3-2003

The Internet and the Persistence of Law

Justin Hughes
Benjamin N. Cardozo School of Law

THE INTERNET AND THE PERSISTENCE OF LAW

JUSTIN HUGHES*

Abstract: Since legal commentators first confronted cyberspace, three broad stories have emerged to describe the interrelation of law and the Internet: the "no-law Internet," the "Internet as a separate jurisdiction," and Internet law as "translation" of familiar legal concepts. This Article reviews these stories, focusing on how ongoing "translation" is giving way to a growing convergence in Internet law. The Article makes the case for convergence among legal responses to cyberspace and proposes a basic taxonomy for different models of convergence. With this taxonomy, the Article examines the ways in which convergence is occurring, as well as its effects on both Internet law and traditional, national legal norms. The Article concludes that the common legal norms being forged will affect national legal systems more deeply than traditional "international" or "transnational" law, and that the conversation on this affect has only just begun.

INTRODUCTION

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.

---

* 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 and Stuart Reimer for research assistance for this manuscript; my thanks to Andrew McLaughlin, Fred Yen, and all the participants of the Boston College Law School Conference on Intellectual Property, E-Commerce, and the Internet for helpful comments and a lively conversation on this Article. The remaining errors are the exclusive intellectual property of the author.

In the short lifetime of cyberspace, at least three broad kinds of stories have already been told about how the Internet and law will interact. These three distinct meta-visions of the relationship between the Internet and law are discussed in Part I: the "no-law Internet," the "Internet as a 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 story, what I will call the "Internet as a separate 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: cyberspace should be its own jurisdiction.

The third story 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 ensure that the inhabitants do not 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: the Communications Decency Act (CDA), Child Online Protection Act (COPA), Children's Internet Protection Act (CIPA), Digital Millennium Copyright Act (DMCA), Uniform Electronic Transaction Act (UETA), Anti-Cybersquatting Consumer Protection Act (ACPA), E-Sign, and Uniform Computer Information Transaction Act (UCITA) are only the American acronymic peaks of a vast international range of legislative proposals and enactments. In California, the *state* legislature saw 258 Internet-related bills introduced in its 1999-2000 session, up from four bills in 1994.

Because the initial wave of immigrants to cyberspace was overwhelmingly American (both natural and juridical persons), American courts were usually the first to address novel legal issues about the Internet (although parallel fact patterns have quickly appeared in other countries). Thus, when American academics began paying attention to the Internet, it felt—despite the "global" rhetoric—like a

wholeheartedly American institution.[1] The initial wave of legal scholars drawn to the Internet were, on the whole, experts in American constitutional, criminal, commercial, and copyright law. Scholars established in international or comparative law were a relative minority of the new cyberlaw gurus.

Even today, novel cyberlaw problems statistically arise first in either the United States or another 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%).[2] Adding Britain, Canada, and the United States, a bare majority of Internet traffic still comes from common-law, English-oriented countries (50.52%).[3] If American legal scholars have been too "Americentric" about the Internet (and there 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[4]—advice as true for the law. By one estimate, Americans will comprise only one quarter of all Internet users as early as 2005.[5] While the United States 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.[6]

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

---

[1] This also causes, in some countries, the perception that the Internet is yet another American intrusion into local or national societies. *See, e.g.*, ANDRÉ LUCAS, DROIT D'AUTEUR ET NUMÉRIQUE 7 (1998) (noting the "little polemical debate" in France over whether the Internet is a "vehicle for American thinking").

[2] *China Second to US in Web Traffic: Study*, SYDNEY MORNING HERALD, Aug. 1, 2002, *available at* http://www.smh.com.au/articles/2002/08/01/1028157806643.html.

[3] 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).

[4] Amy Harmon, *An Internet Guru's Lexicon*, N.Y. TIMES, May 13, 2001, § 3, at 14.

[5] 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.

[6] *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 Internet).

producing and will continue to produce a significant amount of convergence of legal systems. Recently, in discussing intellectual property, French commentators Michel Vivant and Agnès Maffre-Baugé have made similar observations. Noting that there is an inherent tension or conflict between private entities that want to circulate themselves or their goods widely through the Internet and the nation-states that 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.[7]

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 recognizes the emergence of new international or *transnational* legal norms to which nation-states and domestic legal systems increasingly adhere.[8] Another way to think about this convergence focuses on the way the project of translation gradually returns 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.[9] Part I 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.[10] Because the Internet is weaving itself increasingly into our daily, meatspace lives, the comparison to *lex mercatoria* is inadequate. Part I offers some ruminations

---

[7] Michel Vivant et Agnès Maffre-Baugé, *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* LUCAS, *supra* note 1, at 13 (recognizing that a comparative-law approach is necessary to the minimal harmonization of law needed on the Internet).

[8] Jeremy Bentham 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 (J.H. Burns & H.L.A. Hart eds., 1970) (1789). Philip Jessup recommended replacing Bentham's phrase with a broader concept of "transnational law." PHILIP C. JESSUP, TRANSNATIONAL LAW 2 (1956).

[9] *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1019–21 (1994) (drawing parallel to *lex mercatoria*); David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1389–90 (1996).

[10] *See infra* notes 16–47 and accompanying text.

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 II presents a simple attempt at a taxonomy of the emergence of legal norms governing the Internet. 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 Internet-related legal principles.

The taxonomy set in Part II 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 that produce the treaty. Development of the legal norms is, at least in the final stages, fairly transparent. The 1996 World Intellectual Property Organization (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. American legal scholars are arguably the most conscious of, and the most involved in, this kind of convergence.

The second type of 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 the literal legal language, of the international model. Part II discusses both how the Uniform Dispute Resolution Policy for the ".com" top level domain has become the preeminent model for such convergence and how model laws for electronic contracting put forth by the United Nations Commission on International Trade Law (UNCITRAL) have been less successful.[11]

Part II then turns to a third kind of convergence: emergence of legal norms without the intervention of diplomats and bureaucrats working internationally.[12] In this *invisible hand* or *parallelism convergence,* market forces produce a limited range of options for each economy; countries must either adopt laws within this range or forego the economic potential of the Internet. Part II discusses Internet serv-

---

[11] *See infra* notes 56–75 and accompanying text.

[12] *See infra* notes 75–110 and accompanying text.

ice provider (ISP) liability and baseline rules on electronic contracting as examples of invisible hand or parallelism convergence.

Part II also takes up a fourth area of convergence, one that is not really convergence at all.[13] 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. For example, Canada and many European countries permit speech restrictions that are antithetical to Americans; China and Saudi Arabia impose restrictions that would be wholly unacceptable to Europeans.

