The Internet and the Persistence Of Law

Justin Hughes
Benjamin N. Cardozo School of Law
Yeshiva University

Boston College Conference on Intellectual Property, E-Commerce and the Internet

OCTOBER 18-19 2002 Boston

The Internet and the Persistence Of Law

Justin Hughes *

INTRODUCTION

* Justin Hughes is Assistant Professor of Law, Cardozo School of Law, Yeshiva University, and the 2003 Hosier Distinguished Visiting Chair in Intellectual Property at DePaul College of Law, Chicago. My thanks to Kenneth Roost, Stuart Reimer, and Susan Berkowitz for assistance for this manuscript; my thanks to Andrew McLaughlin, Fred Yen, and all the participants of the Boston College Conference on Intellectual Property, E-Commerce, and the Internet for helpful comments and a lively conversation on this paper. The remaining errors are the exclusive intellectual property of the author.

Whether the advent of radio or the rise (or fall) of the Soviet Union, any momentous social development tends to trigger a wave of enthusiastic observations about the way the new world will be. The Internet was no exception. First generation commentary about the Internet was often so extreme as to make one thankful to be among second generation commentators. That includes much of the initial analysis, predictions, and prescriptions on how law and cyberspace would interact. In scholarly pursuits as in military maneuvers, those in the vanguard bear both the pleasure of arriving first and the danger of becoming cannon fodder.

In the short lifetime of cyberspace, at least three broad kinds of stories have already been told about how law and the Internet will interact. These three distinct meta-visions of the relationship between the Internet and law are discussed in Part II: the *no-law Internet*, the *Internet as separate jurisdiction*, and Internet law as *translation*. In the no-law Internet story, cyberspace is fundamentally inhospitable to traditional law as a mechanism of control. Laws that serve entrenched interests simply will not stick to cyberspace – whether it is censorship by the Singaporean government or copyright enforcement by Bertelsman. In the second vision, what I will call the "kingdom" of the Internet or the Internet as a jurisdiction, cyberspace is both amenable to and in need of some kind of laws. But the same technological characteristics that make cyberspace resistant to traditional laws of traditional sovereigns lead to another conclusion: that cyberspace should be its own jurisdiction.

The third kind of narrative is less vision and more a practical program of *translation*: finding legal tools to reach roughly the same balance of interests in the Internet that we have developed for the rest of our world. Perhaps one can think of the Internet as an Atlantis-like continent that has risen from the sea, been promptly populated, and now needs sufficient order to make sure the inhabitants don't hurt one another -- or the people on other continents – too much. The new region is now undergoing a program of "colonization": lawyers, legislators, and lobbyists have moved quickly to extend familiar laws and regimes into the new territory.

The pace of this colonization has been staggering: CDA, COPA, CIPA, DMCA, UETA, ACPA, E-Sign, UCITA are only the American acronymic peaks of a vast range of legislative proposals and enactments. In California, the *state* legislature saw 258 net-related bills introduced in its 1999-2000 session, up from four bills in 1994.[1]

Because the initial wave of immigrants to cyberspace were overwhelmingly American – both natural and juridical persons -- novel legal issues about the Internet have usually been tested first in American courts (although parallel fact patterns have quickly appeared in other countries). So, when American academics began paying attention to the Internet, it felt – despite the "global" rhetoric -- like a wholeheartedly American institution.[2] The initial wave of legal scholars drawn to the Internet were, on the whole, experts in American constitutional, criminal, commercial, and

---

1 THE INDUSTRY STANDARD, August 15, 2000.

2 Also causing, in some countries, the perception of the Internet as yet another American intrusion into local or national societies. *See, e.g.* ANDRÉ LUCAS, DROIT D'AUTEUR ET NUMÉRIQUE 7 (Litec, 1998) (noting the « a little polemical debate » in France over whether the Internet is a « vehicle for American thinking.")

copyright law. Scholars established in international or comparative law were a relative minority of the new cyberlaw gurus.

Even today, a novel cyberlaw problem is statistically likely to first arise in the U.S. or, more broadly, in a common law jurisdiction. Survey information for 2002 puts Americans at 42.65% of Internet traffic, dwarfing number two China (6.63%) and number three Japan (5.24%).[3] Adding Britain, Canada, and the U.S., a bare majority of Internet traffic is still common law, English-oriented (50.52%).[4] If American legal scholars have been too Americentric about the Internet (and there certainly have been exceptions), this is a good explanation for the myopia.

After the cyber-stock meltdown of 2000, it became the fashion of well-paid consultants to tell business people that "we're still in the early innings" of the Internet[5] – advice as true for the law. By one estimate, by as early as 2005, Americans will only be one quarter of all Internet users.[6] While the U.S. will remain the single largest, monolingual, legally-integrated economy on the Net, Americans are now, for day-to- day purposes, like the largest shareholder in a vast corporation in which no one has majority control. [7]

This reality of the Internet means that the pragmatic project of translation is forcing express and implicit consideration of how national legal systems resolve the same or similar problems differently. One way or another, these differences have to be overcome -- or not allowed to arise in the first place. The result is that the Internet is producing and will continue to produce a significant amount of convergence of legal systems. Recently, in discussing intellectual property, French commentators Michel and Agnès Maffre-Baugé have made similar observation. Noting that there is an inherent tension or conflict between private entities that want to circulate themselves or their good widely through the Net and nation-states which still rely on territoriality, Vivant and Maffre-Baugé conclude:

> This gives an indispensable characteristic to the adoption of rules that are convergent, if not common, whenever possible. In truth, this means of harmonization has, for a long time, been relied upon by States. But the 'Internet phenomenon' seems to make alternative formulae emerge which one will need to consider for a moment.[8]

---

3 *China second to US in web traffic: study*, available at www.smh.com.au/articles/2002/08/01/1028157806643.html.

4 A reader may quibble that much Canadian traffic is Quebecois and, therefore, French and civil law oriented. But this bare English majority does not include Australia, New Zealand, Singapore, Ireland, Kenya, Nigeria, India or South Africa [the last four being common law countries with English being the vastly dominant language of Internet users].

5 Amy Harmon, *An Internet Guru's Lexicon*, THE NEW YORK TIMES, May 13, 2001 at 14, col, 6.

6 Michael Pastore, *Global Internet Population Moves Away from US*, Jan. 11, 2001, at http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_558061,00.html.

7 *See, generally* MILTON L. MUELLER, RULING THE ROOT (2002) (describing development of ICANN and political control issues surrounding "the root" control space for domain names, hence order on the Net).

8 Michel Vivant et Agnes Maffre-Bauge, *Internet et la propriété intellectuelle: le droit, l'information et les réseaux*, LES NOTES DE L'IFRI 59 (Institut français des relations internationals, Paris, June 2002). *See also*

Indeed, there are both different ways to think about this convergence and different ways this convergence is occurring.

As to how to think of this convergence, one way is that we are seeing the emergence of new international or *transnational* legal norms to which nation-states and domestic legal systems increasingly adhere.[9] Another way to think about this convergence is that the project of translation is gradually returning us to a vision of the Internet as its own separate jurisdiction. Quite a few commentators saw the parallel to *lex mercatoria,* which transcended national commercial laws to create what we might now think of as a virtual jurisdiction among transnational merchants.[10] But Part II also argues that some visions of the Internet as its own jurisdiction have tended to see the Internet as more separate and distinct from the rest of reality than it is. Because the Internet is weaving itself increasingly into our daily, meatspace lives, the comparison to *lex mercatoria* is inadequate. Part II offers some ruminations on how we might think of this *distinct* jurisdiction which is not so *separate.*

Whatever metaphors we employ, the convergence of legal norms being produced or prompted by the Internet is remarkable and remarkably fast-paced. Part III presents a simple attempt at a taxonomy of how legal norms governing the Internet are emerging. This taxonomy is only a tentative proposal, an outline of a framework that may help people understand the nature of emerging Internet law. Such a framework, as presented here or as more thoroughly developed, might also help activists understand how to contribute more effectively to the formation of legal principles related to the Internet.

The taxonomy set in Part III presents four types of "convergence" of law. The first is the creation of multilateral treaty regimes to which nations and domestic legal systems adhere. In this *top-down convergence*, private lobbying focuses on the international organs which produce the treaty. Development of the legal norms is, at least in the final stages, fairly transparent. The WIPO copyright treaties are a successful example of top-down convergence. The negotiations over a possible Hague Convention on jurisdiction offer another example of this kind of legal norm formation. Arguably, American legal scholars are most conscious of, and the most involved in this kind of convergence.

The second means to convergence is *model-based* or *soft law convergence*. Instead of a treaty regime, an international model emerges and domestic legal systems gradually adopt the standards, if not literal legal language, of the international model. Part III discusses how the Uniform Dispute Resolution Policy for the <.com> top level domain has become the preeminent

---

Lucas, *supra* note __ at 13 (recognizing that a comparative law approach is necessary to the minimal harmonization of law needed on the Internet).

9 Jeremy Betham introduced the notion of "international law" as a more rigorous concept than "law of nations." *See* JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION 296 (1789) (Burns & Hart, eds. 1970). Philip Jessup recommended replacing Bentham's concept with a broader concept of "transnational law." PHILIP C. JESSUP, TRANSNATIONAL LAW 1 (1956).

10 I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1051 – 1053 (1994) (drawing parallel to lex mercatoria); David R. Johnson and David G. Post, *Law And Borders -- The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, _____ (1996) (same).

model for such convergence, while UNCITRAL's model laws for electronic contracting have been less successful.

Part III then turns to a third kind of convergence: emergence of legal norms without the intervention of diplomats and bureaucrats working internationally. In this *invisible hand* or *parallelism convergence*, market forces produce a limited range of options for each economy: either adopt law within X range or forego the economic potential of the Internet. Two examples discussed in Part III are internet service provider liability and baseline rules on electronic contracting.

Part III also takes up a fourth are of convergence which is really no convergence at all. The most obvious area of law where the Internet is unlikely to produce substantial harmonization of legal norms in the medium term is freedom of expression. Canada and many European countries permit restrictions on speech that are antithetical to Americans; China and Saudi Arabia impose restrictions that would be wholly unacceptable to Europeans.

