U.S. soil[192] or the Digital Trademark Right provision of the Anticybersquatting Consumer Protection Act (ACPA) that allows a U.S. court to transfer a foreign registrant's domain name to the U.S. trademark owner despite of the Uniform Domain Name Dispute Resolution Policy (UDRP) of the ICANN,[193] are just the demonstration of this state of affairs.

Given this situation, we could pose the question of what would happen if some day the U.S. decided on its own to shut down the whole Internet for alleged national security reasons, if only because it has the ability to do so. What would be the grounds to contest that kind of decision? Is there any answer or any theory that could be opposed to such an act on the part of the U.S.? We may try here to develop a new way of thinking about the Internet provided by an international institution that has been left almost to oblivion for many years now, the Common Heritage of Mankind concept. In order to assess the applicability of this concept to the Internet, it would be good to analyze the origin and the elements that define this institution in International Law.

4.2.2 History

The Common Heritage of Mankind (CHM) concept first came up in regard to the Law of the Sea. This concept is generally attributed to Ambassador Arvid Pardo, Malta's U.N. representative, who proposed that the General Assembly declare the seabed and the ocean floor and its resources a "common heritage of mankind" and take the necessary steps to embody this basic principle in an internationally binding document.[194] Pardo's ideas were taken up by Part XI of the 1982 Law of the Sea Convention (LOS),[195] which provided in Art. 136 that the International Seabed Area "and its resources are the common heritage of mankind" and established an international regime (with an International Seabed Authority) to administer the access to and exploitation of the Seabed Area.[196]

As some scholars have pointed out, however, this concept had already appeared in the field of Outer Space and in the Antarctic Treaty, .[197] The General Assembly's "Declaration of Legal Principles

---

Hegemony, EUROPEAN LAW JOURNAL 511, 522 (2003).

[191] *See* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 27 (2000) (engaging in a thorough critical assessment of the creation of ICANN by the Department of Commerce).

[192] *See* Mayer, *supra* note 52, at 165.

[193] *See* Xuan-Thao N. Nguyen, *The Digital Trademark Right: A Troubling New Extraterritorial Reach of United States Law*, 81 N.C.L. Rev. 483, 547 (stating that "[p]otentially, if an ICANN panel ruled in favor of a foreign domain name registrant, the foreign nation will accept the panel's decision. On the other hand, if the trademark holder complainant in that case decided, after the unfavorable UDRP decision, to bring an ACPA action against the domain name, U.S. courts are not bound by the UDRP decision and could rule in favor of the trademark holder complainant").

[194] *See* Reservation Exclusively for Peaceful Purposes of the Sea-bed and of the Ocean Floor, and the Subsoil thereof, Underlying the High Seas Beyond the Limits of Present National Jurisdiction and the Use of Their Resources in the Interest of Mankind, U.N. Doc. A/6695 (1967).

[195] Third United Nations Conference on the Law of the Sea: Final Act, U.N. Doc. A/CONF. 62/121, Dec. 10, 1982; 21 I.L.M. 1245 (1982).

[196] *See* W. Michael Reisman, *The Common Heritage of Mankind: Success or Failure on International Regulation?*, CANADIAN COUNCIL OF INTERNATIONAL LAW 228, 233 (1985) (stating that "the Seabed Authority provisions of the Law of the Sea Treaty represent the most complete effort at implementing the core of Pardo's common heritage").

[197] *See* Stephen Gorove, *The Concept of "Common Heritage of Mankind": A Political, Moral or Legal Innovation?* 9 SAN DIEGO L. REV. 390, 391 (1971-1972); Mary Victoria White, *The Common Heritage of Mankind: An Assessment*, 14 CASE W. RES. J. INT'L L.

Governing the Activities of States in the Exploration and Use of Outer Space"[198], which referred to the "common interest of all mankind," was followed by the 1967 Outer Space Treaty,[199] which stated that exploration and use of outer space shall be "the province of all mankind" (Art. I). Later, the 1979 Moon Treaty, adopted by a General Assembly resolution,[200] became the first treaty in force to give effect to the CHM principle,[201] as it went into effect on July 11, 1984. Art. 11(1) of this treaty proclaims that "(t)he moon and its natural resources are the common heritage of mankind." The Antarctic Treaty[202] dates back to 1959, and although it does not refer expressly to the CHM, it has been widely seen as an international regime in which CHM elements are found.[203] Other examples where the CHM is deemed to be applicable are cultural and natural resources,[204] for which there is also an international convention,[205] as well as the environment,[206] although in this latter field the concept of Common Concern of Mankind is preferred.[207]

Initially, the U.S. was willing to apply the CHM principle to the deep seabed.[208] Also, because the result of the space race between the U.S. and the Soviet Union was uncertain, the U.S. wanted to have CHM elements inserted in the Outer Space Treaty.[209] Soon, however, this CHM was associated with a "socialist" type of claim on the part of developing states, and opposition from developed countries emerged.[210] Developed states pressed hard for the amendment of Part XI of the LOS Convention, which took place in 1994,[211] and introduced some important changes in the exploitation system previously devised (decision-making process and financial requirements), watering down the CHM features of the 1982 LOS Convention.[212]

4.2.3 Status and Elements of the CHM

509, 510 (1982) (presenting an account of the history of this principle).