One can find characteristics of each model in almost any area where the Internet is bringing pressure for development of new law. And there are many areas of law that may yet gravitate toward one model of convergence over another. A few of these are briefly discussed in Part III.[14] Indeed, the details of reality will spill over the edges of any taxonomy. As noted earlier, this Article is a first suggestion for a taxonomy of the development of Internet law. 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, "There is room for words on subjects other than last words."[15]

I. 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: 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 legal norms. If anything, this raises the stakes for each nation-state in the development of the Internet legal norms.

---

[13] *See infra* notes 111–117 and accompanying text.

[14] *See infra* notes 118–119 and accompanying text.

[15] Robert Nozick, Anarchy, State, and Utopia, at xii (1974).

A. *The "No-Law" Internet*

The first vision of the Internet and law was simple: never the twain shall 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 were all founded on a determinism in which technology became, as Reg Whitaker noted, "the autonomous engine of history."[16]

This determinism was built on a surprisingly fixed understanding of the Internet's technology, an understanding that one can appreciate in the context of the moment. Early cyberphilia treated the Internet as the *end* of History: claims like "[c]yberspace is Platonism as a working product"[17] and "[t]he Net wires the world for Hegelian *Geist*"[18] 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 "[rather], it is a fixed state in which the end of history and the total realization of mind is finally achieved."[19] Some legal commentators were understandably drawn in to this heady, but static vision.

The ingredients of the vision started with the Internet's basic distribution characteristics—almost frictionless, almost instantaneous, very decentralized, and with information flowing from and through different nodes—which made geography seem irrelevant.[20] Minimal relevance of geography for distribution purposes was combined with at least two other basic ingredients of the Y2K Internet. One ingredient was the amount of information in relation to humans and their institutions. As Johnson and Post wrote, "The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to [the government authorities to

---

[16] REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 47 (1999).

[17] Michael Heim, *The Erotic Ontology of Cyberspace*, *in* CYBERSPACE: FIRST STEPS 59, 64 (Michael Benedikt ed., 1991).

[18] MARK C. TAYLOR & ESA SAARINEN, IMAGOLOGIES: MEDIA PHILOSOPHY 3 (1994) ("Simcult").

[19] Julian Stallabrass, *Empowering Technology: The Exploration of Cyberspace*, 211 NEW LEFT REV. 3, 9 (1995).

[20] As Judge Nancy Gertner characterized the Internet in 1997, "[T]he 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." Digital Equip. Corp. v. AltaVista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997).

permit meaningful control]."[21] Johnson and Post's conclusion depended on a particular understanding of the technology that still seems correct, but is and will be challenged.[22]

Another basic characteristic was anonymity. Of course, this anonymity seemed ubiquitous because of fairly primitive technology—written words on a glowing screen instead of the human voice or visage. E-mail from someone or something other than the purported author 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 Web-cams 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 slow, and too geographically and technically limited to regulate a global citizenry's fleeting interactions over [this] mercurial medium."[23] If the rise of modern law depended, as Henry Maine observed, on a definition of political belonging based on "topographical limits,"[24] then a cyberworld without territory or topographical limits would be inhospitable to both the enforcement mechanisms and the analytic tools of modern law. Examples of attempted enforcement mechanisms include any number of attempts to censor the Internet with firewalls. An example of the inability of analytic tools of modern law to adapt to the Internet is Martin Redish's 1998 suggestion that the ubiquitous nature of the Internet made the old jurisdictional tools irrelevant[25]—a conclusion

---

[21] Johnson & Post, *supra* note 9, at 1372.

[22] For example, Packetshaper software promises real time analysis and discrimination based on protocol, application, URL, etc. One can find a description of Packetshaper at http://www.packeteer.com/products/packetshaper/index.cfm. Developments in artificial intelligence will further undermine the assumption that government eyes and ears cannot be everywhere.

[23] James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 183 (1997). Boyle's message in this excellent article is that the "infolibertarians should not be so quick to write off the state," a prognosis that has proved amply correct. *Id.* at 184.

[24] *See* SIR HENRY SUMNER MAINE, ANCIENT LAW 124–26 (Univ. of Ariz. Press 1986) (1864).

[25] *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, 605–06 (1998) ("[T]he technological development of the Internet effectively renders the concept of purposeful availment both conceptually incoherent and practically 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

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 (ABA) receives complaints about materials on the Web, reviews those materials pursuant to pornography/obscenity standards applied to broadcasts, and sends "take-down" orders when it deems inappropriate certain materials hosted on Australian sites.[26]

There is much about the Australian law that appears wrongheaded—starting with the application of broadcast, not print, standards for pornography to the Internet. Looking beyond those substantive questions, however, the law serves as a wonderful example of a sovereign's inability to control the Internet effectively. During the second six months of 2000, the ABA handled complaints directed at prohibited materials on 139 sites.[27] Of these 139 sites, Australia hosted only six, all of which received take-down notices from the ABA. As to the other 136 sites, the ABA forwarded information from the complaints to software filtering companies[28] 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 a remark made in 2002 by a deputy minister in Iran's Ministry of Culture and Islamic Guidance that "control has no meaning on the Internet."[29]

But the descriptive account on which the "no-law" Internet was founded suffers from two shortcomings. The first was the naiveté of its technological determinism. One does not 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, and detours into niches and eddies that few

---

carefully made the decision either to affiliate with the forum state or seek to acquire its benefits.").

[26] Greg Taylor, *Regulatory Failure: Australia's Internet Censorship Regime*, Electronic Frontiers Australia (May 5, 2001), *at* http://www.efa.org.au/Publish/aba_analysis.html.

[27] *Id.*

[28] *Id.* ("[T]he 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.").

[29] Nazila Fathi, *Taboo Surfing: Click Here for Iran . . .*, N.Y. TIMES, Aug. 4, 2002, § 4, at 5.

would have anticipated. Centuries of military technology[30] and our recent experience with communication technologies offer examples of the unanticipated flow of technology.[31] The image of a "continuing race of offensive and defensive technologies" on the Internet[32] is metaphorical to some and very real to others, but, in either case, it is a race in which no one should 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, did not 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 the fact 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 who 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 Web sites will merely drive them or their material off-shore, a very different situation applies to ISPs, telecoms, and cybercafés. A state's effective enforcement 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 Internet services who are not quite as mobile as the flitting and frequently anonymous inhabitants of cyberspace."[33] China, known for its "great firewall of China" approach to censorship, is increasingly turning toward control of ISPs and cybercafés.[34] In 2002, China began

---

[30] *See generally* WILLIAM M. MCBRIDE, TECHNOLOGICAL CHANGE AND THE UNITED STATES NAVY, 1865-1945 (2000).

[31] When broadcast television was introduced, one could easily 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 practically rendered publishing in some less common languages (Dutch, Danish, Swahili, Bambara, etc.) an economic dead-end, but the advent of desktop publishing technology undid some or all of those economic disadvantages.

