1-1-2007

Messages from the Front: Hard Earned Lessons on Information Security from the IP Wars, 16 Mich. St. J. Int'l L. 71 (2007)

Doris E. Long
John Marshall Law School - Chicago, profdelong@gmail.com

MESSAGES FROM THE FRONT: HARD EARNED LESSONS ON INFORMATION SECURITY FROM THE IP WARS

Doris E. Long[*]

ABSTRACT

Cyberspace is often a battlefield with a wide array of armies posed to challenge one another across the increasing array of rhetoric and technology that has made it such a potent arena for global digital commerce. Perry Barlow's infamous demand that cyberspace be left to its own devices because of its unique unregulated nature may have been answered by Larry Lessig's reply that code may in fact be used to regulate cyberspace, but the reality is that social norming demands, the evanescence of technological controls, and the perceived utility of illicit conduct utilizing the internet make any regulation problematic at best. Similarities between critical issues in the two areas suggest that some of the lessons learned in the hard-fought battles over legal protection for intellectual property in the digital world may provide guidance for the critical issues currently under discussion in the on-going efforts to establish international protection norms in the e-commerce domain. Compressed into ten lessons, involving such critical issues as the distinction between protected information in the hard goods world versus cyberspace, the role of technology, and the international needs of electronic communication, these lessons lead to the ultimate conclusion that in crafting rules, policy must be created with a firm view toward the special nature of the internet and in maintaining its potential to level the commercial playing field to allow all countries to participate in their own economic and commercial development.

---

* Professor of Law and Chair, Intellectual Property, Information Technology and Privacy Group, The John Marshall Law School and Visiting Professor, Michigan State University, College of Law. I would like to thank the organizers of the E-Commerce Conference on Challenges to Privacy, Integrity and Security in a Borderless World for the opportunity to present an earlier version of this Article. I would also like to thank Leslie Reis, Director of the Center for Privacy and Information Technology Law of The John Marshall Law School, for her helpful insights into some of the challenges facing those who seek to establish international security standards for e-commerce. As always, any mistakes in understanding belong solely to me.

TABLE OF CONTENTS

INTRODUCTION

There is no question that the internet[1] changed in the 1990's from a largely information and communication medium to a medium of commerce.[2] Despite over a decade dealing with the reality of the internet as a global digital marketplace, however, we continue to struggle to determine what laws from the so-called "hard goods" world need to be modified to assure the orderly functioning of this increasingly complex and varied new marketplace. Economists, such as Don Tapscott, have described the new "wikinomics" of the internet, as collaboration becomes a new social norm,[3] while Chris Anderson describes the "long tail" that has emerged as niche marketing becomes not only a reality in the new global digital marketplace, but perhaps even a necessity.[4] Even the development of a digital underground

---

1. Although common usage continues to use initial capitals to describe "the Internet," such usage no longer seems appropriate given the internet's wide-spread and long standing use. Just as "the Telephone" has become "the telephone," so too, it is time to recognize that "the Internet" has become an accepted and longstanding communication form which no longer needs to be treated with the exclamatory reverence of initial capital letters. Such special treatment, I believe, has been used in part to relieve international law of its responsibility to resolve the legal issues surrounding intellectual property on the internet. Capital letters subconsciously tell us all that the "Internet" is something new, so new that we cannot yet be expected to deal with the problems it poses. The time for such complacency, along with the initial capital letters, is long past.

2. *See, e.g.*, JOSEPHA SHERMAN, THE HISTORY OF THE INTERNET (2003); JOHN NAUGHTON, A BRIEF HISTORY OF THE FUTURE: FROM RADIO DAYS TO INTERNET YEARS IN A LIFETIME (2000); CHRIS ANDERSON, THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE (2006).