[198] G.A. Res. 1962, 18 U.N. GAOR Supp. No. 15, at 15, U.N. Doc. A/5515 (1963).

[199] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, April 21, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

[200] G.A. Res. 34/68, U.N. GAOR, 34th Sess., Supp. No. 46, U.N. Doc. A/34/664 (1979). The Moon Treaty was opened for signature Dec. 18, 1979.

[201] *See* Harminderpal Singh Rana, *The "Common Heritage of Mankind" & the Final Frontier: A Revaluation of Values Constituting the International Legal Regime for Outer Space Activities*, 26 RUTGERS L.J. 225, 247 (1994).

[202] *See* The Antarctic Treaty, December 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 (entered into force June 23, 1961).

[203] *See* Eric Suy, *Antarctica: Common Heritage of Mankind?*, in THE ANTARCTIC ENVIRONMENT AND INTERNATIONAL LAW 93, 96 (Verhoeven, Sands & Bruce eds. 1992); Colin Diehl, *Antarctica: An International Laboratory*, 18 B.C. ENVTL. AFF. L. REV. 423 (1991).

[204] *See* Alexander-Charles Kiss, *La Notion de Patrimoine Commun de l'Humanite [The Notion of Common Heritage of Mankind]*, 175 COLLECTED COURSES OF THE HAGUE ACADEMY OF INTERNATIONAL LAW 99, 171 (1982) (asserting that this Convention establishes the CHM principle for cultural goods and natural resources even though they are located within a given State and so under its sovereignty).

[205] *See* Convention for the Protection of the World Cultural and Natural Heritage, November 16, 1972, 27.1 U.S.T. 37, 15511 U.N.T.S. 1037 (entered into force December 17, 1975).

[206] *See e.g.* Pemmaraju Sreenivasa Rao, *Environment as a Common Heritage of Mankind: a Policy Perspective*, in INTERNATIONAL LAW ON THE EVE OF THE TWENTY-FIRST CENTURY, VIEWS FROM THE INTERNATIONAL LAW COMMISSION 201 (United Nations ed. 1997).

[207] *See* PATRICIA W. BIRNIE & A. E. BOYLE, INTERNATIONAL LAW AND THE ENVIRONMENT, 143 (2002).

[208] *See* LOUIS HENKIN, LAW FOR THE SEA'S MINERAL RESOURCES 52 (1968).

[209] *See* BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 156 (1997); Stacey L. Lowder, *A State's International Legal Role: From the Earth to the Moon*, 7 TULSA J. COMP. & INT'L L. 253, 268 (1999); Julie A. Jiru, *Star Wars and Space Malls: When the Paint Chips Off a Treaty's Golden Handcuffs*, 42 S. TEXAS L. REV. 155, 162 (2000).

[210] *See* ANTONIO CASSESE, INTERNATIONAL LAW IN A DIVIDED WORLD 381 (1986).

[211] GA Res. 48/263, opened to signature on July 29, 1994. *See* D.H. Anderson, *Legal Implications of the Entry into force of the Convention on the Law of the Sea: A Redistribution of Competences between States and International Organizations in Relation to the Management of the International Commons*, 44 INT'L & COMP. L.Q. 313 (1995).

[212] *See* CASSESE, *supra* note 150, at 94.

Regarding the legal status of the CHM, it is difficult to ascertain whether the CHM constitutes a principle of international law, a theory, a doctrine, or just a political or philosophical concept. There has been much debate about the legal standing of the CHM, with many of the international law writers concluding that it may only be taken as a political challenge from developing countries so that "the CHM as a legal concept is dead"[213] and therefore "belongs to the realm of politics, philosophy or morality".[214] On the other hand, it is undeniable that the CHM is written in applicable international treaties[215] which have effectively prevented private enterprise from developed countries from starting to exploit CHM spaces until now.[216] Its legal status nowadays is far from being clear, because if in the 1980's it was progressively gaining momentum,[217] in the 1990's and the 2000's it is starting to be questioned again.[218] It may be too early to predict the success or failure of this concept.[219] We can, nevertheless, agree with Baslar that the CHM seems to be a concept rather than a principle of international law, although some of the elements of the CHM concept have become principles themselves.[220]

Since Pardo's proposal was presented, it has been understood that there are five elements incorporated into the CHM concept: a) the absence of a right of appropriation in CHM areas; b) common governance and management of CHM areas by international authority; c) the duty to exploit the resources in the interest of mankind in such a way as to benefit all, including developing countries; d) the obligation to explore and exploit for peaceful purposes only; and e) the duty to protect and preserve given resources for the benefit and interest of mankind and especially for future generations.[221] Even if there are pessimistic views on the actual possibilities of the CHM in current International Law,[222] it would be good for Internet governance to further at least some of the elements of the CHM. This is not a proposal based on natural-law-type norms,[223] but a *de lege ferenda* proposal which needs to be confirmed by state consent in the form of international treaties or otherwise.