Characteristics of each model can be found in almost any area where the Internet is bringing pressure for development of the law. And there are many areas of law that may yet gravitate toward one model or the other. A few of these are briefly discussed in Part IV. And the details of reality, of course, spill over the edges of any taxonomy. As I said earlier, this is a first suggestion for a taxonomy of how Internet law is developing. It is intended to further, not fulfill, a conversation about this topic. As Robert Nozick reminded us at the beginning of his own intellectual journeys, "[t]here is room for words on subjects other than the last word."[11]

II. COMPETING VISIONS OF THE INTERNET'S LAW AND THE CASE FOR CONVERGENCE

At a meta-level, there have been at least three distinct visions of the relationship between the Internet and law: what I will call the *no-law*, *separate jurisdiction*, and *translation* visions of Internet law. Perhaps only the first two deserve to be called "visions." The third is more an ongoing "project" – a practical mission taken up in piecemeal fashion by practitioners and policy makers. "Cyberlaw" 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. Ultimately, this project of translation is returning us to seeing the Internet as a special jurisdiction. But not as a hermetically-sealed jurisdiction; the Internet is a jurisdiction whose legal norms will increasingly overshadow divergent national legel norms. If anything, this raises the stakes for each nation-state in the development of the Internet legal norms.

A. The no-law Internet

The first vision of the Internet and law was simple: never the twain should meet. The Internet was the brave new world in which law would be both unneeded and unworkable. Visions of a no-law Internet came in different flavors – conservative, leftist, utopian, anarchical – but they

---

11 ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA xii (1974).

were all founded on a determinism in which, as Reg Whitacker noted, technology became "the autonomous engine of history."[12]

This determinism was built on a surprisingly fixed understanding of the Internet's technology. This too was understandable in the milieu of the moment. Early cyberphilia treated the Internet as the *end* of History: claims like "[c]yberspace is Platonism as a working product"[13] and "[t]he Net wires the world for Hegelian *Geist*"[14] came from the mouths of early prognosticators. As Julian Stallabrass has noted, "the Hegelianism of the cyberphiles" was not a dialectic of thesis, antithesis, and synthesis, but "[ra]ther, is a fixed state in which the end of history and the total realization of mind is achieved."[15] Some legal commentators were understandable drawn in this heady, but static vision.

The ingredients of the vision started with the Internet's basis distribution characteristics – almost frictionless, almost instanteous, very decentralized, and with information flowing from and through different nodes – made geography seem irrelevant.[16] But miminal relevance of geography for distribution purposes was combined with at least two other basic ingredients of the Y2K Internet. One was the amount of information in relation to humans and their institutions. As Post and Johnson wrote, "[t]he volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to the government authorities to permit meaningful control."[17] That conclusion depended on a particular understanding of the technology that still seems correct, but is and will be challenged.[18]

Another basic characteristic was anonymity. Of course, this anonymity seemed ubiquitous because fairly primitive technology – written words on a glowing screen instead of the human voice or visage. E-mail from someone/something other than who the author purported to be became a device in the plots of Broadway shows, motion pictures, and television programs. The anonymous characteristics of the Internet will ebb and flow as anonymizer and identifier technology duke it out, with broadband and webcams lurking on the edges of the Net's presently text-based world.

An Internet without law was an understandable first response to this amazing non-geography of the Internet. In James Boyle's apt description of this view, "[t]he state is too big, too

---

12 REG WHITACKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 47 (1999).

13 Michael Heim, *The Erotic Ontology of Cyberspace*, in BENEDIKT, ED. CYBERSPACE, FIRST STEPS 64 (1991).

14 MARK C. TAYLOR AND ESA SAARINEN, IMAGOLOGIES: MEDIA PHILOSOPHY (1994), "Simcult" at 3.

15 Julian Stallabrass, *Empowering Technology: The Exploration of Cyberspace*, 211 NEW LEFT REVIEW 3, 9 (1995).

16 As one American judge characterized the Internet in 1997, "The Internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps 'no there there,' the 'there' is everywhere where there is Internet access." Judge Nancy Gertner, Digital Equipment Corp. v. Altavsita Technology, Inc. 1997

17 Johnson and Post, *Law and Borders, supra* note ___ at ___. (same).

18 For example, "Packetshaper" software promises real time analysis and discrimination based on protocol, application, URL, etc. *See* < http://www.packeteer.com/products/packetshaper/index.cfm >. Developments in artifical intelligence must further undermine the assumption that government eyes and ears cannot be everywhere.

slow, too geographically and technically limited to regulate a global citizenry's fleeting interactions over [this] mercurial medium."[19] If the rise of modern law depended, as Henry Maine observed, on a definition of political belonging based on "topographical limits,"[20] then a cyberworld which had no territory, no topographical limits would be inhospitable to both the enforcement mechanisms and analytic tools of modern law. Examples of the former include any number of attempts to censor the Internet with firewalls. An example of the latter is Martin Redish's suggestion in 1998 that the ubiquitious nature of the Internet made the old jurisdictional tools irrelevant[21] -- a conclusion that any number of courts, compelled by real cases and zero legislative guidance, blissfully ignored.

One can still find evidence to support the notion that the Internet is inhospitable to the mechanisms of modern law. For example, Australia has a law by which the Australian Broadcast Authority receives complaints about materials on the web, reviews those materials pursuant to pornography/obscenity standards applied to broadcasts, and send "takedown" orders when it find what it deems to be inappropriate materials hosted on Australian sites.

There is much about the Australian law that appears wrong-headed – starting with the application of broadcast, not print, standards for pornography to the Internet. But looking beyond those substantive questions, the law serves as a wonderful example of the sovereign's ineffectiveness in controlling the Net. During the second six months of 2000, the ABA handled complaints directed at prohibited materials on 139 sites.[22] Of these, only 6 were hosted in Australia and subject to the ABA's take-down notices. As to the other 136 sites, information from the complaints was forwarded to software filtering companies[23] and to the Australian federal police, but there is no evidence of any attempt to prosecute the foreign sites in Australia. The Australian experience comports with the remark made in the summer of 2002 by a deputy minister in the Iranian Ministry of Culture of Islamic Guidance that, "control has no meaning for the Internet."[24]

---

19 James Boyle, *Foucault in Cyberspace*, 66 U. CINCINNATI L. REV. 177, ___ (1997); a version of this paper is available at www.duke.edu/boylesite/foucault.htm. Boyle's message in this excellent article is that the "info-libertarians should not be so quick to write off the state," a prognosis that has proved amply correct.

20 SIR HENRY MAINE, ANCIENT LAW (New York, 1864) 124 - 126.

21 *See e.g.*, Martin H. Redish, *Of New Wine and Old Bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution*, 38 Jurimetrics J. 575, 605-606 (1998) (". . . the technologicial development of the Internet effectively renders the concept of purposeful availment both conceptually incoherent and pratically irrelevant. An individual or entity may so easily and quickly reach the entire world with its message that it is simply not helpful to inquire whether, in taking such action, that individual or entity has consciously and carefully made the decision either to affiliate with the forum state or seek to acquire its benefits.")

22 AUSTRALIAN BROADCASTING AUTHORITY, SIX MONTH REPORT ON CO-REGULATORY SCHEME FOR INTERNET CONTENT REGULATION JULY TO DECEMBER 2000, released 19 April 2001. Greg Taylor, *Regulatory Failure: Australia's Internet Censorship Regime*, Electronic Frontier Australia, 5 May 2001, available at <www.efa.org.au/Analysis/aba_analysis.html.>

23 Taylor, *supra* note __ at 4 ("The report indicates that the ABA is spending over 95% of its effort on complaints about overseas sites that are then referred to filtering companies. This represents a government subsidy to a largely US-based industry that is probably already well ahead of the government anyway.")

24 Nazila Fathi, *Taboo Surfing: Click Here for Iran . . .* , NEW YORK TIMES, August 4, 2002, at 5, col. 1.

But the descriptive account on which the no-law Internet is founded suffers from two shortcomings. The first was the naivete of its technological determinism. One doesn't have to be against determinism to be skeptical of human omniscience. If we know anything about the flow of technology, it is that it goes back and forth, moves in unexpected directions, detours into niches and eddies that few would have anticipated. This is true for centuries of military technology[25] and all our recent experience with communication technologies.[26] The image of a "continuing race of offensive and defensive technologies" on the Internet[27] is metaphorical to some and very real to other, but in either case, it's a race for which it may be foolish to expect a final "winner."

The second shortcoming was a more basic and fundamental incompleteness in the non-law Internet narrative. This was a certain myopia about the nature of the Internet's connection to meatspace. The culture of computer scientists is not one with much familiarity with the instruments of state power. Whatever their geekishness, early Netizens were people who paid their taxes, didn't commit felonies in physical space, and, often, lived deep within institutions (universities, corporations, foundations) where *other people* took care of compliance with law. The early idealism overlooked that while the material of the Internet could move from server to server across borders to evade the law, the people who controlled the servers – *or were identifiably responsible for the content* – could not. Usually those people have mortgages, bank accounts, and dinner plans for Saturday night.

If efforts to go after offending websites will merely drive them or their material off-shore, a very different situation applies to Internet Service Providers, telecoms, and cybercafes. An effective enforcement state mechanism does not have to touch *all* actors as long as it touches actors who can impact everyone else's behavior. The obvious strategy, as James Boyle noted years ago, was to "seek out private actors involved in providing Net services who are not quite as mobile as the flitting and frequently anonymous inhabitants of cyberspace."[28] So, China, known for its "great firewall of China" approach to censorship, is increasingly turning toward control of ISPs and cybercafes. In 2002, China began promoting "self discipline pacts" with ISPs by which the ISPs agree to ban not just illegal content, but content "harmful to national security and social stability."[29]

And while it is certainly more efficient to go after larger infrastructure entities, it is also certainly possible for the sovereign to do nasty things to individual cybernauts whose corporeal bodies remain on the sovereign's side of the computer screen. The 2002 Chinese crackdown on cybercafes has included the installation of software that records attempts by café users to access

---

25 *See e.g.* WILLIAM M. MCBRIDE, TECHNOLOGICAL CHANGE IN THE UNITED STATES NAVY, 1865 - 1945 (2000).