[32] Erik Eckholm, . . . *And Click Here for China*, N.Y. TIMES, Aug. 4, 2002, § 4, at 5.

[33] Boyle, *supra* note 23, at 197.

[34] *See* BBC News, *China Internet Firms "Self-Censoring"* (July 5, 2002), *available at* http://news.bbc.co.uk/1/hi/world/asia-pacific/2098530.stm.

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."[35]

While it is certainly more efficient to go after larger infrastructure entities, a sovereign also has the ability to do nasty things to individual cybernauts whose corporeal bodies remain on the sovereign's side of the computer screen. For example, in 1997, Germany prosecuted the head of CompuServ's German subsidiary on pornography charges stemming from Internet traffic.[36] More recently, the 2002 Chinese crackdown on cybercafés has included the installation of software that records attempts by café users to access banned sites.[37] Also that year, a forty-year-old former policeman, Li Dawei, became the first individual Chinese citizen sentenced to prison for downloading materials deemed politically unacceptable.[38]

B. *The Kingdom of the Internet*

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 technology, a series of commentators from the mid-1990s onward—M. Ethan Katsh, William Mitchell, Larry Lessig, and Joel Reidenberg[39]—reminded everyone that in cyberspace software code is law, or a form of restraint as good or better than law. Some person did write the software code, even if that person did not write it with Tibetan dissidents, Napster, and billions of bizarre Web pages in mind. Nevertheless, the code could be rewritten.

---

[35] *Id.*

[36] Dr. Gunnar Bender, *Bavaria v. Felix Somm: The Pornography Conviction of the Former CompuServ Manager*, INT'L J. COMM. L. & POL., Summer 1998, ¶ 2, *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 TRIB., Apr. 17, 1997, at 13.

[37] Eckholm, *supra* note 32.

[38] *China Jails Politically Incorrect Net User 11 Years*, MERCURY NEWS (San Jose), Aug. 5, 2002, *at* http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3803541.htm.

[39] *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); WILLIAM MITCHELL, CITY OF BITS (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 (1996); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911 (1996); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) [hereinafter Reidenberg, *Lex Informatica*].

In terms of self-organization, consensus, and new forms of law, David Johnson and David Post have been perhaps the two most eloquent commentators for this vision of the Internet.[40] In this view, self-organization is seen as the mechanism by which a variety of communities will emerge with different governing contractual structures and by which individuals will have the freedom to move among those emerging communities.[41] Such a vision is very much akin to the self-ordered libertarian world of varied communities put forward in *Anarchy, State, and Utopia*.[42]

It is only a small step or series of steps from seeing the Internet as 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 its own law and legal institutions."[43] 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 clearer and more rational rules. Although the concept of a self-ordered Internet was popular for only a brief moment, one may still hear its echoes when countries undertake organized, national efforts to address the legal quandaries created by the Internet.[44]

---

[40] *See generally* 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*, *at* http://www.cli.org/selford/essay.htm (last visited May 9, 2003); David R. Johnson & David G. Post, And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law (Sept. 5, 1996) (draft), *available at* http://www.cli.org/emdraft.html.

[41] *See, e.g.*, Johnson & Post, *supra* note 9, at 1398–1400 (noting that "exit options" from virtual communities mean that different communities could flourish with people free to move easily among them); John O. McGinnis, *The Once and Future Property-Based Vision of the First Amendment*, 63 U. CHI. L. REV. 49, 100–07 (1996). In his article, McGinnis noted that, up until 1996, the Internet's "growth ha[d] been achieved with no guidance from the state and little regulation outside the enforcement of private ordering through contract." *Id.* at 102.

[42] *See generally* NOZICK, *supra* note 15.

[43] Johnson & Post, *supra* note 9, at 1367.

[44] *See, e.g.*, Lesley Stones, *Delegates Disagree About Regulation of Laws*, BUS. DAY (Johannesburg), Apr. 23, 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.

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 accidentally strays across the border into Cyberspace."[45] 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. As our appliances become "smart," our houses become "wired," our telephony is done with packet-switching, and our cable, telephone, and Internet services bundle and unbundle, will we know when we "crossed" the cyberspace border? Even if we did know, 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. When General Motors completes a multi-million dollar deal 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 hermetically sealed world in which different economic models could be developed for everything from copyright to antitrust,[46] 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 authorization to sell or trade. It is not that the real world dashed the idealism of the cybernauts without provocation; on the contrary, 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 DMCA. But the publicly justifiable principle is, *at best*, one of translation, i.e., that

---

[45] Johnson & Post, *supra* note 9, at 1379.

[46] *See id.* at 1382–84 (discussing antitrust and copyright models).

we should use existing instruments and preserve "balances" of interests whenever possible.

I say the publicly justifiable principle is *at best* one of translation 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 the results of e-commerce is that it produces "disintermediation" and "reintermediation," new ways to express the creative destruction of a market economy. Travel agents have found themselves increasingly disintermediated as consumers book hotel reservations and buy airline tickets online from either the hotels or the airlines or from the new information aggregators, i.e. Travelocity.com and Orbitz.com. Traditional auction houses have also suffered economically at the hands of eBay, and car dealers have barely slowed the automobile manufacturers from selling directly to the public. Why have these people gone unprotected from an Internet-driven "re-balancing" 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 would have only the makings of interesting comparative law. But content on the presently configured Internet gives national boundaries the same deference as do migratory birds, viruses, and carbon gas emissions. Because of its similar migratory nature, regulating the content on the Internet requires "[c]ooperation among all countries . . . [to] assist in the construction of a seamless environment for electronic commerce."[47] In other words, governments will have to accept a zone of harmonized Internet law that, at a minimum, functions as an autonomous region within their legal systems—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 as to *how* this area can still be distinct from the rest of a nation's law. The vision of a separate "contiguous" cyberspace jurisdiction does not adequately acknowledge how the Internet—e-commerce, e-communications, e-socialization—perme-

[47] Joint Statement on Elec. Commerce, Jan. 30, 1999, U.S.-U.K., *available at* http://www.iwar.org.uk/e-commerce/resources/usukecommerce.htm.

ates each national society. Instead, the hackneyed metaphor of the information superhighway may help. The American interstate highway system penetrates and bisects fifty jurisdictions that retain their own road and 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 system is nearly seamless in that each interstate highway has the same construction, same style of signs, same grades of ramps for ingress and egress, and largely consistent speed limits. The interstate system thus functions much like a separate jurisdiction that 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 increasingly influence laws governing behavior off the Internet. For example, some people 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, the same justification should suffice to change *all* defamation law because a person defamed *off* the Internet will be able to use the Internet as a successful platform for response. 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 not as a general rule. 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 will result in 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).[48]

The mid-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 (Trade-Related Aspects of Intellectual Property Rights) Agreement and the Marrakesh Agreements as a whole. The TRIPS Agreement, however, created a problem for WIPO. WIPO administered the traditional, dominant multilateral intellectual property treaties (the Paris and Berne Conventions), but found that TRIPS gave the World Trade Organization (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, twenty-first century multilateral intellectual property obligations *which were not* integrated into TRIPS.