---

[213] Bradley Larschan & Bonnie C. Brennan, *The Common Heritage of Mankind Principle in International Law*, 21 COLUM. J. TRANSNAT'L L. 305, 336 (1982).
[214] *See* Gorove, *supra* note 197, at 402.
[215] *See* Aldo Arnaldo Cocca, *The Common Heritage of Mankind: Doctrine and Principle of Space Law*, in 29 PROC. COLL. LAW OUTER SPACE 17, (1986) (speaking of positive international law).
[216] *Cf.* Brian M. Hoffstadt, *Moving the Heavens: Lunar Mining and the "Common Heritage of Mankind" in the Moon Treaty*, 42 UCLA L. REV. 575, 620-621 (1994).
[217] Joyner said in 1986 that the CHM was at most an "emergent principle of international law" -*see* Christopher C. Joyner, *Legal Implications of the Concept of the Common Heritage of Mankind*, 35 INT'L. & COMP. L.Q. 190, 199 (1986), whereas in 1998 he stated otherwise -*see* CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION (1998).
[218] *See* Stephan Hobe, *ILA Resolution 1/2002 with regard to the Common Heritage of Mankind Principle in the Moon Agreement*, 47 PROC. COLL. LAW OUTER SPACE 536 (2004) (arguing that, in the new international context of growing commercialization and privatization of space activities together with the 1994 amendment to the LOS Convention, the interpretation of the CHM has been modified and its equitable sharing element has been abandoned).
[219] *See* SHAW, *supra* note 154, at 454.
[220] *See* KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW, 2-3 (1998).
[221] *See e.g.* Jennifer Frakes, *The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?*, 21 WIS. INT'L L.J. 409, 411 (2003).
[222] *See* Carol R. Buxton, *Property in Outer Space: The Common Heritage of Mankind Principle vs. The "First in Time, First in Right" Rule of Property Law*, 69 J. AIR L. & COM. 689, 705-708 (2004).
[223] *But see* BASLAR, *supra* note 220, at 8 (stating that the CHM "is a moral philosophical idea acquiring its existence and legal normativity from, above all, natural law rather than state consent and auto-limitation [which] marks the end of positivist Westphalian international law").

4.2.4 CHM and the Internet

There is clearly a failure in the way the CHM was designed in the 1960's and 1970's. The use and exploitation of common resources like the Seabed, Outer Space and (maybe) Antarctica need important economic investments that can only be brought about by private companies. A free market approach combined with a regulatory umbrella may then be a sound solution for the current impasse,[224] with the U.N. playing a central role.[225] The Internet does not need such a push towards a market-oriented approach, because it is already a private-led field. On the contrary, it may be useful to have recourse to some of the traditional CHM elements to try to develop an international regime for common governance of the Internet. For this purpose, we consider that the CHM is a functional rather than a territorial concept,[226] so that it is theoretically possible to extend it to this particular field. Support to this interpretation may also be found in the 1984 Declaration of Buenos Aires on Transborder Data Flow, where Latin American countries considered informatics as "Mankind's Heritage".

First, the "non-appropriation" principle may not be the most crucial element to be applied to the CHM proposal for the Internet if we consider the decentralized nature of cyberspace. The Internet is nowhere and everywhere, so it may be said that no state has command and control of the Internet. However, we have already seen that the Internet is run according to U.S.-established parameters, where the private enterprise leads and ultimately the U.S. government can exercise authority over the technical body called ICANN.

Even if this wasn't true, there would be every reason to try to set up a coordinated system for "international Internet governance".[227] The Declaration of Principles of the World Summit on the Information Society has just called for an "[e]nabling environment" (Principle no. 6) where "[t]he international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations".[228] The Working Group on Internet Governance (WGIG) set up by the Secretary-General of the U.N. according to the aforementioned Declaration of Principles has recently handed out its first report in which it identifies, as the first group of public policy issues relevant to internet governance, those "relating to the infrastructure and the management of critical Internet resources, including the administration of the domain name system and Internet protocols and addresses (IP addresses), administration of the root server system, technical standards, etc.".[229]

---

[224] *See* Lynn M. Fountain, *Creating Momentum in Space: Ending the Paralysis produced by the "Common Heritage of Mankind" Doctrine*, 35 CONN. L. REV. 1753, 1774 (2003).
[225] *See* Rana, *supra* note 201, at 234.
[226] *See* BASLAR, *supra* note 220, at 91.
[227] *See* Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 7.
[228] *Id.* at 6.
[229] *See* Report from the Working Group on Internet Governance, World Summit on the Information Society, Geneva 2003-Tunis 2005, at 4, Doc. WSIS-II/PC-3/DOC/5-E (stating, in regard to the administration of the root zone files and system, that there is a unilateral control by the United States Government).

In the Internet field, therefore, there are vital resources that should be considered, not the property or the invention of a given state (even if it is so for historical reasons), but the common heritage or common concern of mankind. Even if the U.S. does not want to give up its current control over the technical and physical features of the Internet,[230] it may nevertheless agree to declare the Internet as a CHM resource. Ultimately, the non-appropriation principle does not necessarily have to apply to every CHM resource, as is evident in the cultural[231] and environmental[232] fields, for the concept to be useful and applicable.