26 When broadcast television was introduced it was easy to predict that the flow of technology was against small cultures, sub-cultures, and minority points of view. Cable television and rising disposable income undid these dire, technology-based predictions; the market for audiovisual works continues to fragment and differentiate as it becomes possible to deliver more and more channels into each home. In 1965, technology seemed to render publishing in small languages (Dutch, Danish, Swahili, Bambara, etc.) an economic dead-end, but the advent of desktop publishing technology seemed to undo some or all of those economic disadvantages.

27 Erik Eckholm, *Taboo Surfing: . . And Here for China* , NEW YORK TIMES, August 4, 2002, at 5, col. 4.

28 Boyle, *supra* note at __.

29 *China announces 'self-discipline' scheme for Internet providers*, Yahoo! News, Friday, July 5, 2002, 12:18pm, available at <sg.news.yahoo.com/020705/1/308mo.html>. last visited August 6, 2002.

banned sites.[30] In 1997, we saw headlines when Germany prosecuted the head of CompuServ's German subsidiary on pornography charges stemming from Internet traffic.[31] Five years later, a 40 year old former policeman, Li Dawei, became the first individual Chinese citizen sentenced to prison for downloading from the Internet materials deemed politically unacceptable.[32]

B. The kingdom of the Internet

Back in theory mode, if one travels down the path that traditional "law" cannot apply to the Internet, one faces a fork in the road. Either one envisions the Internet as an anarchical environment *or* one imagines the establishment of order – including non-legal rules – through principles of self-organization or consensus mechanisms *or technology*. As to the latter, a series of commentators from the mid-1990s onward -- M. Ethan Katsh, William Mitchell, Larry Lessig, and Joel Reidenberg[33]– reminded everyone that in cyberspace software code is law -- or a form of restraint as good or better than law. The software code was written by someone, even if they did not write it with Tibetan dissidents, Napster, and billions of bizarre webpages in mind. It could be rewritten.

As to self-organization, consensus, and new forms of law, David Post and David Johnson have been perhaps the two most eloquent commentators for this vision of the Internet.[34] In this view, self-organization is seen as the mechanism by which a variety of communities will emerge with different governing contractual structures and individuals being free to move among such communities[35] – a vision very much akin to the self-ordered libertarian world of varied communities put forward in *Anarchy, State, and Utopia*.

---

30 *Id.*; Eckholm, *supra* note ___.

31 Gunnar Bender, *Bavaria v. Felix Somm: The Pornography Conviction of the Former CompusServe Manager*, INT, J. OF COMM. LAW AND POLICY, available at http://www.digital-law.net/IJCLP/1_1998/ijclp_webdoc_14_1_1998.html. Edmund L. Andrews, *CompuServ Unit Chief is Indicted in Germany*, INT'L HERALD TRIBUNE, April 17, 1997, at 13.

32 *China jails politically incorrect Net user for 11 years*, YAHOO! ASIA TECH, August 6, 2002, available at http://asia.tech.yahoo.com/020806/reuters/asia-118939-tech.html, last visited August 7, 2002; *China jails politically incorrect Net user for 11 years*, THE MERCURY NEWS online, posted on August 5, 2002, available at <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3803541.htm>, last visited August 7, 2002.

33 WILLIAM MITCHELL, CITY OF BITS (MIT Press, 1995); M. Ethan Katsch, *Software Worlds and the First Amendment: Virtual Doorkeepers in* Cyberspace, 1996 U. CHI. LEGAL F. 335; Lawrence Lessig, *Reading the Constitution in* Cyberspace, 45 EMORY L. J. 869, 896 – 97 (1996); Joel Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911 (1996); Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

34 *See* David G. Post & David. R. Johnson, *"Chaos Prevailing on Every Continent": Toward a New Theory of DeCentralized Decision-Making in Complex Systems*, 73 Chi.-Kent L. Rev. 1055 (1998); David R. Johnson, *Let's Let the Net Self-Regulate: The Case for Allowing Decentralized, Emergent Self-Ordering to Solve the "Public Policy" Problems Created by the Internet* (April 7, 2000) <http://www.cli.org/selford/essay.htm>; David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Virtues of Decentralized, Emergent Law* (April 7, 2000) ,www.cli.org/emdraft.html.

35 *See, e.g.* John O. McGinnis, *The Once and Future Property-Based Vision of the First Amendment*, 63 U. Chi. L. Rev. 63, 100 – 107 (1996); *see id.* At 102 (noting how, up until then, the Internet's "growth ha[d] been achieved with no guidance from the state and little regulation outside the enforcement of private order-

It is only a small step or series of steps from seeing the Internet has needing non-legal rules to seeing the Internet as needing some sort of legal rules, even if those rules were to be as radically different from existing law as "socialist law" had been (or proclaimed itself to be) a radical departure from established capitalist law. As Johnson and Post reasoned in 1996, the virtual world was separate from the "real world" and "[t]his new boundary defines a distinct Cyberspace that needs and can create new law and legal institutions of its own."[36] In other words, this was a vision of the Internet as its own jurisdiction, a kind of *kingdom of cyberspace* where we would have the chance to rethink law and implement rules that have greater clarity and rationality.

The pure vision of the Internet as its own jurisdiction with thoughtful, consensus-among-Net-user-developed rules was perhaps popular for only brief moment, but it still has significant echos, particularly when countries undertake organized, national efforts to look at the legal quandries created by the Internet.[37]

In retrospect, this vision suffered from seeing cyberspace as *too* separate from the "real world." In positing a consent-based, separate legal regime for the Internet, Johnson and Post made the pithy point that "[n]o one inadvertently strays across the border into Cyberspace."[38] But is that as true today as it was five years ago? The Internet is being woven into the rest of reality, technologically, socially, and economically. Technologically, as our appliances become "smart," our houses become "wired," our telephony is done with packet-switching, and our cable, telephone, and Internet service bundle and unbundle, will we know when we "crossed" some border?

And even if we did, should it matter? No one unknowingly strays into a phone call, but that does not mean that the wires and ether of telephone conversations should be their own jurisdiction separate from the rest of our lives. Economically, when General Motors places a multi-million dollar order with IBM over the Net, will either party want different contract law to apply to that transaction as distinct from the rest of their dealings? With thousands of its residents ordering consumer goods over the Internet, how long can a state ignore the lost tax revenue on the grounds that its citizens crossed into another jurisdiction?

Instead of being a hermeutically sealed world in which different economic models could be developed for everything from copyright to antitrust,[39] cyberspace was having significant real world effects: children were getting access to pornography that they otherwise could not get, political dissidents were able to get and give information they otherwise could not get and give, people were selling, trading, and giving away things – often things they did not have or did not have the

---

ing through contract."); Johnson and Post, *Law and Borders, supra* note ___ (meaningful 'exit options' from virtual communities mean that different communities could flourish with people free to move easily among them.)

36 David R. Johnson and David G. Post, *Law And Borders -- The Rise of Law in Cyberspace*, '48 STAN. L. REV. 1367, _____ (1996).

37 *See, e.g. South Africa: Delegates Disagree about Regulation of Laws*, AFRICA NEWS SERVICE, May 2, 2001 (describing South African national conference on e-commerce laws where some advocated "a few tweaks and twiddles to existing laws" and others sought "one new, all-embracing law covering every aspect of e-commerce") available at <http://allafrica.com/stories/200104230184.html> last visited August 6, 2002.

38 *Id.* at ___.

39 Johnson and Post, *Law and Borders, supra* note ___ at ___ and ____ (discussing antitrust and copyright models respectively).

authorization to sell or trade. It is not that the real world dashed the idealism of the cybernauts without provocation. It is that the effects of cyberspace first spilled over into meatspace. And reality bit back.

So, the utopian vision of a no-law Internet and the theoretical vision of a kingdom of cyberspace gave way to a very practical project: a project of *translating* real world laws, so that the balance they draw in the real world would be roughly replicated in cyberspace. Certainly some private entities have used the moment to try to shift the balance in their favor – this is how many scholars understand the Digital Millennium Copyright Act. But the publicly justifiable principle is, *at best,* one of *translation*, i.e. that existing instruments should be used when possible and existing 'balances' of interests should be preserved when possible.

I say "at best" because governments do not always intervene to transfer the existing balance of real world interests into cyberspace, a lesson that travel agents have learned very well. One of great promises of e-commerce is that it allows for "disintermediation" and "reintermediation," new ways to express the creative destruction of a market economy. Travel agents have found themselves increasingly disintermediated as consumers make travel arrangements on line, book hotel reservations, and buy airline tickets, either from the airlines or from the new information aggregators, i.e. <Travelocity.com> and <Orbitz.com>. Traditional auction houses have suffered at the hands of <e-Bay.com> and car dealers have barely slowed the automobile manufacturers from selling directly to the public. Why have these people gone unprotected from an Internet-drive "rebalancing" while intellectual property owners have been shielded in increasingly fortress-like statutes? The explanations range from good economic theory to raw public choice theory.

C. *Translation, convergence, and the Internet as a special kind of jurisdiction, not just a special jurisdiction*

If each country could colonize its own zone of the Internet, we have only the makings of interesting comparative law. But stuff on the [presently configured] Internet gives national boundaries the same deference as do migratory birds, viruses, and carbon gas emissions. As with all of those, regulating the stuff on the Net requires, in the words of the January 1999 U.S./U.K. joint statement on electronic commerce, "[c]ooperation among all countries . . .[to] . assist in the construction of a seamless environment for electronic commerce."[40] In other words, governments will have to accept a zone of harmonized Internet law that, at minimum, functions as an autonomous region within their legal system – just as the expectation of international merchants that *lex mercatoria* would govern their transactions could only develop where national governments willingly recognized *lex mercatoria* principles as governing such transactions.

But the question remains *how* this area can be autonomous from the rest of a nation's law. The vision of a separate continguous cybperspace jurisdiction does not adequately acknowledge how the Internet – e-commerce, e-communications, e-socialization – permeates each national society. Instead, the hackneyed metaphor of the information superhighway may help. The American interstate system penetrates and bisects 50 jurisdictions that retain their own road and

---

40 U.S.-U.K. JOINT STATEMENT ON ELECTRONIC COMMERCE, London, January 30, 1999.

driving laws; the interstate system is woven into those local road systems where local rules govern. Yet the interstate system imposes a wide range of uniformity on the conduct of those who use it; the interstate highway system is seamless – same construction, style of signs, same grades of ramps for ingress and egress, largely consistent speed limits, etc. The interstate functions much like a separate jurisdiction which is blended and completely integrated into each state's economic and social life.