While the WCT and WPPT "clarified" certain copyright issues that had become more important in the digitized, networked environment, the treaties were principally intended to augment international copyright norms in three respects. The three basic additions to international norms of copyright law were: (a) generalizing existing rights of distribution, broadcast, and public performance into the 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 the distribution and use of their works.

The generalized right to make 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.[49] It is,

---

[48] *See* WIPO Copyright Treaty, *opened for signature* Dec. 20, 1996, 36 I.L.M. 65, WIPO Publication No. 227(E) [hereinafter WCT], *available at* http://www.wipo.int/treaties/ip/wct; WIPO Performances and Phonograms Treaty, *opened for signature* Dec. 20, 1996, 36 I.L.M. 76, WIPO Publication No. 227(E) [hereinafter WPPT], *available at* http://www.wipo.int/treaties/ip/wppt.

[49] *See* WCT, *supra* note 48, arts. 6, 8, 36 I.L.M. at 69–70. 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 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

in a sense, an admission that despite the fact that past copyright law responded to technological developments in a piecemeal fashion, future copyright law should anticipate future developments by seeking 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 countries to implement it. The troika of new copyright norms were drafted in sufficient generality that implementation of the norms quickly became an area of intense jockeying by interested parties.[50] Generalizing the author's right to control dissemination of the work was perhaps the easiest element of the two treaties to implement because that norm was already expressed in most countries' copyright laws and/or can be re-expressed again and again with each new technology. The implementation of rights management information and the WCT/WPPT protection of "technological measures" has been far more contentious.

The treaties require signatories to provide "effective legal remedies against the circumvention of effective technological measures that are used by authors" in the exercise of their copyright rights.[51] In other words, countries must provide 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 at all.[52]

It became quickly clear to interested parties that domestic implementation of new legal norms by the United States, the European Union, and Japan would determine the actual content of international legal norms. The provisions of the DMCA and the European

---

"communication to the public." *See also* WPPT, *supra* note 48, arts. 8, 10, 36 I.L.M. at 83 (showing that the WPPT has provisions that parallel those in the WCT).

[50] 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), *opened for signature* May 23, 1969, 1155 U.N.T.S. 331 (stating that when 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").

[51] WCT, *supra* note 48, art. 11, 36 I.L.M. at 71; WPPT, *supra* note 48, art. 18, 36 I.L.M. at 86.

[52] *See, e.g.*, 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.18[A] (2002).

Union Copyright Directive[53] on "technological measures" are sufficiently consistent that they de facto fill the "content" of these WCT/WPPT legal norms,[54] although a few countries, like Burkina Faso and Australia, believe that they can meet the treaty obligations with much less normative content.

In the world of policy and law, negotiations of multilateral treaty obligations and their subsequent implementation are high profile affairs, so much so that people sometimes see them as the sole means of harmonizing law. For example, one commentator, looking at the Internet in 1998 and citing the eight years needed to negotiate the WTO Agreements, concluded that "harmonization of legal standards is not a realistic solution to global information issues."[55] 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 this has been the 1996 UNCITRAL model law on electronic commerce.[56] A more subtle and successful example is the Uniform Dispute Resolution Policy (UDRP) for addressing "cybersquatting" disputes between domain name (or DN) registrants and trademark (or TM) holders.

---

[53] *Compare* Digital Millennium Copyright Act, 17 U.S.C. §§ 1202–1205 (2000) *with* Council Directive 2001/29/EC, 2001 O.J. (L 167), *available at* http://www.eurorights.org/eudmca/CopyrightDirective.html.

[54] 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 United States and the European Union have established prohibitions on technological protection measures that attack controls on *access*; however, if access is a *right* of copyright holders, it has usually been a right protected by real property law (control of access to cinemas and concert halls, etc.) rather than copyright law. Alain Strowel, *Droit d'auteur et accès à l'information: de quelques malentendues et vrais problèmes a travers l'historie et les développements récents*, 12 LES CAHIERS DE PROPRIÉTÉ INTELLECTUELLE 185, 206–08 (1999) ("[L]a partie la plus importante de cette reglementation concerne les measures touchant à l'accès, mais, en revancne, à l'égard de ces measures, aucune obligations n'existe en vertu des Traites de l'OMPI" and observing that this might cause a divergence in norms).

[55] Reidenberg, *Lex Informatica*, *supra* note 39, at 577.

[56] *Model Law on Electronic Commerce with Guide to Enactment*, G.A. Res. 162, UNCITRAL, 51st Sess. (1996), *available at* http://www.uncitral.org/english/texts/electcom/mlecomm.htm [hereinafter UNCITRAL E-Commerce Model Law].

The problem of "cybersquatting" arises when A controls a domain name that is the same or substantially similar to 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 simply an address on the Internet, not a communicative message. Although superficially appealing, this has *always* been a bogus argument. A domain name of the form "http://www.paed.uscourts.gov" is not really an *address*: the actual address for the Web site of the United States District Court for the Eastern District of Pennsylvania is "http://204.170.64.143." If that court's Web site is located on the particular server that hosts it, the court has no choice but to accept that numeric address just as one has no choice in one's street or road address if one wants to live in a certain house.

The domain name system, however, creates memorable alphanumeric names that are overlaid upon and correspond to the actual Internet addresses. A better analogy to real world addresses involves the modern trend of corporate entities identifying their buildings with names such as "One Chase Plaza" or "Trident Center." These "addresses" do not eliminate the numbered street addresses; they are simply overlaid on top of the street addresses. And if "Trident Center" were 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. To reach reasonable results, however, courts often had to stretch and distort traditional trademark notions of unfair competition, initial interest confusion, and dilution.[57]

In 1999, WIPO produced a report at the behest of the Internet Corporation for Assigned Names and Numbers (ICANN) on how to handle DN/TM disputes in the generic top level domains (gTLDs) administered by ICANN. The report became the basis for the UDRP, a

---

[57] *See, e.g.*, Porsche Cars N. Am. v. Porsche.net, 302 F.3d 248, 261 (4th Cir. 2002) ("[T]he enactment of ACPA eliminated any need to force trademark dilution law beyond its traditional bounds in order to fill a past hole . . . ."); Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 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.").

mandatory, but non-binding arbitration procedure for any party that registers a domain name in the .com, .net, or .org environments.[58] Under the UDRP, a trademark holder can recover a DN in one of these gTLDs on a showing:

- 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,
- that the DN has been registered and is being used in bad faith.[59]

The UDRP then provides an elaborate, but non-exhaustive list of evidence for and against "bad faith" registration and use.[60]

The UDRP has suffered from occasionally questionable, inconsistent, and/or celebrity-solicitous decisions.[61] Nevertheless, the UDRP remains a powerful example of *lex Internet* through a model law. Although originally drafted, promoted, and promulgated to apply only to three gTLDs (.com, .net, and .org), the UDRP's principles have quickly been adopted for new generic TLDs.[62] More importantly, the UDRP has become the basis for dispute resolution standards in at least twenty-five country's TLDs (ccTLDs). Countries such as Mexico, Venezuela, and Guatemala have adopted *both* the actual UDRP mechanisms *and* the arbitral institutions.[63] In addition, countries such

---

[58] *Uniform Domain Name Dispute Resolution Policy*, ICANN (Sept. 29, 1999) [hereinafter UDRP], *available at* http://www.icann.org/udrp/udrp-policy-29sept99.htm.