Second, it follows from the above explanation that the CHM element relative to "common management" is fully applicable to the CHM proposal for the Internet. The only question would be how to articulate this common management, and what would be the appropriate body or forum, existing or to be construed, for this coordinated governance. The WGIG has proposed four different models, ranging from the creation of a strong international body called Global Internet Council with widespread competences which would take over the functions currently performed by the Department of Commerce of the U.S. Government, to the simple enhancement of the ICANN's Governmental Advisory Committee.[233] In any case, the WGIG recommends that any such body or forum should be linked to the U.N. and that no single government should have a pre-eminent role.[234]

The third element, the "benefits sharing" element of the CHM proposal for the Internet, relates to the same problem already addressed by the CHM concept that came up in the field of the Law of the Sea and Outer Space Law, that is, development or access to resources by developing countries. In this case, however, there are no physical resources to be exploited (i.e. minerals), but the benefits from the Internet Society flow from the very existence of an enabling infrastructure and connectivity capacity, which are lacking in many developing countries. The World Summit on the Information Society has therefore taken up the "commitment to build a people-centred, inclusive and development-oriented Information Society".[235] In other words, "the benefits of the information technology revolution are today unevenly distributed between the developed and developing countries," and so the objective becomes "turning this digital divide into a digital opportunity for all".[236] In this vein, Principle no. 11 of the Declaration of Principles, named "International and Regional Cooperation," calls for a commitment to the "Digital Solidarity Agenda" set forth in the Plan of Action and to the goals contained in the Millennium Declaration.[237]

---

[230] *See* John Markoff, *Overseer of Net Addresses Ends Dispute With Verisign*, N.Y.TIMES, October 25, 2005 at www.nytimes.com/2005/10/25/technology/25internet.html?th=&emc=th (stating that the US government has recently said that it no longer plans to give over control of ICANN to an international organization); Tomas Delclos, *EEUU Avisa de que no Cedera el Control Tecnico de Internet [The US Warns that it Will not Give Up its Technical Control Over the Internet]*, EL PAIS, October 29, 2005 at www.elpais.es/articulo/elpporsoc/20051029elpepisoc_7/Tes.

[231] *See* Kiss, *supra* note 204, at 231 (distinguishing between CHM by "nature" and CHM by "affectation", as in the case of cultural goods, the second case implying that the CHM concept applies even if the actual good is under a given state sovereignty).

[232] *See* BASLAR, *supra* note 220, at 279 and 287 (admitting that, where environmental resources like global commons are located in the territory of one state, this state would be under an obligation of custody, as a trustee, in which case the non-appropriation principle does not apply and so it would be better to talk about the Common Concern of Mankind as an alternative concept).

[233] *See* Report from the Working Group on Internet Governance, *supra* note 229, at 12-13.

[234] *Id.* at 10.

[235] *See* Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 1.

[236] *Id.* at 2.

[237] *Id.* at 8.

The fourth element relative to the "peaceful use" of the CHM also makes sense in the Internet context.[238] Information and telecommunications technologies and Internet infrastructure should serve to promote education, knowledge, information and communication. Governments should therefore cooperate in order to avoid any kind of warfare using the Internet as a possible, even an easy battlefield,[239] and they should also cooperate to prevent terrorist uses of the Internet.[240]

The final element, regarding the "preservation" of the CHM resources may not be applicable to a CHM proposal for the Internet, because the resources are not exhaustible in the same sense they are with the Seabed, Outer Space or Antarctica resources. It may apply only if we consider the Internet Network as a precious infrastructure that has to be preserved from other kind of dangers, such as attacks or purported blackouts through viruses, but again those are not related to the exhaustion of a given resource.

As we have seen, the elements of the CHM concept apply very well to the Internet. The Internet is a global resource that should not be appropriated by any single state, should be subject to a common management system, be managed for the benefit of all mankind (paying due regard to the developing countries needs),[241] and be used for peaceful purposes only. Nevertheless, the concept of the CHM has not even been mentioned to date by writers or representatives at the World Summit on the Information Society. Maybe this concept still evokes the socialist type of claims presented by Pardo, so that it would be better not to use it while trying to negotiate with the U.S. to give up to its control over the Internet. Maybe it is better to talk about the CHM in relation to the Internet once an international Internet governance regime designed along the lines of the CHM concept is already in place.

4.3 ACCESS TO THE INTERNET AS A HUMAN RIGHT

4.3.1 Introduction

Freedom of expression plays an important role in the political and legal analysis of the Internet.[242] Indeed, "the Internet has been conceptualized as a forum for free expression with near limitless potential for individuals to express themselves and to access the expression of others".[243] Even if this is an overstatement, scholars vividly debate the best way to establish conditions allowing each citizen to exercise meaningfully his or her right to freedom of expression.[244] Against the Net libertarian school, which contends that it is the privatization of speech forums that best advances the free speech values on the

---

[238] *But see* BASLAR, *supra* note 220, at 106 (asserting that this CHM element is applicable only if a territorial, instead of functional, concept of the CHM is sustained).
[239] *See* above Section 4.1.
[240] *See* Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 5 (Principle no. 5 on "building confidence and security in the use of ICTs").
[241] *But see* Section 4.3.3 *infra*.
[242] *See* the Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 1 (recalling Art. 19 of the Universal Declaration of Human Rights and stating that communication is a fundamental social process).
[243] *See* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace* 20 BERKELEY TECH. L.J. 1115 (2005).
[244] *Id.* at 1144.