As the internet penetrates each national society, we should expect that laws governing the internet will have more and more influence on laws governing behavior off the internet. For example, some people have noted that defamation law might be adjusted for the Internet environment to reflect the fact that a person defamed on the Internet has more opportunity/power to respond in kind. *If* that is true, as everyone becomes wired, why isn't that a justification to change *all* defamation law, i.e. a person defamed *off* the Internet will be able to use the Internet as a successful platform for response (because everyone reading the paper is also reading the Net). Does it really make sense, as the Internet permeates our lives, to have different online and offline laws for contract, consumer protection, defamation, or trademark infringement? Sometimes perhaps, but as a general rule, no.

If this is correct, the pressure to produce a set of convergent or harmonized legal norms to govern behavior in the jurisdiction of the Internet is a pressure to produce new legal norms that will wear away at older, differing legal norms in each national system.

II. A TAXONOMY OF INTERNET LAW FORMATION

There are at least four ways legal norms are converging (or not) via the economic and social force of the Internet.

A. Top-Down Convergence: Treaty-Based Development of Legal Norms

The first of these is "top down" convergence in which a multilateral treaty is negotiated and countries are pressured to ratify, then implement, the new legal norms of the treaty regime. Perhaps the best example, to date, of top down convergence of Internet-related laws has been the WIPO copyright treaties crafted in December 1996 – the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).[41]

The mind-1990s certainly had elements that pointed toward a "top down" solution to the new phenomenon of the Internet. The international bureaucratic community was flush with the successful negotiation and conclusion of the TRIPS Agreement and the Marrakesh Agreements as a

---

41 WIPO COPYRIGHT TREATY (WCT) (1996), WIPO Publication No. 227(E), AND WIPO PERFORMANCES AND PHONOGRAMS TREATY (WPPT) (1996), WIPO Publication No. 227(E), both adopted by the WIPO Diplomatic Conference on Certain Copyright and Neighboring Rights Questions in Geneva, on December 20, 1996. <http://www.wipo.int/treaties/ip/wct/> <http://www.wipo.int/treaties/ip/wppt/> respectively, last visited August 8, 2002.

whole. In the U.S. and the EU, there was a certain amount of public and private expertise [lobbyists] which had ramped up for the World Trade Organization (WTO) negotiations and now was in need of work.

As or more importantly, the TRIPS Agreement created a problem for the World Intellectual Property Organization (WIPO). WIPO administered the traditional, dominant multilateral intellectual property treaties [the Paris and Berne Conventions], but now found that TRIPS gave the WTO jurisdiction over the new generation of multilateral intellectual property obligations. One sure way for WIPO to reinvigorate its role would be a round of new, 21st century multilateral intellectual property obligations which were *not* integrated into TRIPS.

The WCT and WPPT clarified certain copyright issues that have become more important in the digitized, networked environment, but are principally intended to make three basic additions to international norms of copyright law. These three new legal of international copyright law are: (a) generalizing existing rights of distribution, broadcast, and public performance into a more generic rights to "make available to the public" or "communicat[e] to the public"; (b) creating obligations about the protection of "rights management information"; and (c) creating obligations vis-à-vis "technological measures" that copyright owners use to control who gets their works and how they are used.

The generalized right to make a work available -- or communicate a work -- to the public is intended to capture both how the Internet works and how future technologies for disseminating content might work.[42] In a sense, it is an admission that in the past copyright law has responded to technological developments in a piecemeal fashion and it would be better to establish a generalized characterization of the author's right to control dissemination of a work.

Top-down convergence is not simply a matter of writing a treaty and waiting for everyone to implement it. The troika of new copyright norms are drafted in sufficient generality that implementation of the norms quickly became an area of intense jockeying by interested parties.[43] Generalizing the author's right to control dissemination of the work was perhaps the easiest element of the two treaties because that norm is already expressed in most countries' copyright laws and/or can be re-expressed again and again with each new technology. The issue of rights

---

42 Article 6 of the WCT is captioned "Right of Distribution" and establishes a general "exclusive right of authorizing the making available to the public of the original and copies" of works; Article 8 of the WCT is captioned "Right of Communication to the Public" and establishes that authors shall enjoy an "exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their work in such a way that members of the public may access these works from a place and at a time individually chosen by them." This last phrase is intended to describe generally internet distribution and delivery, but the interconnection of the two Articles is clear in that Article 8 equates a "making available to the public" via wire or wireless means as a "communication to the public." The parallel provisions in the WPPT are Articles 8 and 10, respectively.

43 And properly so, not just for practical reasons, but because the content of international legal norms can depend on their interpretation and implementation by nation-states. *See* Vienna Convention on the Law of Treaties, art. 31(3)(b) (in interpreting a treaty, account shall be taken of "any subsequent practice in the application of the treaty which establishes the agreements of the parties regarding its interpretation"), opened for signature May 23, 1969, 1155 U.N.T.S. 331.

management information and the WCT/WPPT protection of "technological measures" have been far more contentious.

The treaties require signatories to provide "effective legal remedies against the circumvention of effective technological measures that are used in authors" in the exercise of their copyright rights.[44] In other words, legal remedies against "digital lock picks" that can be used to disrupt or circumvent encryption, scrabbling, watermarks, and passwords used by copyright owners to protect their works. These new copyright legal norms have been the subject of tremendous debate – even as to whether they are *copyright* legal norms to begin with.[45]

It became quickly clear to interested parties that the implementation of the new legal norms by the U.S., the EU, and Japan would determine the actual content of the norms. The provisions of the Digital Millennium Copyright Act and the EU Copyright Directive[46] on "technological measures" are sufficiently consistent that it would be difficult to argue against these as the 'content' of the WCT/WPPT legal norms,[47] although a few countries, like Burkina Faso and Australia, believe they can meet the treaty obligations with much less.

In the world of policy and law, negotiations of multilateral treaty obligations and their subsequent implementation are high profile affairs, so much so that they are sometimes seen as the sole means of harmonizing law. For example, one commentator looking at the Internet in 1998 concluded that "harmonization of legal standards is not a realistic solution to global information issues,"[48] citing only the eight years needed to negotiate the WTO Agreements. But there are other ways to skin a cat or produce a legal norm.

B. Model-Based Emergence of Legal Norms

In addition to the "hard law" model of multilateral treaty making, there is a "soft" form of top-down formation of Internet legal norms: the development in an international forum of a model law or set of principles which gain currency. An express, but not completely successful attempt at

---

44 Article 11 of the WCT; Article 18 of the WPPT.

45 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.18[A].

46 Directive 2001/29/EC of the European Parliament and the of the Council, 22 May 2001, available at http://www.eurorights.org/eudmca/CopyrightDirective.html

47 Implementation of the WCT/WPPT by the United States and the European Union may have wandered beyond the four squares of the norms established by the treaties. For example, Alain Strowel has noted that in implementing WCT Article 11, both the U.S. and the EU have established prohibitions on technological protection measures that attack controls on *access*, but "access" if it is a *right* of copyright holders has usually been a right protected by real property law [control of access to cinemas and concert halls, etc.], not copyright law. Alain Strowel, *Droit d'auteur et acces a l'information: de quelques malentendues et vrais problems a travers l'historie et les developments recents*, 12 LES CAHIERS DE PROPRIETE INTELLECTUELLE 185, 206 - 208 (1999) (". . .la partie la plus importante de cette reglementation concerne les measures touchant a l'acces, mais, en revance, a l'egard de ces measures, aucune obligations n'existe en vertu des Traites de l'OMPI" and observing that this might cause a divergence in norms).

48 Reidenberg, *supra* note ___ at 577.

this has been the 1996 UNCITRAL model law on electronic commerce.[49] A more subtle and successful example is the Uniform Dispute Resolution Policy (UDRP) for addressing "cybersquatting" disputes between domain name (DN) registrants and trademark holders.

The problem of cybersquatting arises when A controls a domain name that is substantially the same as a trademark controlled by B. Typically, A registered and/or maintains control of the DN with knowledge of its similarity to the trademark. If A simply warehouses the DN, it denies B an obvious -- sometimes the most obvious -- way to exploit his trademark on the Internet. Among other arguments, defenders of cybersquatters argued that a domain name is nothing more than an address on the Internet, not a communicative message. Although superficially appealing, this was *always* a bogus argument. A domain name of the form <http://www.paed.uscourts.gov> is not really an *address*: the actual address for the website of the U.S. district court for eastern Pennsylvania is http://204.170.64.143. As long as that court's website is hosted on the particular server where it is hosted, they have no choice in that numeric address – just as you have no choice in your street or road address if you want to live in the same house.

The domain name system creates memorable alphanumeric names which are overlaid upon and correspond to the actual Internet addresses. So, if you want an analogy to real world addresses, the better analogy is to the modern trend of corporate entities to give their buildings names like "One Chase Plaza" or "Trident Center. These "addresses" do not eliminate the numbered street addresses; they are simply overlaid on top. And if a "Trident Center" was renamed "One Coca-Cola Place" without the permission of the Coca-Cola Bottling Company, there would be a colorable trademark problem.

Courts have generally been unsympathetic to such cybersquatters, especially when the person offers the DN for a high price or diverts the trademark holder's (potential) customers. But to reach reasonable results, courts often stretched and distorted traditional trademark notions of unfair competition, initial interest confusion, and dilution.[50]

In 1999, WIPO produced a report at the behest of ICANN on how to handle DN/TM disputes in the gTLDs administered by ICANN. The report became the basis for the Uniform Domain Name Dispute Resolution Policy (*commonly abbreviated* UDRP), a mandatory, but non-binding arbitration procedure for any party that registers a domain name in the .com, .net, or .org

---

49 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), available at www.uncitral.org/english/texts/electcom/ml-ecomm.htm. (hereinafter UNCITRAL E-Commerce Model Law).