3. DAN TAPSCOTT & ANTHONY D. WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2006).

4. ANDERSON, *supra* note 2.

marketplace composed of darknets, peer-to-peer trading in copyrighted works, and other illicit economic activities has begun to be recognized and discussed.[5] Yet on the legal side of the fence, we remain mired in debates at both the domestic and international level over the shape of regulation of this exponentially expanding marketplace. In fact, claims harkening back to the earliest days of development that cyberspace should either remain unregulated – the wild west of the 21st Century – or should only be regulated by the social norms developed by its end users create a constant background noise.[6] Perry Barlow's infamous

---

5. *See, e.g.*, Doris Estelle Long, *Strategies for Securing the Cyber Safety Net Against Terrorists: A Multi-Disciplinary Approach*, OXFORD FORUM ON PUBLIC POLICY (forthcoming 2007) (copy on file with author) (discussing the development of diverse underground markets, including those based on spam and other illicit uses of the technological advantages of the internet) [hereinafter Long, *Strategies*]. *See also* PETER GRABOSKY, RUSSELL G. SMITH & GILLIAM DEMPSEY, ELECTRONIC THEFT: UNLAWFUL ACQUISITION IN CYBERSPACE (2001) (detailing diverse illicit uses of cyberspace); SAMUEL C. MCQUADE, III, UNDERSTANDING AND MANAGING CYBERCRIME (2006) (analyzing the opportunities for crime presented by cyberspace, including alternative views of deviant behavior); JOHN BIGGS, BLACK HAT: MISFITS, CRIMINALS AND SCAMMERS IN THE INTERNET AGE ch. 6 (2004) (detailing the black market for copyrighted and pirated goods).

6. *See, e.g.*, Daniel J. Gervais, *The Price of Social Norms: Towards A Liability Regime for File-Sharing*, 12 J. INTELL. PROP. L. 39 (2004) (analyzing the utility of social norms in creating international protection standards); Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49 (2006) (implying that social norms should be considered in changing DMCA to allow fair use); JESSICA LITMAN, DIGITAL COPYRIGHT (2001) (advocating relying on normative behavior to reform copyright law for the Digital Age) [hereinafter LITMAN, DIGITAL COPYRIGHT]; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (suggesting that norms regulate cyberspace) [hereinafter Lessig, *Law of the Horse*]; MARK SABLEMAN, MORE SPEECH, NOT LESS: COMMUNICATIONS LAW IN THE INFORMATION AGE (1997) (advocating end user regulation of content through norming processes). *Cf.* STEVEN HETCHER, NORMS IN A WIRED WORLD (2004) (analyzing the social conformity role of norms in internet privacy behaviors). I do not mean to suggest that social norms should play no role in the consideration of the legal regime governing internet based activities. Such norms are helpful in determining the demands which society may make of the internet. Thus, for example, the development of social networking sites, and the increased ability of end users to manipulate third parties' works to create mash ups, parodies and other transformations, has raised serious questions about whether the types of uses considered "fair" under copyright doctrines should be expanded to permit such new uses. *See, e.g.*, ROSEMARY J. COOMBE, THE CULTURAL LIFE OF INTELLECTUAL PROPERTIES: AUTHORSHIP, APPROPRIATION AND THE LAW (1998) (detailing various appropriations of intellectual property that are part of today's reproduction culture); SIVA VAIDHYANATHAR, COPYRIGHTS AND COPYWRONGS: THE RISE OF INTELLECTUAL PROPERTY AND HOW IT THREATENS CREATIVITY (2001) (detailing the potentially harmful impact of current copyright regimes on the creation of new works); KEMBREW MCLEOD, FREEDOM OF EXPRESSION: OVERZEALOUS COPYRIGHT BOZOS AND OTHER ENEMIES OF CREATIVITY (2005) (discussing sampling and other techniques where copyright protection is used to stifle free expression and creativity); DAVID

demand that cyberspace be left to its own devices because of its unique unregulated nature[7] may have been answered by Larry Lessig's reply that code may in fact be used to regulate cyberspace.[8] But the reality is that social norming demands, which norms often exist outside current legal regimes (or at least operate in contradistinction to such regimes),[9] the evanescence of technological controls,[10] and the perception of illicit activity on the net as useful for achieving economic and other goals[11]

BOLLIER, SILENT THEFT: THE PRIVATE PLUNDER OF OUR COMMON WEALTH (2002) (advocating methods for reducing the enclosure of the commons through IP regulation which may ultimately free works for new uses). Yet I believe, for reasons too numerous to fully explain here, such norms should only serve as *guideposts* in creating an acceptable regulatory regime for the digital marketplace. The social norm of free use of copyrighted works on the internet (without regard to copyright or other mechanisms for authorial control) may serve the goals of the creation of *new* works, but may *not* serve the additional and *potentially equally important* goal of replenishing the public domain with works of *enriching* creativity. *See, e.g.*, Doris Estelle Long, *Dissonant Harmonization: Limitations on Cash 'n Carry Creativity*, ALB. L. REV. (forthcoming 2007) (manuscript on file with author) [hereinafter Long, *Dissonant Harmonization*].