Internet,[245] the school defending an affirmative conception of the First Amendment requires the government's involvement in the market for free speech in order to incorporate certain collective values.[246] This latter conception of the First Amendment finds judicial expression in the development of the "public forum doctrine". Under this doctrine, U.S. courts impose on the government the affirmative obligation to make public facilities available for persons wanting to exercise their free speech rights.[247] Nevertheless, the failure to act on the part of the courts or the legislature has led to a situation in which the Internet has become transformed by privatization into a group of privately-owned and privately-regulated places, where scrutiny under the First Amendment is absent.[248] Increasingly, the ability to produce speech is only open to large scale producers of content who are also owners of the physical network,[249] which undermines the very idea of a free market of ideas and meaningful freedom of expression.[250]

As it is well known, freedom of expression is internationally protected by the International Bill of Rights, i.e. the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights (ICCPR); and the International Covenant on Economic, Social and Cultural Rights (CESR).[251] Specifically, Art 19 (1) and (2) of the ICCPR guarantees an individual the right to hold opinions and a right to freedom of expression without interference. On the other hand, Arts 19 (3) (a), (b) and 20 of the ICCPR provide for exceptions to freedom of expression based on public order or the rights of others.[252] Of course, the Internet is not any different from the real world in this regard either, and since very un-democratic governments "seek to control the content of information to which their citizens are exposed or are imparting over the Internet, individuals around the world are experiencing human rights violations".[253] This should be, then, a primary issue of concern for international lawyers, and the existing international mechanisms for the protection and enforcement of freedom of expression should be fully applied and exhausted in the Internet field to the same extent.

To start, in order to enjoy meaningful freedom of expression, connectivity to the Internet network becomes a prerequisite. As stated by principle No. 2 of the Declaration of Principles of the World Summit on the Information Society, "connectivity is a central enabling agent in building the Information Society".[254] Telecommunications and the Internet therefore have the potential to ensure, not only the right to inform and the right to communicate, but also to ensure the economic, educational and social parity

---

[245] *See, e.g.* Richard A. Epstein, *Cybertrespass* 70 U. CHI. L. REV. 73 (2003).
[246] *See* CASS SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH 18 (1993).
[247] *See, e.g.* Richard A. Posner, *Free Speech in an Economic Perspective* 20 SUFFOLK U. L. REV. 1, 52 (1986).
[248] *See* Nunziato, *supra* note 243, at 1151 (arguing that this situation is also due to the U.S. Supreme Court decision holding that Internet access provided by public libraries does not constitute a public forum).
[249] *See* Dean Colby, *Conceptualizing the "Digital Divide": Closing the "Gap" by Creating a Postmodern Network that Distributes the Productive Power of Speech* 6 COMM. L. & POL'Y 123 (2001) (stating that the end-user is increasingly less capable of creating content to "push" onto the network).
[250] *Cf.* CASS SUNSTEIN, REPUBLIC.COM 153 (2001).
[251] Universal Declaration of Human Rights, G.A. Res. 217 A(III), U.N. Doc. A/180 (1948), at 71; International Covenant on Civil and Political Rights, December 19, 1966, G.A. Res. 2200 (XXI), U.N. GAOR 21st Sess., Supp. No. 16 at 52, U.N. Doc. A/6316, 999 U.N.T.S. at 171; International Covenant on Economic, Social and Cultural Rights, December 16, 1966, G.A. Res. 2200A(XXI), 993 U.N.T.S. at 3.
[252] *See* the discussion *supra* Section 3.1 on harmful content.
[253] *See* Antoine L. Collins, *Caging the Bird Does not Cage the Song: How the International Covenant on Civil and Political Rights Fails to Protect Free Expression over the Internet* 21 J. MARSHALL J. COMPUTER & INFO. L. 371, 388 (2003).
[254] *See* the Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 3.

necessary to attain equality for each member of society.[255] Countries that do not provide access for their citizens to telecommunications services will generate a world were citizens are denied many benefits of basic and advanced communications, including healthcare, education and economic opportunities, and the increased ability to participate in the political process.[256] The fact is that to date not everyone has the ability to seek, receive, and impart information and ideas through the Internet, and as a result, an important segment of the world population misses out on the political, economic, and social opportunities offered by the digital revolution.[257] In short, what we have today is the actualization of information "haves" and "have-nots," in other words, a "digital divide".[258] The digital divide is found both at the domestic level[259] and at the international level.[260]

4.3.2. Human Rights and the First Digital Divide

Is there something close to a right to be online? Is there a right to Internet access or even a right to communicate? Are these the proper subject for human rights law?