50 Sporty's Farm L.L.C. v. Sportsman's Mkt., 202 F.3 489, 497 (2d Cir. 2000) (the ACPA "was adopted specifically to provide courts with a preferable alternative to stretching federal dilution law when dealing with cybersquatting cases"); Porsche Cars North America v. Porsch.net, 4th Cir., August 23, 2002 (". . . the enactment of ACPA eliminated any need to force trademark dilution law beyond its traditional bounds in order to fill a past hole . . ."), available at http://laws.findlaw.com/4th/012028p.html.

environments.[51] Under the UDRP, a trademark holder can recover a DN in one of these gTLDs on a showing that:

+ that the DN is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
+ that the DN registrant has no rights or legitimate interests in respect of the domain name; and
+ that the DN has been registered and is being used in bad faith.[52]

The Policy then provides an elaborate, but non-exhaustive list of evidence for and against "bad faith" registration and use.[53]

Although the UDRP has suffered from occasionally questionable, inconsistent, and/or celebrity-solicitious decisions,[54] it is a powerful example of *lex Internet* through a model law. Originally drafted, promoted, and promulgated as being applicable only to three generic top level domains (gTLDs) - .com,.net, and .org -- the UDRP's principles have quickly been adopted for new generic TLDs[55] and, much more importantly, it become the basis for dispute resolution standards in at least 25 country TLDs (ccTLDs). Some, like Mexico, Venezuela, and Guatemala have adopted the actual UDRP mechanisms *and* arbitral institutions.[56] Some, like Japan and Singapore, have adopted the UDRP verbatim or almost verbatim.[57]

The United States has passed its own Anticybersquatting and Consumer Protection Act (ACPA) that wanders from the precise UDRP formula, but its nine factor test for bad faith hones

---

51 The Internet Corporation for Assigned Names and Numbers (ICANN),Uniform Domain Name Dispute Resolution Policy, posted September 29, 1999, available at http://www.icann.org/udrp/udrp-policy-29sept99.htm. (Hereinafter UDRP).

52 UDRP, Article 4(a)(i)-(iii).

53 UDRP, Article 4(b).

54 ANDRE R. BERTRAND, LE DROIT DES MARQUES, DES SIGNES DISTINCTIFS ET DES NOMS DE DOMAINE 578 - 583 (2002) (noting "the numerous contradictory decisions rendered on identical facts" ["les nombreuses décisions contradictoires rendues a propos de faits identiques."] and the very broad definition of "trademark" used by WIPO UDRP panels) (hereinafter, BERTRAND, NOMS DE DOMAINE); Laurence R. Helfer & Graeme Dinwoodie, *Designing Non-National Systems : The Case of the Uniform Domain Name Dispute Resolution Policy*, 43 WILLIAM AND MARY LAW REVIEW 141 (2002). *See also* Note, Ian L. Stewart, *The Best Laid Plans: How Unrestrained Arbitration Decisions Have Corrupted the Uniform Domain Name Resolution Policy*, 53 Fed. Comm. L. J. 509 (200X).

55 For example, Paragraph 4(a) of the Start-Up Trademark Opposition Policy '"STOP" for the .biz gTLD repeats the UDRP three part test.

56 BERTRAND, NOMS DE DOMAINE, *supra* note __ at 579 (also counting Romania, the Philippines, the Bahamas, and Cyprus as countries that have adopted UDRP arbitration at WIPO for their country TLDs.)

57 When Singapore adopted dispute resolution procedures to deal with claims of cybersquatting in the <.sg> space, the Singaporeans adopted ICANN=s Uniform Dispute Resolution Policy almost whole cloth, but added a distinct mediation procedure. *See*, SINGAPORE DOMAIN NAME DISPUTE RESOLUTION POLICY (Version 1 - 6 November 2001), available at < http://www.nic.net.sg/pdf/SDRP.pdf>. The Singaporeans did, however, add a mediation process; article 4(e) provides that the parties Awill be invited to consider whether they wish to the dispute mediated by the Administrative Panel before the Administrative Panel is called upon to decide the dispute,@ then sets out procedures for such mediation.

close to the UDRP's understanding of the conditions that should trigger a DN transfer.[58] Similarly, the dispute resolution policy of Nominet, the administrator of Britain's .uk TLD formulates its policy in terms of "abusive registration" of a domain name, but the non-exhaustive list of appropriate evidence on this question bears a strong resemblance to the UDRP and ACPA.[59] Even in France, which has not enacted any specific laws to address cybersquatting and cybersquatting decisions under its trademark law have been the subject of some controversy, the UDRP decisions are recognized as a "pertinent jurisprudential source" for deciding cases.[60]

The model effect can also strengthen the emerging international legal norms by affecting law at the *sub-national* level. A prime example of this are judiciary guidelines promulgated in August 2000 by the Beijing Higher People's Court.[61] These guidelines to judges – hence to lawyers and business people – state that "bad faith registration and preemption of other people's well-known trademarks are acts . . . to which the General Principles of the Civil Law and which the Unfair Competition Law Regulates."[62] The guidelines then integrate the UDRP standards. Article V provides:

> "To determine whether or not an act of domain name registration constitutes domain name registration in bad faith, the act shall be examined to determine whether or not it simultaneously meets the three necessary conditions as follows:
> (1) That the registered domain name is identical with or deceivingly similar to a representation owned by the rightholder thereof;
> (2) That the domain name holder does not enjoy any other priority right in the representation of said domain name; and
> (3) That the domain nam e is registered and used in bad faith."

Given the difficulty of translating western legal text into Chinese, this is clearly an effort to reflect the UDRP standards. Article V further sets out examples of subsection 3 bad faith which mimic those of the UDRP: offering the domain name for sale or other assignment to the trademark holder, inducing Internet users to visit the person's website for profit, creating deliberate confusion with the trademark, preventing someone else from "registering the trademark and business name as a domain name; or registering the domain name for the purpose of impairing another person's business good will."[63] All familiar types of bad faith conduct from the UDRP and its jurisprudence.

---

58 The ACPA has a non-exhaustive nine factor test, 15 U.S.C. § 1125(d)(1)(B)(i), which is very similar to the conditions of UDRP Article 4(a) and (b) together.

59 Nominet .uk, Dispute Resolution Service Policy, Articles 3 and 4, available at http://www.nominet.org.uk/ref/drs-policy.html.

60 BERTRAND, NOMS DE DOMAINE, *supra* note __ at 571 ("[L]es décisions rendues sous l'égide du Centre de médiation et d'arbitrage de l'OMPI apparaissent dans ce contexte comme une source jurisprudentielle pretinente au regard du droit français.")

61 Guidelines Set Forth for Hearing Cybersquatting Cases, issued by the Beijing Higher People's Court in August 2000, also translated as Guidelines for "Vicious Domain Name Registation." Available in English at www.cpahkltd.com/Newsletter/DomainCase.html.

62 *Id.* at Article IV.

63 *Id.* at Article V.

Thus, the UDRP has helped prevent development of inconsistent national standards for cybersquatting cases[64] -- something that was of such concern in the late 1990s that the Clinton Administration initially opposed the ACPA on the grounds that it would be a greenlight for other countries to write their own unique cybersquatting laws.

One could make a "tipping" argument that the dominance/importance of .com meant that as soon dispute principles were adopted in that gTLD everything would move in that direction. In sheer number of inhabitants, the .com environment dwarfs the next three TLDs combined (.de, .net, and .uk). Interestingly, the popularity of the <.com> TLD extends far beyond obvious groups (like companies that operate internationally [airlines], that market internationally [liquor brands], or that need to appear Internet savvy).[65] The allure of <.com> arises, in part, from perceived commercial advantage; as one domain name dispute arbitrator commented, "anyone with knowledge of domain name economics knows that common, generic , terms under the <.com> TLD are the best domains to have because they generate the most traffic."[66]

But such a "tipping" effect would not conceptually distinguish this from other situations in which model codes or laws are drafted at the international level and become carriers of new, dominant legal norms for the Internet. Given the amount of acknowledgement they received, the UNCITRAL rules on electronic contracting had the potential to do this, but have not had influence on the scale of the UDRP.[67] If the Hague Convention on Jurisdiction is unable to resolve its present impasse, jurisdictional rules for Internet-based transactions and interactions might be another place to start viable, modest model law proposals. One could imagine either (a) jurisdictional models on limited areas of law and/or (b) jurisdictional models that allow countries to extent jurisdictional treatment reciprocally to Net participants from like-minded nations.

A comparison between the international success of the UDRP and the domestic failure of UCITA as a model law might also lead us to one conclusion: model codes for cyberspace will generally become successful statements of legal norms when they address limited issues where genuine agreement can be forged. The UDRP disavowed a wide range of DN problems: conflicts

---

64 A possible example is Belgium's proposal of, but final decline to enact, an anti-cybersquatiing law. *See* Alexandre Cruquenaire, LE REGLEMENT EXTRAJUDICAIRE DES LITIGES RELATIFS AUX NOMS DE DOMAINE 19 - 21 (Cahiers du Centre des Recherches Informatiques et Droit, Brussels, 2002).

65 For example, <.com> is the home for, in the UK, a local employment site [workfromhome.com], local telephone directory information [yell.com], and the official beer of the Edinburgh Festival [caledonian80.com]; in the Netherlands, an Amsterdam restaurant [cobracafe.com]; in China, a construction company [haikaigroup.com] and fashion operations [k-boxing.com]; in Japan, a gay bar [3across2.com]; in Korea, a city guide for Seoul <nmetro.com> and a restaurant <samwongarden.com>. Even in France, a country often irritated by things American, <.com> has plenty of adherents among companies who market mainly to locals, like <retrodor.com> [a old style bread maker], <celio.com> [a Paris GAP-like chain], <recrut.com> [a France employment agency]; and <cocomer.com> [a restaurant], not to mention publicly-supported arts entities like <lepalaisroyale.com> and <letheatreroyale.com>.

66 Ha'Aretz Daily Newspaper Ltd. v. United Websites, Ltd., WIPO Arbitration and Mediation Center, Case No. D2002-0272, July 3, 2002 (Dr. Milton Mueller, dissenting).

67 Space limitations do not permit me to compare, for example, the many ways UETA and E-Sign in the United States did *not* follow model approaches advocated by UNCITRAL's 1996 document. More recently, UNCITRAL adopted an additional e-commerce model law which appears more inspired by UETA and E-Sign than vice versa. *See* UNICTRAL Model Law on Electronic Signatures with Guide to Enactment with Guide to Enactment (2001), available at http://www.uncitral.org/en-index.htm.

with personal name holders; conflicts about geographical terms or indications; and conflicts involving competing intellectual property interests. As drafted, the UDRP focuses narrowly on situations where there is someone who holds trademark rights and someone who holds a same or substantially similar DN and no other rights attendant to that DN. In contrast, the UCITA project sought to create a model law for all occasions. Overly complex and suffering from apparent bias,[68] UCITA's real problem as a harbinger of new legal norms is that it reflects compromise, not agreement.