[59] *Id.* ¶ 4(a)(i)–(iii).

[60] *Id.* ¶ 4(b).

[61] ANDRE R. BERTRAND, LE DROIT DES MARQUES, DES SIGNES DISTINCTIFS ET DES NOMS DE DOMAINE 578–83 (2002) (noting "the numerous contradictory decisions rendered on identical facts" and the very broad definition of "trademark" used by WIPO UDRP panels); Laurence R. Helfer & Graeme Dinwoodie, *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*, 43 WM. & MARY L. REV. 141, 255–56 (2002); *see also* Ian L. Stewart, Note, *The Best Laid Plans: How Unrestrained Arbitration Decisions Have Corrupted the Uniform Domain Name Resolution Policy*, 53 FED. COMM. L.J. 509, 518–22 (2001) (arguing that the arbitration process, being unrestrained, has damaged an otherwise decent dispute resolution process, using cases involving celebrities' names as an example).

[62] For example, paragraph 4(a) of the Start-Up Trademark Opposition Policy ("STOP") for the .biz gTLD repeats the UDRP three part test.

[63] BERTRAND, *supra* note 61, at 579 (counting Romania, the Philippines, the Bahamas, and Cyprus as countries that have adopted UDRP arbitration at WIPO for their country TLDs).

as Japan and Singapore have adopted the UDRP verbatim or almost verbatim.[64]

The United States has passed its own Anti-cybersquatting and Consumer Protection Act (ACPA) that wanders from the precise UDRP formula, but its nine factor test for bad faith hones close to the UDRP's understanding of the conditions that should trigger a DN transfer.[65] 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.[66] 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, UDRP decisions are recognized as a "pertinent jurisprudential source" for deciding cases.[67]

The model effect can also strengthen the emerging international legal norms by affecting law at the *sub-national* level. For example, judiciary guidelines promulgated in August 2000 by the Beijing Higher People's Court 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."[68] 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,

---

[64] When a "Singaporean entity" adopted dispute resolution procedures to deal with claims of cybersquatting in the ".sg" space, the Singaporeans adopted ICANN's UDRP almost whole cloth but added a distinct mediation procedure. *See Singapore Domain Name Dispute Resolution Policy*, Singapore Network Information Centre (SGNIC) (Nov. 6, 2001), *available at* http://www.nic.net.sg/pdf/SDRP.pdf. The Singaporean entity did, however, add a mediation process; paragraph 4(e) provides that the parties will be invited to consider whether they wish to have 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. *Id.* ¶ 4(e).

[65] The ACPA has a non-exhaustive nine factor test that is very similar to the conditions of UDRP Article 4(a) and (b) together. *Compare* 15 U.S.C. § 1125(d)(1)(B)(i) (2000), *with* UDRP, *supra* note 58, ¶¶ 4(a)–(b).

[66] *Dispute Resolution Service*, Nominet.uk: The UK Internet Names Organization, ¶¶ 3, 4, *at* http://www.nominet.org.uk/ref/drs-policy.html (last visited Mar. 2003).

[67] BERTRAND, *supra* note 61, 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.")

[68] *Guidelines Set Forth for Hearing Cybersquatting Cases*, Beijing Higher People's Court (Aug. 2000), *available at* http://www.cpahkltd.com/Newsletter/DomainCase.html.

> 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 right-holder 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 name is registered and used in bad faith.[69]

Given the difficulty of translating western legal text into Chinese, this is clearly an effort to hone close to 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 Web site for profit, creating deliberate confusion with the trademark, preventing someone else from "registering the trademark and business name as a domain name; or register[ing] the domain name for the purpose of impairing another person's business good will."[70] These are all familiar types of bad faith conduct from the UDRP and its jurisprudence.

Thus, the UDRP has helped prevent development of inconsistent national standards for cybersquatting cases[71]—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" means that as soon as dispute principles are 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 internation-

---

[69] *Id.* art. V.

[70] *Id.*

[71] A possible example is Belgium's proposal of, but final decision against enacting, an anti-cybersquatiing law. *See* ALEXANDRE CRUQUENAIRE, LE REGLEMENT EXTRAJUDICAIRE DES LITIGES RELATIFS AUX NOMS DE DOMAINE 19–21 (2002).

ally (liquor brands), or that need to appear Internet savvy).[72] 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."[73]

Such a "tipping" effect, however, 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 attention they received, the UNCITRAL rules on electronic contracting had the potential to do this, but they have not had influence on the scale of the UDRP.[74] 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 extend jurisdictional treatment reciprocally to Internet 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

---

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

[73] Ha'Aretz Daily Newspaper Ltd. v. United Websites, Ltd., (WIPO Arbitration and Mediation Center, No. D2002-0272 (July 3, 2002) (Mueller, Arb., dissenting).

[74] 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. *Compare* UNCITRAL E-Commerce Model Law, *supra* note 56, *with* Electronic Signatures in Global and Nat'l Commerce Act, 15 U.S.C. §§ 7001–7006, 7021, 7031 (2000) *and* UNIFORM ELECTRONIC TRANSACTIONS ACT (Proposed Official Draft, 1999), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

where genuine agreement can be forged. The UDRP disavowed a wide range of DN problems: conflicts 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 one person holds trademark rights and another person holds the 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,[75] 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 convergence, 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 phenomenon 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 be expected when animals from different lines of descent have had to overcome especially demanding problems in order to survive" in the same environmental niche.[76] Legal systems respond separately to a changing environment and may, like animals, make the same adaptations, so

---

[75] 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 Law approved a series of amendments to UCITA on August 2, 2002. *See* AMENDMENTS TO UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (Proposed Official Draft 2002), *available at* http://www.law.upenn.edu/bll/ulc/ucita/UCITA_Amds_AM02.htm; *see also* Ted Bridis, *Group Oks Changes for Net Commerce* (Aug. 6, 2002), *available at* http://www.siggraph.org/pub-policy/pdf/ECommerce.pdf.