From the point of view of International Law, the question arises whether access to the Internet, universal access, as an issue related to connectivity rather than freedom of expression, can then be articulated as a human right, as a right every human being has. In this regard, out of the economic, social, and cultural rights established in the CESCR of 1966, cultural rights initially seem to more adequately incorporate the right to Internet access. Under Art 15 of the CESCR, cultural rights contain the following rights: the right to take part in cultural life, the right to enjoy the benefits of scientific progress and its applications, the right to benefit from the protection of the moral and the material interests resulting from any scientific, literary or artistic production of which the beneficiary is the author, and the freedom indispensable for scientific research and creative activity.[261] Alternatively, this right of access may form part of the right to education, protected by Art's. 13 and 14.

If we turn to the practice of States, developed countries, such as the U.S. and the EU, have adopted and implemented legal regimes incorporating universal service obligations in an effort to achieve the goal of increased access to the Internet and telecommunications services in general. The concept of universal

---

[255] *See* Patricia M. Worthy, *Racial Minorities and the Quest to Narrow the Digital Divide: Redefining the Concept of "Universal Service"* 26 HASTINGS COMM. & EN. L.J. 1, 3 (2003).
[256] *See* Jennifer A. Manner, *Achieving the goal of Universal Access to Telecommunications Services Globally* 13 COMMLAW CONSPECTUS 85, 86 (2004); Mark N. Cooper, *Inequality in the Digital Society: Why the Digital Divide Deserves All the Attention it Gets* 20 CARDOZO ARTS & ENT. L.J. 73 (2002) (demonstrating that the digital divide is likely to persist).
[257] *See* Peter K. Yu, *Symposium - Bridging the Digital Divide: Equality in the Information Age. Introduction* 20 CARDOZO ARTS & ENT. L.J. 1, 2 (2002).
[258] *See* Markenzy Lapointe, *Universal Service and the Digital Revolution: Beyond the Telecommunications Act of 1996* 25 RUTGERS COMPUTER & TECH. L.J. 61, 80 (speaking of the risk of "information apartheid"); Patricia F. First & Yolanda Y. Hart, *Access to Cyberspace: The New Issue in Educational Justice* 31 J.L. & Educ. 385, 403 (2002) (arguing that existing civil rights in the U.S. can be applied by those affected by the digital divide to achieve access to cyberspace).
[259] *See* KAREN MOSSBERGER *ET AL.*, VIRTUAL INEQUALITY. BEYOND THE DIGITAL DIVIDE (2003); RANETA LAWSON MACK, THE DIGITAL DIVIDE (2001).
[260] Nate Brennaman, *G8's Dotforce Initiative: Bridiging the Digital Divide or Widening it?* 11 MINN. J. GLOBAL TRADE 311 (2002); J.M. Spectar, *Bridging the Global Digital Divide: Frameworks For Access and the World Wireless Web* 26 N.C. J. INT'L L. & COM. REG. 57 (2000).
[261] *See* Asbjorn Eide, *Economic, Social and Cultural Rights as Human Rights*, in ECONOMIC, SOCIAL AND CULTURAL RIGHTS 32 (A. Eide, C. Krause & A. Rosas eds., 1995).

service is commonly attributed to Theodore Vail, president of AT&T, who used it in 1907[262] and generally refers to a public policy initiative designed to provide widespread access to telecommunications services.[263] The deregulation process that affected monopolies in telecommunications services in the 1990's, like those implemented through the Telecommunications Act of 1996 in the U.S. and the EU Directives on market liberalization,[264] was accompanied by the enactment of universal service obligations.[265]

In short, the universal service program provides subsidies to high-cost regions to ensure affordable telecommunications services in these areas. The universal service system has been criticized on several fronts,[266] but even if it has to be modified,[267] it seems clear that the universal service concept has socio-economic justifications and ultimately "is principally about politics", which therefore makes it highly unlikely that it can simply be retired.[268] It is said that the universal service concept should embrace not only the provisioning of network access, but also of personal computers to low-income families, just as telephone sets were traditionally provided as part of basic telephone service.[269] Even if the content of universal service is not completely clear, this regime has to some extent created some rights for individuals,[270] although they do not seem to fit very well into the currently existing human rights framework.[271]

While it would be possible to include the right to Internet access among the cultural rights internationally protected, however, there is the question of the underdeveloped justiciability of these rights due to the wording of these provisions and the relatively weak international monitoring mechanism set up by the Covenant.[272] Despite the efforts deployed by some scholars in order to confer them a true legal value,[273] there is also a pragmatic approach advanced by other authors under which those rights remain to