7. *See, e.g.*, John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, at 84; Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19 (1996). For a popular culture history of the changing views of internet regulation with regard to copyright regimes, see TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE (2007).

8. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000) [hereinafter LESSIG, CODE].

9. These norms include demands for greater access and use of intellectual property protected works and stronger protection for the private nature of on-line activities. *See* sources cited *supra* note 6.

10. I have earlier described myself as a "technosceptic" and nothing in today's current technology battles has altered this point of view. Doris Estelle Long, *Is a Global Solution Possible to the Technology/Privacy Conundrum?*, Address at John Marshall Law School Symposium (Nov. 18, 2005), *in Copyright and Privacy: Collision or Co-existence*, 4 J. MARSHALL REV. INTELL. PROP. L. 242, 248-57 (2005) [hereinafter Long, *Global Solution*]. The modern history of cyberspace remains an arms race in technological control efforts, including the establishment of legal protection regimes for technological protection measures for copyrighted works that only serve to demonstrate how fleeting any efforts in this area remain. *Id. See also New Jersey Teen Cracks iPhone Network Lock,* ASSOCIATED PRESS, Aug. 24, 2007, *available at http://www.msnbc.msn.com/id/20424880*; John Schwartz, *iPhone Flaw Lets Hackers Take Over, Security Firm Says*, N.Y. TIMES, July 23, 2007, http://www.nytimes.com/2007/07/23/technology/23iphone.html; *Can Anyone Police File Sharing?*, INSIDE HIGHER EDUCATION, Aug. 3, 2007, http://www.insidehighered.com/news/2007/08/03/filesharing. In fact, efforts to control the technology used to prevent the unauthorized reproduction of motion pictures from lawfully distributed copies has proven so unavailing that a Finnish court recently declared the technology – CSS – unavailable for protection under national anti-circumvention statutes because it was so easily hacked. Helsingin käräjäoikeus, case R 07/1004, 25.5.2007. An English translation can be found at http://www.turre.com/css_helsinki_district_court.pdf. The case is currently on appeal.

11. *See, e.g.*, Long, *Strategies*, *supra* note 5; PAT CHOATE, HOT PROPERTY: THE

continue to play a critical role in the debate over the nature of market regulation of cyberspace. I do not mean to suggest that such issues should not be considered. I merely agree with many others who suggest that to achieve any sort of practical legal regime we must put aside rhetoric and consider the goals we seek to achieve in the digital universe.

Unfortunately, even when we put aside rhetoric, we are still faced with a lack of agreement on what are the precise changes that are required in applying hard goods regulation to cyberspace. Regardless of whether we are considering the application of jurisdictional rules, tax liability or copyright laws, the largely "borderless" nature of the cybermarket,[12] its international reach,[13] and its constantly changing content make the application of legal norms developed for a bordered world problematic at best.[14]

STEALING OF IDEAS IN AN AGE OF GLOBALIZATION (2005) (describing how countries used patent laws, including violations of those laws, to promote industrial and commercial development); DORON S. BEN-ATAR, TRADE SECRETS: INTELLECTUAL PIRACY AND THE ORIGINS OF AMERICAN INDUSTRIAL POWER (2004) (describing how the United States built its early commercial industries, including the printing and clothing industries, based on the pirating of other countries trade secrets and copyrighted works).