[76] Janet Moore & Pat Willmer, *Convergent Evolution in Invertebrates*, 72 BIOLOGICAL REVS. CAMBRIDGE PHIL. SOC'Y 1, 3 (1997). Whales provide an example of "convergent design" because whales, despite being genetically closer to humans than fish, are designed more like fish because they live in an aquatic environment. *See also* John O. Hunter & Jukka Jernvalla, *Hypocone as a Key Innovation in Mammalian Evolution*, 92 PROC. NAT'L ACAD. SCI. 10718 (1995) (describing convergent tooth designs in animals).

that the "descendent" laws (animals) in different countries look more like one another than like their respective ancestor laws (animals).[77]

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 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 ISP liability and, second, basic legal treatment of electronic signatures and documents.

1. Internet Service Provider Liability

One of the earliest legal issues facing the Internet was the liability of ISPs for torts committed by non-related persons through the Internet. Serious slander and libel got to the Internet 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 1995, in *Stratton Oakmont v. Prodigy*, a New York court held an ISP strictly liable as the publisher of defamatory comments made by an unidentified party on one of Prodigy's bulletin boards.[78] In the same spirit, the United States Department of Commerce's early analysis of copyright and Internet issues analogized ISPs to publishers, putting substantial liability on them for third party infringements.[79] In 1999, in *Godfrey v. Demon*, the Queen's Bench also concluded that a United Kingdom ISP could be

---

[77] Moore and Willmer define "convergent evolution" as occurring "when distantly related animals evolve separately, yet produce similarity: the descendants are therefore more alike than were the ancestors." Moore & Willmer, *supra* note 76, at 5; *see also* SIMON CONWAY MORRIS, THE CRUCIBLE OF CREATION 202–03 (1998) (showing animals from divergent ancestries that converge in body design).

[78] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *3 (N.Y. Sup. Ct. May 24, 1995).

[79] *See generally* BRUCE LEHMAN, U.S. DEP'T OF COMMERCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP IN INTELLECTUAL PROPERTY RIGHTS (1995).

liable under English defamation law if it had been advised of the alleged defamation.[80]

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

But market economics provides 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 either will be weighted down one by one by large defamation or infringement judgments or will be driven out of business by the enormous policing costs necessary to keep defamatory and infringing material off of their system. The costs cannot be passed on without severely limiting Internet access.

Barring improbable technology developments,[81] 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. One sees this result over and over again; in fact, one commentator recently noted that "the rules for ISPs [are] increasingly settled."[82]

In the United States, commentators and courts reacted swiftly to the *Stratton Oakmont* decision.[83] One example of the first choice of

---

[80] Godfrey v. Demon Internet Ltd., 2001 Q.B. 201, 212, 218–20 (1999). The *Godfrey* case was not a strict liability holding because Demon had been put on notice of the defamation. *See id.* at 206.

[81] Technological developments are improbable because all fixed works moving through the Net are (a) eligible for copyright and (b) potential carriers of defamatory material such that it would be very hard for an automated system to screen.

[82] Michael Geist, *Internet "Choke Points" Put the Squeeze on Content*, GLOBE & MAIL (Toronto), July 11, 2002, at B11.

[83] *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1377 (N.D. Cal. 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"); 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). *See generally* Sega Enters.,

completely shielding ISPs from liability is section 230 of the Consumer Decency Act of 1996 (CDA).[84] Section 230 of the CDA 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."[85] As long as a provider of "an interactive computer service" does not have responsibility "for the creation or development of [the] information," the provider is shielded from liability.[86] American courts have generously interpreted this provision.[87]

As to the second approach, significant jurisdictions such as the United States 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 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 is 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.

One can find the above-described formula in the United States' 1998 DMCA, a law giving ISPs a safe harbor from contributory and vicarious liability for copyright infringement.[88] This formula is also manifest in the European Union's 2000 Electronic Commerce Directive

---

Ltd. v. Maphia, 948 F. Supp. 923 (N.D. Cal. 1996); Playboy Enters., Inc. v. Chuckleberry Publ'g, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996).

[84] 47 U.S.C. § 230(c)(1) (2000).

[85] *Id.*

[86] *See id.*

[87] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330–35(4th Cir. 1997); Blumenthal v. Drudge, 992 F. Supp. 44, 49–53 (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).

[88] *See* 17 U.S.C. § 512 (2000).

and its implementing national legislation, a law concerning liability for third party defamation and intellectual property infringement.[89]

Internet defamation cases in Japan have followed the same general trend—which Japanese copyright officials recommended in December 2000 as a template for copyright infringement actions.[90] At 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 of China issued interpretative guidelines on "several issues relating to adjudication of and application of law to cases of copyright disputes on computer networks."[91] Article 5 of the interpretive guidelines 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, failure to take measures for removal and elimination of the infringing contents in order to eradicate the consequence of the infringement, the people's court shall investigate it and the network user, and impose joint liability thereon according to the provision of Article 130 of the General Principles of the Civil law."[92]

---

[89] *See* Council Directive 2000/31/EC, 2000 O.J. (L 178) 1, arts. 12–14 (on Certain Legal Aspects of Information Society Services, in Particular, Electronic Commerce, in the Internal market) [hereinafter E-Commerce Directive], *available at* http://europa.eu.int/comm/internal-market/en/ecommerce/2k-442.htm; *see also* Draft U.K. Electronic Commerce (EC Directive) Regulations 2002, arts. 17–19, *available at* http://www.dti.gov.uk/industry_files/pdf/regulations.pdf.

[90] Experts Working Group, First Sub-Committee, Copyright Council of Japan, *Interim Report (on Recourse and Punishment)* (Dec. 2000) (reporting on 1997 and 1999 Tokyo District Court cases regarding the issue of ISP liability).

[91] Adjudication Commission of the Supreme People's Court of China, 1144th mtg., *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* (Dec. 21, 2000), *available at* http://www.cpahkltd.com/Archives/nterpretation_by_the_Supreme_People.html.

[92] *Id.* art. 5.

The interpretative guidelines reflect the familiar ideas of shielding the ISP from liability in the other direction.[93]

In 2002, some content providers started casting about for new ways to increase ISP liability or to find, to use Michael Geist's phrase, other "choke points" in the infrastructure of the Internet where liability could be applied against available "deep pockets."[94] I believe that most of these "deep pocket" entities will be able to adopt the same "structural" positions as the ISPs. Without these entities, 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 reasonably to 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 private third parties, but pressure the same access providers into "pacts" to filter content dangerous to the state. In the same spirit, in October 2001, in *J'accuse v. General Communications*, a Paris court declined to hold French ISPs responsible for a hate-speech site hosted in the United States and accessible in France-but the court noted that "it will not be possible to delay much longer the debate on a more active participation by all Internet participants, . . . including access providers."[95]

---

[93] 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[] be liable for breach of contract." *Id.* art. 8. Article 8 also transfers liability for such "claims for compensations for damages" to "the person giving the warning," i.e. the copyright holder. *Id.*

[94] Geist, *supra* note 82, at B11 (reasoning that given that ISPs are shielded from liability, the new targets are credit card companies and Internet search engines). For example, in August 2002, a number of record companies filed a complaint against Internet backbone providers seeking to force them to block a China-based Web site, "http://www. Listen4ever.com," in *Arista Records v. AT&T Broadband* (S.D.N.Y. filed Aug. 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.