---

[262] *See, e.g.* Mark Young, *The Future of Universal Service. Does it have One?* 13 INT'L J. L. & TECH. 188, 189 (2005).
[263] *See* Worthy, *supra* note 255, at 54 (arguing that the 1996 Telecommunications Act retain a functional, and therefore evolving, concept of universal service, which may include access to the Internet, that has not been taken up by the FCC yet). The EU has adopted also a functional notion of the universal service concept, *see* Art 4 (2) Universal Service Directive (2002).
[264] *See, e.g.* William P. Cassidy, *Universal Service in a Competitive Telecommunications Environment: The Current State of Universal Service in the European Union and the United States* 25 N.C. J. INT'L L. & COMM. REG. 107, 117 (1999-2000).
[265] *See* ANTONIO SEGURA SERRANO, EL INTERES GENERAL Y EL COMERCIO DE SERVICIOS [GENERAL INTEREST AND TRADE IN SERVICES] 194 (2003).
[266] *See, e.g.* Stuart Buck, *TELRIC vs. Universal Service: A Takings Violation?*, 56 FED. COMM. L.J. 1, 3 (stating that the universal service system obliges the common carrier to offer its wholesale access at cost, while it must still sell its retail services to all customers at an average price that ignores costs, which could drive the utilities to the point of insolvency); James B. Speta, *Deregulating Telecommunications in Internet Time* 61 WASH. & LEE L. REV. 1063 (2004) (arguing that the 1996 Act should have taken additional steps to create conditions of competition).
[267] *See* Allen S. Hammond, IV, *Universal Service: Problems, Solutions, and Responsive Policies* 57 FED. COMM. LAW J. 187, 197 (2005) (arguing that in order to sustain the universal service a revision of the current system to provide for equitable contribution from all platforms is needed).
[268] *See* Young, *supra* note 262, at 191, 203 (arguing that the concept of universal service relies on the idea that telecommunications services are so essential to social activity that everyone should have access to a basic level of communication facilities and services, to ensure that they are able to participate as citizens in modern society).
[269] *See* Worthy, *supra* note 255, at 55-56.
[270] *See* Wolf Sauter, *Universal Service Obligations and the Emergence of Citizens' Rights in European Telecommunications Liberalization*, in PUBLIC SERVICES AND CITIZENSHIP IN EUROPEAN LAW, PUBLIC AND LABOUR LAW PERSPECTIVES 117, 118 (M. Freedland & S. Sciarra eds., 1998).
[271] *See* Cosmo Graham, *Human Rights and the Privatisation of Public Utilities and Essential Services*, in PRIVATISATION AND HUMAN RIGHT IN THE AGE OF GLOBALISATION 33, 56 (K. De Feyter & F. Gomez Isa eds., 2005) (noting the problems of enforcing positive obligations and enforcing these obligations against private bodies).
[272] *See* Phillip Alston, *No Right to Complain About Being Poor: The Need for an Optional Protocol to the Economic Rights Covenant*, in THE FUTURE OF HUMAN RIGHTS PROTECTION IN A CHANGING WORLD 86-88 (A. Eide & J. Helgesen eds., 1991).
[273] *See* Phillip Alston & G. Quinn, *The Nature and Scope of States Parties' Obligations under the International Covenant on Economic, Social and Cultural Rights*, 9 HUM. RTS. Q. 156, 164 (1987); G.J.H. van Hoof, *The Legal Nature of Economic, Social and*

be concretized only within a given economic and social context.[274] So when Secretary General of the ITU refers to the "right to communicate"[275] it seems that he does so in political terms, because a generally accepted public notion in international law of such a right has not so far emerged.[276]

4.3.3. Human Rights and the Second Digital Divide

There is another digital divide along the lines of the North-South development's fracture. Developed countries account for more than eighty percent of the world market for information technology, while Internet penetration is very limited in sub-Saharan Africa, the Middle East, Latin America, and South Asia.[277] Accordingly, the World Summit on the Information Society has called in Principle No. 11 of the Declaration of Principles for a "Digital Solidarity Agenda" which will contribute to "bridge the digital divide".[278]

The right to development, interpreted in the light of today's Internet role, could possibly be invoked in order to include a right of universal access. The right to development was first recognized by the UN Commission on Human Rights in 1977 and was also explicitly adopted by the General Assembly in the 1986 Declaration on the Right to Development.[279] It has been described as a right to solidarity among third generation rights[280] based on natural law,[281] and related to the New International Economic Order[282] (NIEO).[283] The content of this right is then "unusually open-ended and indeterminate", which nevertheless should be considered as a strength that gives the concept the "degree of flexibility" needed in this area.[284] The question remains, however, as to whether this right to development has achieved a sufficient degree of legal status, taking into account the important disagreement still existing with respect to the issues related to the content and the subject of this right (the individual or the collective).[285]

Certainly, there have been some voices pointing to some kind of resources transfer in order to

---

Cultural Rights: A Rebuttal of Some Traditional Views, in THE RIGHT TO FOOD 97 (P. Alston & K. Tomasevski eds., 1984); Phillip Alston, *Out of the Abyss: The Challenges Confronting the New U.N. Committee on Economic, Social and Cultural Rights*, 9 HUM. RTS. Q. 332, 360 (1987).

[274] *See* MARY DOWELL-JONES, CONTEXTUALISING THE INTERNATIONAL COVENANT ON ECONOMIC, SOCIAL AND CULTURAL RIGHTS: ASSESING THE ECONOMIC DEFICIT 8 (2004).

[275] ITU, Press Release, "ITU World Telecommunication Development Conference adopts Valletta Action Plan with series of bold measures to improve access to telecommunications worldwide", ITU/98-16 1. April 1998, at 5.

[276] *See* GREWLICH, *supra* note 82, at 84.

[277] *See* Yu, *supra* note 257, at 4.

[278] *See* the Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 8.

[279] Declaration on the Right to Development, adopted December 4, 1986, G.A. Res. 41/128 (1986) (Annex), UN GAOR, 41st Sess, Supp. No. 53, at 186, UN Doc. A/41/53 (1987).