C. Invisible Hand Convergence: Environment-Based Emergence of Legal Norms

In the third kind of covergence, legal norms for the Internet emerge without any intervention by international bureaucrats. This type of convergence occurs because of market (or environmental) forces: either the economy adopts legal norms within a narrow spectrum of possibilities *OR* the economy will not enjoy significant development of the Internet on present models.

This type of legal convergence parallels a similar phenomena that has been observed in evolutionary biology: animals of different genetic ancestries may "converge" in that they adopt the same structural design to solve the same environmental problem. As Janet Moore and Pat Willmer have argued, "convergence is to expected when animals from different lines of descent have had to ocver especially demanding problems in order to survive" in the same environmental niche.[69] Legal systems respond separately to a changing environment and may, like animals, make the same adaptations, so that the "descendent" laws (animals) in different countries look more like one another than like their respective ancestor laws (animals).[70]

When I propose that convergence can result from market or environmental forces, this is not to diminish the political importance that coordinated, transnational lobbying has in affected areas. Private actors often urge one nation to adopt another nation's law as its own, but such lobbying will not produce consistent harmonization unless environmental factors point toward one

---

68 In 2002, UCITA's backers continued to try to amend its provisions to make them more palatable. The National Conference of Commissioners on Uniform State approved a series of amendments to UCITA on August 2, 2002. Amendments to the model law available at http://www.law.upenn.edu/bll/ulc/ucita/UCITA_Amds_AM02.htm, last visited August 7, 2002. *See also* Ted Bridis, *Group Oks Changes for Net Commerce*, Washintonpost.com, Tuesday, August 6, 2002; 2:13 AM, available at http://www.washingtonpost.com/wp-dyn/articles/A48570-2002Aug6.html, last visited August 7, 2002.

69 Janet Moore and Pat Willmer, *Convergent Evolution in Invertebrates*, 72 BIOLOGICAL REVIEWS OF THE CAMBRIDGE PHILOSOPHICAL SOCIETY (UK) 1, 3 (1997). An example of "convergent design" are whales, who willing being genetically closer to humans than fish, are designed more like fish because they have been designed for an aquatic environment. *See also* John O. Hunter & Jukka Jernvalla, *Hypocone as a key innovation in mammalian evolution*, 92 PROCEEDINGS OF THE NAT. ACAD. SCI. USA 10718 (Nov. 1995) (describing convergent tooth designs in animals).

70 Moore and Willmer define "convergent evolution" as occurring "when distantly related animals evolve separately, yet produce similarity: the descendants are therefore more alike than the ancestors." *Id.* at 5. *See also* SIMON CONVWAY MORRIS, THE CRUCIBLE OF CREATION 202-203 (1998) (showing animals from divergent ancestries converge, over millennia, in body design).

basic (kind of) solution. In this sense, legal systems share "genetic material" in a way that distant, but converging animal species would not. Two examples of this are, first, limitations on Internet service provider (ISP) liability and, second, basic legal treatment of electronic signatures and documents.

1. Internet Service Provider Liability

One of the earliest legal issues for the Internet was the problem of liability of Internet Service Providers (ISPs) for torts committed by non-related persons through the Internet. Serious slander and libel got to the Net long before serious e-commerce. In addition to defamation, ISPs can confront liability for third party data transfers that cause copyright infringement, trademark infringement, disclosure of trade secrets, and violations of privacy rights.

Early on, it looked like ISPs would have broad exposure for third- party copyright infringement or defamation. In the 1995 *Stratton Oakmost v. Prodigy* case in New York, the ISP was held to strict liability as the publisher of defamatory comments made by an unidentified party on one of Prodigy's bulletin boards.[71] In the same spirit, the U.S. Department of Commerce's early analysis of copyright and Internet issues concluded that ISPs should be analogized to publishers, putting substantial liability on them for third party infringements.[72] In the 1999 *Godfrey v. Demon* case, the English court also concluded that an UK ISP could be liable under English defamation law when it had been advised of the alleged defamation.[73]

Of course, alternative models were always available. Instead of being likened to publishers, ISPs could be likened to telephone systems or even the U.S. Post Office. No one considers the post office or AT&T liable when one of them delivers to C a message by A slandering B. In other words, looking to meatspace did not give us an obvious analogy for the proper liability standard for an ISP.

But market economics do provide an obvious choice among the competing standards of liability. With the present state of technology, a country that imposes strict liability on ISPs for third party defamation and copyright infringement is a country that might not have widespread Internet service. The ISPs that do exist will, one by one, be weighted down by large defamation or infringement judgments *OR* they will be driven out of business by enormous policing costs to keep defamatory and/or infringing material off their system. The costs cannot be passed on without severely limiting Internet access.

---

71 Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1885 N.Y. Misc LEXIS 229, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

72 U.S. Department of Commerce, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP IN INTELLECTUAL PROPERTY RIGHTS (1995) [the "White Paper," as it was called, was directed principally by then Assistant Secretary Bruce Lehman].

73 Godfrey v. Demon Internet Ltd., [1999] 4 All E.R. 342 (Queen's Bench Division, March 26, 1999) The *Godfrey* case was not a strict liability holding, as Demon had been put on notice of the defamation.

Barring improbable technology developments,[74] market forces will force countries to move toward legal systems that either (a) completely shield ISPs from such liability, or (b) enable ISPs to shield themselves from most liability through reasonable, affordable self-policing. This is the result one sees over and over again; as one commentator recently noted, "the rules for ISPs [are] increasingly settled."[75.]

In the U.S., commentators and courts reacted swiftly to the *Stratton Oakmont* decision.[76] An example of the first choice -- virtually complete shielding from liability -- is section 230 of the Consumer Decency Act of 1996 in the United States which concerns Internet defamations. Section 230 provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[77] As long as the provider of "an interactive computer service" is not responsible "for the creation or development of [the] information" the provider is shielded from liability. This provision has been interpreted generously by American courts.[78]

As to the second approach, significant jurisdictions are now shielding ISPs from liability for third party content transfers when the following conditions apply:

+ a ***non-control condition*** that the ISP
  + does not create or control the content of the third party information, and
  + does not control or actively participate in who gets the third party information;
+ a ***limited retention condition*** that the ISP does not retain the information for any longer than reasonable and necessary [which is a short time with transmission services and might be permanent with hosting services];
+ a ***limited knowledge condition*** that the ISP does not know about the violative nature of the information and/or does not have reason to know; **and**
+ an ***expeditious "take-down" condition*** that the ISP remove or disable information when it receives proper notice/allegation of a violation of law.

---

74 Improbable because all fixed works moving through the net are (a) eligible for copyright and (b) potential carriers of defamatory material that it would be very hard for an automated system to screen.

75 Michael Geist, *Internet "choke points" put the squeeze on content*, TORONTO GLOBE AND MAIL, July 11, 2002, at B11.

76 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); Religious Technology Center v. Netcom, 907 F. Supp. 1361, 1377 (N.D. Calif. 1995) (stating that strict liability for ISPs "would chill the use of the Internet because every access provider or user would be subject to liability when a user posts an infringing work to a Usenet newsgroup.") *See also*, Playboy Enterprises, Inc. v. Chuckleberry Publications, Inc., 939 F. Supp. 1032 (1996); Sega Enterprises, Ltd. v. Maphia, 948 F. Supp. 923 (1996).

77 47 U.S.C. §230(c).

78 *See* Blumenthal v. Drudge, 992 F. Supp. 44, 1998 Dist. U.S. LEXIS 5606 (D.D.C. 1998) (finding that section 230(c) shielded AOL from defamation liability by Matthew Drudge, even where Drudge was paid by AOL to provide content to AOL users.); Zeran v. America Online, 129 F.3d 327; 1997 U.S. App. LEXIS 31791; 25 Media L. Rep. 2526; 10 Comm. Reg. (P & F) 456 (4th Cir. 1997).

This is the general formula found in the US's 1998 DMCA, giving ISPs a safe harbor from contributory and vicarious liability for copyright infringement;[79] the same formula is manifest in the EU's 2000 Electronic Commerce Directive and its implementing national legislation, concerning liability for third party defamations and intellectual property infringements.[80]

Internet defamation cases in Japan have followed the same general trend – which Japanese copyright officials recommended in Dcember 2000 as a template for copyright infringement actions.[81] About the same time, China pressed ahead and adopted ISP liability rules along similar lines. On December 21, 2000, the Adjudication Commission of the Supreme People's Court issued interpretative guidelines on "several issues relating to adjudication of and application of law to cases of copyright disputes on computer networks."[82] Article 5 creates the familiar formula of creating liability where either the ISP knows of the infringement or has received adequate notification thereof from the copyright owner:

> "Article 5. Where any Internet service provider engaged in provision of information contents has obtained knowledge that an internet user is, carrying out on the Internet, an act of infringement on another person's copyright, or being warned by the copyright owner based on solid evidence, fails to take measures for removal and elimination of the infringing contents in order to eradicate the consequences of the infringement, the people's court shall investigate it and the network user, and impose joint liability thereon according to provisions of Article 120 of the General Principles of the Civil Law."

The interpretative guidelines reflect the familiar ideas of shielding the ISP from liability in the other direction.[83]

In 2002, some content providers started casting about for ways to increase ISP liability or to find, to use Michael Geist's phrase, other "choke points" in the infrastructure of the Internet

---

79 17 U.S.C. § 512.

80 *See* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular, Electronic Commerce, in the Internal Market, 2000 O.J. (L 178), arts. 12 – 14, [hereinafter E-Commerce Directive]; *see also* draft U.K. Electronic Commerce (EC Directive) Regulations 2002, published _____ 2002, art. 17 - 19, available at _____.

81 Interim Report by the Copyright Council of Japan, [First Sub-Committee – Experts' Working Group], Regarding the Issue of ISP Liability, December 2000 (reporting on 1997 and 1999 Tokyo District Court cases) (unofficial translation on file with author).