[95] J'Accuse v. Gen. Communications, et al., T.G.I. Paris, Oct. 30, 2001, No. RG: 01/57676, note Gomez ('[Q]u'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.'), *available at* http://www.foruminternet.org/telechargement/documents/tgi-par20011030.pdf. Judge Gomez' remarks came 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.

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 a highly developed, highly localized law subject to a great deal of "path dependency." But the Internet creates pressure 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 that 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 legal uncertainties must be solved or else the economy at issue will not have widespread electronic contracting; the solutions most likely not to be wrong are those that are minimal, general solutions to the uncertainty. The most obvious of 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[96] or could *not* be assumed to meet these requirements. For prudent people entering sizeable contracts, the latter uncertainty would be as lethal as being certain of legal shortcomings. One obvious answer to this dilemma is the adoption of "equivalence" rules.[97] Examples of "equivalence" rules include the following: 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

---

See Cons. const., July 23, 1996, D. 1996, 99, *available at* http://www.conseilconstitutionnel.fr/decision/1996/96378dc.htm.

[96] *See, e.g.*, Andrew D. Murray, *Entering into Contracts Electronically: The Real W.W.W.*, *in* LAW AND THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE 17, 19–20 (Lilian Edwards & Charlotte Waelde eds., 2d ed. 2000) (concluding that a "digital document" would have failed to meet document requirements under United Kingdom law in the late 1990s).

[97] *Id.* at 20. As early as 1996, UNCITRAL advocated such a "functional equivalence" approach. *See* UNCITRAL E-Commerce Model Law, *supra* note 56, ¶ 15 (explaining the "functional equivalent" approach).

as the functional equivalent of "sending" or "delivering" paper documents.[98]

This can be achieved by statutory provisions on "legal effect" that are increasingly common. Examples of such statutory provisions include the following: "Information shall not be denied legal effect or enforceability solely by reason that it is in electronic form" (Prince Edward Island, Canada);[99] "[T]he requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures . . . are applied" (Pakistan);[100] "A record or signature may not be denied legal effect or enforceability solely because it is in electronic form" (UETA, as codified in California);[101] and 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" would "result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means" (European Union).[102]

Beyond such baseline equivalencies, an economy may implement legal recognition of particularly secure methods of authentication, producing a "layered" structure of record authentication law, as the European Union did in its 1999 E-Signatures Directive.[103] The 1999 Directive established a legal framework for a system of "advanced electronic signatures which are based on a qualified certificate and which are created in a secure-signature-creation device."[104] Such "advanced" authentication schemes create problems in that they tend to specify technology or require bureaucratic structures unnecessary to the baseline "equivalency" provisions.

---

[98] *See* UNCITRAL E-Commerce Model Law, *supra* note 56, ¶ 15.

[99] Electronic Commerce Act, R.S.P.E.I., ch. E 4.1, art. 4 (2001).

[100] Electronic Transactions Ordinance Promulgated (Sept. 11, 2002), DAWN, *available at* http://www.dawn.com/2002/09/12/top15.htm.

[101] CAL. CIV. CODE § 1633.7(a) (West Supp. 2003). Section 1633.7(b) similarly provides that "[a] contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation." *Id.* § 1633.7(b).

[102] E-Commerce Directive, *supra* note 89, at art. 9(1).

[103] Council Directive 1999/93/EC, 1999 O.J. (L 13) 12–20 (explaining the European Community's framework for electronic signatures), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

[104] *Id.* For a full exploration of the E-Signatures Directive and its implementation in France, see generally THIERRY PIETTE-COUDOL, LA SIGNATURE ÉLECTRONIQUE (2001).

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 us consider two candidate examples.

a. *The Single Publication Rule in Defamation Law*

The single publication rule can have an important impact on the measure of damages and on the time within which one can bring a defamation action. 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.[105] This idea was easy to apply to an orator standing on the corner of Green Park, but the idea loses much of its sensibility when applied to newspapers and books, situations where one defamatory written statement is given to many different people at different places over a single day or over many years. The response to this problem was the "single publication" rule: as long as the defamatory statement remains unchanged, wide distribution of a defamatory statement across geography and time would be treated as *one* publication.[106]

With the Internet, defamation plaintiffs have argued, and will continue to argue, that each downloading of a defamatory statement constitutes a separate publication. One argument claims that the "pull" nature of the Internet makes for a different result than with "push" distribution by traditional publishers.[107] Courts are likely to reject this kind of argument and coalesce around a kind of single publication rule that as long as the defamatory Web site or Internet posting remains unchanged, sequential hits, visits, and/or downloads do not constitute separate publications. Judicial economy—its own sub-category of "market forces"—offers one reason for such convergence. Another reason is the equitable notion common to most societies: a party should not sleep on his or her rights.

---

[105] *See, e.g.*, Duke of Brunswick v. Harmer, 14 Q.B. 185, 188–89 (1849).

[106] Gregoire v. G.P. Putnam's Sons, 1 N.E.2d 45, 46–49 (N.Y. 1948) (finding that a publisher's sale from stock of a copy of a book containing libelous statement was not a new publication); Wolfson v. Syracuse Newspapers, Inc., 4 N.Y.S.2d 640, 642–43 (App. Div. 1938), *aff'd no op.*, 18 N.E.2d 676, 676 (N.Y. 1939); RESTATEMENT (SECOND) OF TORTS § 577A[3] (1977).

[107] Firth v. State, 75 N.E.2d 463, 465 (N.Y. 2002) (arguing 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 limitations.").

b. *Exceptions and Limitations to Copyright Law*

Exceptions and limitations to copyright law are an area of national divergence and, at times, idiosyncrasy, but there are nonetheless common enough themes for one to think that economic and civil society forces might push us toward greater convergence in this area. Alain Strowel has noted five basic types of copyright exceptions that are the most important in an "information society": private copying, citation/quotation, news reporting, education and research, and library and archive exceptions.[108] More importantly, he notes that these exceptions essentially reduce to three "principal finalities": the private sphere, circulation of information, and cultural and scientific development.[109]

The basic notion in all of these examples is that the technological/economic environment causes a kind of "converge or abandon the environment" phenomenon—create electronic signatures or abandon meaningful e-commerce. While I believe that this actually occurs, the failure of grander visions of technological determinism related to the Internet adds 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."[110]

D. *Continued Diversity and Divergence in Legal Norms*

In contrast to the three categories above, in some areas of law, divergence in the dominant norms in national legal systems will continue to affect the Internet. The most visible of these areas of law is the law of free expression, part of First Amendment jurisprudence.