[280] *See* Karel Vasak, *Pour Une Troisieme Generation des Droits de l'Homme [For a Third Generation of Human Rights]*, in STUDIES AND ESSAYS ON INTERNATIONAL HUMANITARIAN LAW AND RED CROSS PRINCIPLES IN HONOUR OF JEAN PICTET 837, 840 (C. Swinarski ed., 1984).

[281] *See* Mohammed Bedjaoui, *The Right to Development*, in INTERNATIONAL LAW: ACHIEVEMENTS AND PROSPECTS 1177, 1182 (M. Bedjaoui ed., 1991).

[282] *See* UN Declaration on Establishment of NIEO, G.A. Res. 3201, U.N. GAOR, S-VI, Supp. No. 1, at 3, U.N. Doc. A/9559 (1974), 13 I.L.M. 715 (1974).

[283] *See* Georges Abi-Saab, *The Legal Formulation of a Right to Development*, THE RIGHT TO DEVELOPMENT AT THE INTERNATIONAL LEVEL, WORKSHOP, THE HAGUE 159, 166 (R.-J. Dupuy ed., 1980).

[284] *See* Phillip Alston, *Revitalising United Nations Work on Human Rights Development*, 18 MELBOURNE UNIVERSITY LAW REVIEW 216, 221 (1991).

[285] *See* Phillip Alston, *People's Rights: Their Rise and Fall*, in PEOPLE'S RIGHTS 259, 284-286 (P. Alston ed. 2001).

close the gap between the North and the South in this field. For example, within the United Nations Educational Scientific and Cultural Organization (UNESCO) it has been asserted that "every citizen in the world should have the right to meaningful participation in the Information Society" because "information technology is by its very nature a human right, ought to be regarded as an obvious human right, and ranks alongside the concept of human liberty itself," calling for a "global governance" of cyberspace "that is not driven by interest."[286] Some scholars, however, have warned that this kind of speech may have the effect of riskily reproducing the power struggle represented by the New World Information and Communications Order (NWICO), centered along the lines of the NIEO that led to the U.S. withdrawal from UNESCO.[287] So what are developing countries doing today? Are they claiming a kind of expanded right to development in order to ensure telecommunications and Internet access to their populations? Not at all, as they seem to embrace Western policies such as competition and deregulation, fostered in the telecommunications field by the Fourth GATS Protocol entered into force in 1998 in order to gain access to cyberspace for their citizens.

Legal regimes based on universal service obligations, which as we have seen have been articulated in developed countries, are probably not suitable models for developing countries because those regimes build on the existence of an extensive infrastructure and are based on a funding mechanism which could not realistically be used in these countries.[288] As a result, developing countries are implementing a less resource intensive model of increasing access to telecommunications service not surprisingly called "universal access". Instead of aiming to provide for a telephone in each home, the goal of the universal access is to provide each citizen access to telecommunications services, without regard to geography, on an affordable basis. There are three key components in this universal access policy: a strong political support from the government; a stable regulatory regime that encourages competition in the log term; and a realistic financing plan for universal access policy.[289] This kind of regime allows developing countries to be able to ensure that people can obtain communications services through a competitive model without having to subsidize substantial infrastructure required by the universal service system, as demonstrated by some countries like Jamaica, Senegal, Ghana and others.[290] This is probably the concept of universal access retained by the World Summit on the Information Society.[291]

It seems, therefore, that the right of Internet access can hardly be deemed incorporated into any of the already established rights protected by the International Covenants or the right to development. This means that, as supporters of a progressive agenda, we would have to encourage such a development, while

---

[286] *See* Ms Vigdis Finnbogadottir's Closing Speech, Info-Ethics 98, at www.unesco.org/webworld/infoethics_2/eng/closing_remarks.htm.
[287] *See* Spectar, *supra* note 260, at 80 and 90.
[288] *See* Manner, *supra* note 256, at 86.
[289] ITU, Global Symposium for Regulators, Universal Access Regulatory Best Practice Guidelines, December 8-9, 2003, at www.itu.int/ITU-D/treg/Events/Seminars/2003/GSR/Documents/BestPractices_E_31.pdf.
[290] *See* Manner, *supra* note 256, at 90 and 103.
[291] *See* the Declaration of Principles of the World Summit on the Information Society, *supra* note 1, at 3-4 ("Universal, ubiquitous, equitable and affordable access to ICT infrastructure and services, constitutes one of the challenges of the Information Society and should be an objective of all stakeholders involved in building it. [In order to achieve this goal] policies that create a favourable climate for stability, predictability and fair competition at all levels should be developed and implemented").

waiting to see when, if ever, this ever more important access to the Internet is deemed a right by states and other international actors, using the traditional law-making avenues existing in International Law or otherwise.[292] In the meantime, states should incorporate the World Summit on the Information Society principle on universal access as an essential policy consideration or principle for action.

5. CONCLUSIONS

[292] *See* Phillip Alston, *Conjuring Up New Human Rights: A Proposal for Quality Control*, 78 AM. J. INT'L L. 607, 620 (1984) (proposing procedural requirements to be met for the new human rights to be recognized).