82 Interpretation by the Supreme People's Court of Several Issues Relating to Adjudication of and Application of Law to Cases of Copyright Disputes on Computer Network, Adopted at the 1144th meeting of the Adjudication Commission of the Supreme People's Court, December 21, 2000, available in English at www.cpahkltd.com/Archives.

83 Article 8 provides that if an ISP takes down apparently infringing material at the request of a copyright owner, then a court will refuse any request from the "accused infringer . . .[that] the Internet service provider to be liable for breach of contract. Article 9 transfers liability for such "claims for compensations for damages" to "the person giving the warning," i.e. the copyright holder.

where liability could be applied against findable, deep pockets.[84] My own view is that most of these entities will be able to adopt the same 'structural' positions as the ISPs – without them the Internet and e-commerce are not possible, and we won't have them if too onerous burdens of policing or too great a financial risk from third party liability is imposed.

Note, too, that sovereigns choosing to reasonably shield ISPs from defamation and copyright infringement – risk and exposure from private third parties – is quite different from sovereigns *not* shielding ISPs from exposure to liability to the sovereign – typically in areas where the state imposes censorship. Thus, the Chinese shield ISPs from liability from priate third parties, but pressure the same access providers into "pacts" to filter content dangerous to the state. In the same spirit, in the October 2001 decision in *J'accuse v. General Communications* case, a Paris court declined to hold French ISPs responsible for a hate-speech site hosted in the United States and accessible in France, but noted that "it will not be possible to delay the debate on a more active participation by all Internet participants, . . . including access providers."[85]

2. Digital Signatures

It would be overly ambitious to claim that, as a whole, electronic contract law is subject to parallel convergence. Contract law, particularly concerning consumers, is highly developed, highly localized law subject to a great deal of "path dependency." But the Internet creates pressures for convergence in at least two ways.

First, the Internet may attract attention to and create pressure against unique and aberrant provisions of contract law. An example is the recent repeal of German laws from the 1930s which made it "unfair competition" for American mail-order operations to offer money-back guarantees and generous, pro-consumer return policies.

Second, and more importantly, there are some baseline components of contract law where parallel convergence can be expected. These are legal uncertainties that must be solved or the economy at issue will not have widespread electronic contracting; the solutions most likely to not to be wrong are those that are minimal, general solutions to the uncertainty. The most obvious of

---

84 For example, in August 2002, a number of record companies brought suit against Internet backbone providers seeking to force them to block a China-based website, www.Listen4ever.com, *Arista Record, et al. v. AT&T Broadband, et al.*, (S.D.N.Y., filed August 16, 2002), available at < http://www.mindspring.com/~macgill/L4Ever%20Complaint.pdf>. The complaint seemed premised on 17 USC 502(j) creating a cause of action, a reading of the DMCA statute which baffled many of us. *See also* Michael Geist, *Internet 'choke points' put the squeeze on content*, TORONTO GLOBE AND MAIL, July 11, 2002, at B11 (reasoning that given that ISPs are shielded from liability, the new targets are credit card companies and Internet search engines).

85 J'Accuse c. General Communications, et al., Tribunal de Grande Instance de Paris, Order of October 30, 2001 ('. . . qu'il ne sera pas possible de différer longtemps encore le débat sur une participation plus dynamique de l'ensemble des acteurs d'internet . . .en ceux compris les fournisseurs d'accès.). The opinion is written by Jean-Jacque Gomez, of Yahoo! fame. Available at www.foruminternet.org/telechargement/documents/tgi-par20011030.pdf. Judge Gomez' remarks comes despite a 1996 ruling from the French Constitutional Court holding an earlier law on ISP liability unconsitutional on structural grounds, but with some emphasis on free expression concerns. *See* Judgment of Conseil constitutionnel, Decision no. 96-378, 23 juillet 1996, Recueil, p. 99 ; RJC, p. I-675 - Journal officiel du 27 juillet 1996, p. 11400, available at < http://www.conseil-constitutionnel.fr/decision/1996/96378dc.htm.

these are when contract law requires a "document," a "writing," a "signature," and "delivery" of one or more of those things. It was self-evident from the beginning that the digital, networked environment either *failed* to meet these requirements[86] or could *not* be assumed to meet these requirements. For a prudent people entering sizeable contracts, the latter uncertainty would be as lethal as being certain of legal shortcomings.

The obvious answer is the adoption of "equivalence" rules,[87] i.e. that, under certain conditions, electronic files are legally sanctioned as functional equivalents of paper documents; that under certain conditions, authentication processes or elements are legally sanctioned as functional equivalents of signatures; and that under certain conditions, sending an electronic file and/or authentication is legally sanctioned as the functional equivalent of "sending" or "delivering" paper documents.

This can be achieved by statutory provisions on "legal effect" that are increasingly common, i.e. "Information shall not be denied legal effect or enforceability solely by reason that it is in electronic form." (Prince Edward Island, Canada)[88]; "the requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures . . . are applied" (Pakistan)[89]; "A record or signature may not be denied legal effect or enforceability solely because it is in electronic form" (UETA, as codified in California)[90] or an obligation to allow "contracts to be concluded by electronic means" that is achieved by a prohibition on any "legal requirements applicable to the contractual process" that would "result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means." (European Union)[91]

Beyond such baseline equivalences, an economy may implement legal recognition of particularly secure methods of authentication, producing a "layered" structure of record authentication law, as the European Union has done in their 1999 E-Signatures Directive.[92] The 1999 Directive establishes a legal framework for a system of "advanced electronic signatures which are

---

86 *See, e.g.* Andrew D. Murray, *Entering Into Contracts Electronically: The Real W.W.W.* in LILIAN EDWARDS AND CHARLOTTE WAELDE, EDS., LAW AND THE INTERNET 17, 19 – 20 (2000) (concluding that a 'digital document' would have failed to meet document requirements under United Kingdom law in the late 1990s).

87 Murray, *supra* note __ at 20. As early as 1996, UNCITRAL advocated such a "functional equivalence" approach. *See* UNCITRAL E-Commerce Model Law, *supra* note ___ at 15 (I.E. of "Guide to Enactment," explaining "functional equivalent" approach).

88 Article 4, Electronic Commerce Act, Bill No. 25, 2nd Session, 61st General Assembly, Province of Prince Edward Island, 2001.

89 From the Pakistani Electronic Transactions Ordinance 2002, promulgated September 11, 2002, as reported in *Electronic Transactions Ordinance promulgated*, DAWN, September 12, 2002, available at < http://www.dawn.com/2002/09/12/top15.htm> last visited November 1, 2002.

90 California Financial Code, section 1633.7(a). Section 1633.7(b) similarly provides that ""A contract may not be denied legal effect or enforceability solely because it is in electronic form."

91 Article 9(1), E-Commerce Directive, *supra* note __ at 11.

92 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013 , 19/01/2000 p. 0012 – 0020.

based on a qualified certificate and which are created in a secure-signature-creation device."[93] A problem with such "advanced" authentication schemes – but beyond the scope of this discussion -- is that they tend to be technology specific or require bureaucratic structures that are unnecessary with the baseline "equivalency" provisions.

3. Smaller issues where market forces cause convergence

In addition to large topics like ISP liability and electronic signatures, there may be small issues – or sub-issues of general legal areas – where market economy or civil society forces will point toward convergence. Let me give two candidates.

The single publication rule in defamation law can have important impact on the measure of damages and the time in which a defamation action can be brought. Under the early common law of defamation, *each* communication of a defamatory statement to a third party constituted a separate "publication" giving rise to a new cause of action.[94] This idea was easy to apply to an orator standing on the corner of Green Park, but lost much of its sensibility when applied to newspapers and books – one defamatory written statement given to lots of different people at different places over a single day or many years. The result was the "single publication" rule: that, as long as the defamatory statement remain unchanged, distribution of a defamatory statement widely across geography and time would be treated as *one* publication.[95]

With the Internet, defamation plaintiffs have argued – and will argue – that each downloading of a defamatory statement constitutes a separate publication. One argument is that the "pull" nature of the Internet makes for a different result than with "push" distribution by traditional publishers.[96] Courts are likely to reject this kind of argument and coalesce around rule that as long as the defamatory website or Internet posting remains unchanged, sequential hits, visits, and/or downloads do not constitute separate publications. Notice that the one reason for convergence is judicial economy – its own sub-category of "market forces." Anther reason is the equitable notion common to most societies that a party should not sleep on their rights.

Exceptions and limitations to copyright law are an area of national divergence and, sometimes, idiosyncracy, but there are nonetheless common enough themes to such limitations and exceptions to think that economic and civil society forces might push us toward greater convergence in this area. Alain Strowel has noted that there are really five sorts of copyright exceptions that are the most important in an "information society": private copying, citation/quotation, news reporting,

---

93 *Id. passim*. For a full exploration of the E-Signatures Directive and its implementation in France, see THIERRY PIETTE-COUDOL, LA SIGNATURE ELECTRONIQUE (Litec, 2001).

94 Duke of Brunswick v. Harmer, 14 Q.B. 185 (1849).

95 Gregoire v. G.P. Putnam's Sons, 298 N.Y. 119, 125 (1948) (publisher's sale from stock of a copy of a book containing libelous statement was not new publication); Wolfson v. Syracuse Newspapers, Inc. 254 App. Div. 211 (1938), *aff'd no op.* 279 N.Y. 716 (1939). Restatement [Second] of Torts, §577A[3].

96 Firth v. State of New York, New York _____ Court, Opinion of July 2, 2002, at 5 (". . . claimaint maintains that . . . because publications on the Internet are available only to those who seek them, each 'hit' or viewing of the report should be considered a new publication that retriggers the statute of limitation.")

education and research; and library and archive exceptions.[97] More importantly, he notes that these really reduce to three "principal finalities": the private sphere, circulation of information, and cultural and scientific development.[98]

The basic notion in all of these examples is that the technological/economic environment is causing a kind of "converge or abandon the environment" phenomena, i.e. create electronic signatures or abandon meaningful e-commerce. While I believe that this is actually happening, the failure of grander visions of technological determinism related to the Internet add a note of caution. In a thoughtful analysis and critique of early views of what the Internet would do to the legal profession, Professor Richard Ross reminds us that such visions tend to "overlook the power of social context to contain (as well as direct or accelerate) effects supposedly immanent within technologies."[99]

D. Continued Diversity and Divergence in Legal Norms

In contrast to the three categories above, there seem to be some areas of law where there will continue to be divergence in the dominant norms in national legal systems that impact the Internet. The most visible of these is the law of free expression.