There is no better manifestation of abiding differences about free expression than the dueling decisions in the *LICRA v. Yahoo!* dispute. In 2001, in *LICRA*, a Paris court found that it had jurisdiction to order Yahoo!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 Inter-

---

[108] Strowel, *supra* note 54, at 198.

[109] *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.").

[110] Richard J. Ross, *Communications Revolutions and Legal Culture: An Elusive Relationship*, 27 LAW & SOC. INQUIRY 637, 639 (2002).

net. The French court subjected the companies to hefty fines for any failure to comply.[111] Less than a year later, a district court in San Jose, California granted Yahoo! summary judgment against any possible enforcement of the Paris court's ruling, basing its decision on First Amendment grounds.[112]

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 United States, forced to explain its particularly robust vision of free expression to other democratic, civil societies that do not have the same constitutional insistence.[113] In the middle camp is a group of democratic countries that forbid—and sometimes prosecute—"hate speech."[114] At the other extreme are countries like China, Saudi Arabia, and Zimbabwe that forbid—and regularly move against—a wide range of Internet speech that they deem dangerous or destabilizing.

Following the powerful language of the United States Supreme Court in *Reno v. ACLU*, the United States seems fixed in its views of free expression on the Internet.[115] It is tempting to predict that the United States 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 *LICRA*, the European Court of Justice (ECJ) has reversed recent French decisions enforcing speech restrictions against a biographer of Petain and anti-Semitic political activists. The ECJ's jurisprudence reflects not just European

---

[111] UEJF et LICRA v. Yahoo!, Inc., T.G.I. Paris, Nov. 20, 2000, No. RG: 00/05308, *available at* http://www.cdt.org//speech/international/001120yahoofrance.pdf.

[112] Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1189–91 (N.D. Cal. 2001).

[113] Philip Reitinger, Legal Aspects of Government-Sponsored Prohibitions Against Racist Propaganda on the Internet: the US Perspective, Presented at the Seminar on the Role of the Internet with regard to the International Convention on the Elimination of All Forms of Racial Discrimination in Geneva, Switzerland (Nov. 10–14, 1997), *available at* http://www.unhchr.ch/html/menu2/10/c/racism/reitinger.htm.

[114] *See, e.g.*, Associated Press, *Norwegian Convicted of Racism on the Internet in a Rare Case* (Apr. 24, 2002) (describing an April 24 Norwegian conviction for racist speech and a March 7 judgment in Sweden against a tabloid that allowed racist comments on its Internet chat site), *available at* http://www.lexis-nexis.com/universe.

[115] *See* 521 U.S. 844 (1997); *see also* Am. Library Assoc. v. United States, 201 F. Supp. 2d 401, 489–90 (E.D. Pa. 2002) (characterizing the Internet as a "public forum" for First Amendment purposes and declaring unconstitutional Congressional tying of library funding to use of ineffective pornography filtering programs).

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."[116]

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,[117] and we should avoid that same mistake when pondering the fate of law on the Internet.

III. WHERE THE VERDICT IS STILL OUT

Many areas remain in which 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. In those areas, we may discover—to 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 the following: extra-copyright protection of databases, protection of the privacy of personal information, the "cultural exception" for audiovisual works in international trade, and 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 above-mentioned examples.

The problem of extra-copyright protection of databases arose from early 1990s court decisions in the United States and Europe that denuded large, comprehensive databases of copyright protection just as the prospect of digital trade in such databases was becoming ap-

---

[116] *Universal Declaration of Human Rights*, art. 19, G.A. Res. 217 A(III) U.N. GAOR, 3d Sess., at 71, 74–75, U.N. Doc. A/810 (1948), *reprinted in* THE UNIVERSAL DECLARATION OF HUMAN RIGHTS 1948-1988: HUMAN RIGHTS, THE UNITED STATES AND AMNESTY INTERNATIONAL (Amnesty International USA 1988).

[117] *See, e.g.*, MAURO F. GUILLEN, THE LIMITS OF CONVERGENCE (2001) (describing the non-convergence of business practices in Spain, South Korea, and Argentina).

parent.[118] 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. As a result, by the time of the December 1996 WIPO Diplomatic Conference, database protection had to be taken off the negotiating table. In short, an early attempt at "top-down" convergence failed.

Since 1998, Congress has considered various bills to establish some kind of extra-copyright protection of databases in the United States. via a misappropriation or unfair competition approach, although no serious empirical demonstration of the need for additional intellectual property in this area has come to light. 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 European Union promulgated a Data Privacy Directive[119]—a directive that 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 the European Commission on this problem with no apparent convergent norms in sight beyond some early and potentially useful guidelines from the Organization for Economic Cooperation and Development (OECD).

---

[118] For an exhaustive account, see Justin Hughes, Political Economies of Harmonization: Database Protection and Information Patents, Presented at the Institut Français de Relations Internationales (June 10, 2002), *available at* http://www.ssrn.com/abstract_id=318486. The cases in question included *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, 499 U.S. 340 (1991), and *Rudolf Jan Romme/Van Dale Lexicograpfie B.V.*, HR 4 Jan. 1991 (translated in PROTECTING WORKS OF FACT 93 (Egbert J. Dommering & P. Bernt Hugenholtz eds., 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 1, at 40 n.79.

[119] Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (focusing on the protection of individuals with regard to the processing of personal data and on the free movement of such data), *available at* http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

CONCLUSION

Consider observations from two thinkers who are decidedly *not* cyber-*anything*. Surveying the legal scene in 1995, Harold Berman questioned the adequacy of "international law" and "transnational law" as conceptual categories for law when the non-lawyers talk about the economy, the environment, and society in terms of "world" and "global."[120] 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."[121] 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.[122] 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."[123]

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 scholars as well as activists.

Common legal norms are being forged which will sink much deeper into national legal systems than did traditional norms of "international" or "transnational" law that 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."[124] The conceptual give and take, the development of new categories and metacategories for law, will be about as interesting as law gets. On every

---

[120] Harold J. Berman, *World Law*, 18 FORDHAM INT'L L.J. 1617, 1617–22 (1995).

[121] *Id.* at 1622.

[122] *See* FREDRIC JAMESON, POSTMODERNISM OR, THE CULTURAL LOGIC OF LATE CAPITALISM 38 (1991).

[123] *See id.*

[124] LUCAS, *supra* note 1, at 13–14.

one of the topics mentioned in this Article, we are very far from the last word.