There is no better manifestation of abiding differences about free expression than the dueling decisions in the *LICRA v. Yahoo!* dispute In 2001, a Paris court found that it has jurisdiction to order Yahoo! in the United States (as well as Yahoo!France) to take technological measures to ensure that Internet users on French territory could not receive visual images of Nazi paraphernalia over the Internet. The French court subjected the companies to hefty fines for any failure to comply.[100] Less than a year later, a district court in San Jose granted Yahoo! summary judgment, on First Amendment grounds, against any possible enforcement of the Paris court's ruling.[101]

The problem of expression that is protected in jurisdiction A flowing into jurisdiction B, where it is prohibited, is not new. For decades, Voice of America broadcasts were intended to do just that. In the present networked world, there are perhaps three broad camps on free expression issues. At one extreme is the US, forced to explain its particularly robust vision of free expression

---

97 Alain Strowel, *supra* note ___ at 198.

98 *Id. See also* Shira Perlmutter, *Future Directions in International Copyright*, 16 CARDOZO ARTS & ENT. L. J. 369 , 370 (1998) (noting that despite variety in limitations and exceptions in national copyright laws, "certain general categories are common.")

99 Richard J. Ross, *Communicatrions Revolutions and Legal Culture: An Elusive Relationship*, 27 LAW AND SOCIAL INQUIRY 637, 639 (2002).

100 UEJF et LICRA v. Yahoo, [Interim Court Order of November 20, 2000], Paris Tribunal de Grande Instance, No. RG: 00/05308, available at http://www.cdt.org//speech/international/001120yahoofrance.pdf last visited August 8, 2002.

101 *Yahoo! Inc. V. La Ligue Contre Le Racisme*, Case No. C-00-21275 JF, Order Granting Motion for Summary Judgment, District Court for Northern California, November 7, 2001

to other democratic, civil societies that do not have the same constitutional insistence.[102] There is a middle camp of democratic countries that forbid -- and sometimes prosecute -- hate speech.[103] And there are countries like China, Saudi Arabia, and Zimbabwe which forbid -- and regularly move against -- a wide range of Internet speech that they deem dangerous or destablizing.

Following the powerful language of the Supreme Court in the 1997 *Reno v. ACLA* case, the U.S. seems fixed in its views of free expression on the Internet.[104] It is tempting to predict that the U.S. will find itself more isolated on this count. But there is also considerable instability in the other two groups. For example, while Paris judge Jean-Jacques Gomez shook the Internet world with his jurisdictional and speech conclusions in the *Yahoo!* case, the European Court of Justice (ECJ) has reversed recent French decisions enforcing speech restrictions against a biographer of Petain and anti-semitic political activitists. The ECJ's jurisprudence reflects not just European conventions on human rights, but the clear norm of the Universal Declaration of Human Rights that freedom of expression includes freedom "to seek, receive, and impart information and ideas through any media and regardless of frontiers."[105]

It should be remembered that non-convergence need not be limited to issues where there are heartfelt, deeply-embedded national differences. Non-convergence may remain the state of affairs when established national differences can be retained with only minor, tolerable losses in efficiency. To give a domestic example, imposing local sales tax on Internet transactions will be possible when either (a) local sales taxes are harmonized [seamlessness], or (b) database technology permits vendors [or their intermediaries] to accurately and efficiently impose differing tax rates. The point is that there has been, perhaps, a tendency to overestimate the harmonizing effects of globalization on meatspace practices[106] and we should avoid that same mistake when pondering the fate of law on the Internet.

IV. WHERE THE VERDICT IS STILL OUT

---

102 Philip Reitinger, U.S. Department of Justice, LEGAL ASPECTS OF GOVERNMENT-SPONSORED PROHIBITIONS AGAINST RACIST PROPOGANDA ON THE INTERNET: THE US PERSPECTIVE, Seminar on the Role of the Internet with regard to the International Convention on the Elimination of All Forms of Racial Discrimination, Geneva, Switzerland, November 10-14, 1997, available at < <http://www.unhchr.ch/html/menu2/10/c/racism/reitinger.htm>, last visited August 8, 2002.

103 *See, e.g.* Associated Press, *Rare Case Has Norwegian Man Convicted of Racism on the Web*, April 24, 2002, available at www.law.com (describing Norwegian conviction that month for racist speech and March 7 judgment in Sweden against tabloid that allowed racist comments on its Internet chat site).

104 521 U.S. 844 (1997). *See also* American Library Assoc. v. United States, 2002 U.S. Dist. LEXIS 9537 (E.D. Pa. , May 31, 2002) (finding that the Internet is a "public forum" for First Amendment purposes and Congressional tying of library funding to use of ineffective pornographer filtering programs was unconstitutional).

105 Universal Declaration of Human Rights; Article 19, G.A. Resolution 217 (III)A, 3(1) U.N. GAOR Resolutions at 71, 74 - 75, U.N. Doc. A/810 (1948).

106 *See, e.g.* MAURO F. GUILLEN, THE LIMITS OF CONVERGENCE (2001) (describing how business practices in Spain, Korea, and Argentina are not converging).

There are many areas where convergent legal norms related to the Internet are possible, probable, and/or desirable. But there are also areas of human activity where it may not be possible to forge harmonized legal norms and we may discover – the happy surprise of many – that the world can get along just fine without a "seamless" legal infrastructure. Such areas of Internet-related law include extra-copyright protection of databases; protection of the privacy of personal information; and the "cultural exception" for audiovisual works in international trade; patents on e-commerce business processes. Each of these has been a bone of contention, with no path to convergence immediately visible. Let me briefly elaborate on two of the examples mentioned above.

The extra-copyright protection of databases is a problem that arose from court decisions in the U.S. and Europe in the early 1990s. The decisions denuded large, comprehensive databases of copyright protection just as the prospect of digital trade in such databases was becoming apparent. [107] In response, in March 1996, the European Union promulgated a directive establishing a strong intellectual property right specific to databases (the "Database Directive"). In the months that followed, awareness of and opposition to the Database Directive grew among scientists, researchers, and educators in the United States. The result was that by the time the WIPO Diplomatic Conference was held in December 1996, database protection had to be taken off the negotiating table. In short, an early attempt at "top down" convergence failed.

Since 1998, Congress has been considering various bills to establish some kind of extra-copyright protection of databases in the U.S. via a misappropriation or unfair competition approach, although there has yet to be any serious empirical demonstration of the need for additional intellectual property in this area. Meanwhile, opposition among developing countries seems to have grown – politically attached to a belief that TRIPS and the WIPO structures are already biased in favor of wealthy nations. In this area, it seems that ultimately there will either be top-down treaty convergence or no convergence at all.

Access to raw data has, from a different angle, also been a sticking point in transatlantic relations in the form of protection of personal data. In 1995, The EU promulgated a Data Privacy Directive[108] which threatens to disrupt data flows to third countries that do not provide commensurate protection and safeguards for personally identified information. Canada, Australia, and the United States have all found themselves embroiled, to one degree or another, with wrangling with and review by the European Commission on this problem – with no apparent convergent norms in site beyond some early and potentially still useful guidelines from the OECD.

---

107 For an exhaustive account, see Justin Hughes, *Political Economies of Harmonization: Database Protection and Information Patents*, paper presented at the Institut Français de Relations Internationales, June 10, 2002, available at www.ssrn.com. The cases in question were Feist Publications v. Rural Telephone Service Corp., 499 U.S. 340 (1991); Van Dale Lexicograpfie v. Van Romme, Supreme Court of the Netherlands (Hoge Raad), Judgment of 4 January 1991, [1993] EUROPEAN INTELLECTUAL PROPERTY REVIEW D-260; also reprinted in English in EGBERT J. DOMMERING AND P. BERNT HUGENHOLTZ, EDS., PROTECTING WORKS OF FACT 93 (1991). Beginning in 1989, French courts also delivered a series of decisions denying copyright protection to factual compilations on the grounds that they did not reach "au rang de création intellectuelle" or constitute an "apport créatif et intellectuel." *See* Lucas, *supra* note ___ at 40, fn. 79.

108 Directive 95/36/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data., available at www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html.

CONCLUSION

Consider observations from two thinkers who are decidedly *not* cyber-*anything.* Surveying the legal scene in 1995, Harold Berman questioned whether "international law" and "transnational law" were adequate conceptual categories for law when the non-lawyers talk about the economy, the environment, and society in terms of "world" and "global."[109] Professor Berman envisioned an understanding of global law that would reintegrate "inter-state law" with "common features of the various legal systems of the civilized world" and "the customary law of transnational communities."[110] A few years earlier, surveying "high tech paranoia" literature, the Marxist writer Fredric Jameson deemed it a genre in which advanced technology was used metaphorically to describe the world system. In what Jameson *thought* was a fictional construct, "circuits and networks of some putatively global computer hookup are narratively mobilized by labyrinthine conspiracies of autonomous but deadly interlocking and competing information agencies."[111]

We have come to see that the global computer hookup is no longer putative; the sources of information are unquestionably interlocking and competing, if not yet deadly; and the circuits have established a transnational community that is slowly but inevitably mobilizing itself against features of various legal systems that are *not* common. Understanding how this mobilization occurs – in both relatively transparent ways and relatively low profile ways – is important for both scholars and activists.

Common legal norms are being forged which will sink much deeper into national legal systems than traditional norms of "international" or "transnational" law did, which applied only between and among sovereign states. Forging such norms is not an easy task. As one jurist noted concerning harmonization of law applicable to the Internet, "[I]n each country, the temptation is the same to bring one's own concepts and categories to the discussion."[112] The conceptual give and take, the development of new categories and meta-categories for law, will be about as interesting as law is allowed to get. On every one of the topics mentioned in this paper, we are very far from the last word.

---

109 Harold J. Berman, *World Law*, FORDHAM INT. L. J. 1617 (1995).

110 *Id.* at 1622.

111 FREDRIC JAMESON, POSTMODERNISM OR, THE CULTURAL LOGIC OF LATE CAPITALISM 38 (1991).

112 Lucas, *supra* note __ at 13 – 14.