12. The lack of physical borders in cyberspace makes economic transactions difficult to regulate. In the hard goods world, the sale of illegal goods across international borders can be regulated through border measures which allow customs officials to inspect cargo and deny access to goods which violate local laws. Thus, for example, the U.S. Customs Service has the power to seize pirated goods at the physical borders of the United States. *See, e.g.*, 19 C.F.R. §§ 133.42-.46 (2003). *See generally* TIMOTHY TRAINER & VICKI ALLUMS, PROTECTING INTELLECTUAL PROPERTY RIGHT ACROSS BORDERS (2006). Such goods are usually detected through a physical inspection of the goods at the port of entry. By contrast, when pirated goods enter the United States through digital transmissions there is no physical good at the border to be inspected, making the discovery of any such goods unlikely. The lack of physical borders, however, does *not* mean that cyberspace lacks physical attachments per se. *See Special Report: Putting it in its Place - Geography and the Net*, ECONOMIST, Aug. 11-17, 2001, 18-20 (discussing the physical geography of the internet in the form of servers, cables, etc.). To the contrary, the right of countries to monitor content which is received or transmitted by users within the physical territory of a country has long been recognized. The lack of physicality, however, makes certain issues, such as the confirmation of verified contracts between parties or the determination of illegal content in digitally transmitted goods more difficult than in the hard goods, physical world.

13. While internet penetration differs on a country-by-country basis, there is no country which lacks at least some internet connectivity, even if such connectivity may be limited to the capital city. I myself have discovered internet cafes in such disparate and remote places as Kathmandu, Nepal, Lhasa Tibet and Conakry, Guinea. I do not mean to suggest that the existence of the internet in a capital city indicates a necessary parity in internet access. It does, however, demonstrate the potential global reach of the opportunities the internet provides if the adequate legal and communications infrastructures are provided.

14. The problems posed by the transitory nature of the internet was recognized early in

In considering the relationship between the demands of e-commerce, including in particular the protection of digital transaction documents and the protection of commercially significant information,[15] with the demands of intellectual property and the protection of a particular type of "information"[16] – that which is legally recognized as being creative and/or innovative[17] – I was struck by how many issues they share in common. These similarities suggest that some of the lessons we have learned in the hard-fought battles over legal protection for intellectual property in the digital world may provide guidance on some of the

---

legal scholarship regarding the newly emerging digital world. *See, e.g.*, Lessig, *Law of the Horse*, *supra* note 6. So too was the unique jurisdictional issues posed by a transaction space that lacked traditional physical borders. *See, e.g.*, David R. Johnson & David Post, *Law and Borders - The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (contending that cyberspace is a borderless environment which should be governed by its own legal regime); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998) (contending that the internet is a bordered world, governed by territorial sovereignty). *But see* JONATHAN WALLACE & MARK MANGAN, SEX, LAWS AND CYBERSPACE (1996) (contending that when it comes to speech issues, cyberspace requires no different treatment than other communications media, including television, cable and radio). What remains hotly debated is the extent to which the newly emerging market place of electronic commerce requires new or different applications of present legal regimes. *See, e.g.*, Jerome H. Reichman & Tracy Lewis, *Using Liability Rules to Stimulate Local Innovation in Developing Countries: Application to Traditional Knowledge*, *in* INTERNATIONAL PUBLIC GOODS AND TRANSFER OF TECHNOLOGY UNDER A GLOBALIZED INTELLECTUAL PROPERTY REGIME (Keith E. Maskus & Jerome H. Reichman eds., 2005); YOCHAI BENKLER, THE WEALTH OF NEWTORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006); LITMAN, DIGITAL COPYRIGHT, *supra* note 6; LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001).

15. Such information includes digital signatures and other authenticating information with regard to commercial transactions, as well as commercially sensitive information including customer or supplier identities, and purchase practices. This Article does not consider the whether such information should be propertized or otherwise "owned" by a particular party, but focuses instead on what issues need to be addressed in deciding the scope and nature of any such protection that may be established.

16. I use the term "information" advisedly. While patent protection, which attaches to novel, non-obvious, and useful inventions, might be applied to "information" including for example, methods and processes, copyright protection is expressly limited to protectible *expression*. 17 U.S.C. § 101 (1999) (excluding ideas, facts, etc. from protection under copyright law.). *See, e.g.*, Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539 (1985). I am using the term simply to mimic continuing claims that copyright protection should not apply to internet distributed works because "*information* wants to be free." *See, e.g.*, STEWART BRAND, THE MEDIA LAB: INVENTING THE FUTURE AT MIT 202 (1987).

17. Thus, for example, copyright law protects creative or original works of authorship while patent law protects innovative works that demonstrate the appropriate level of novelty, non-obviousness and utility. *See* 17 U.S.C. § 101; 35 U.S.C. § 101; TRIPS, *infra* note 130, at arts. 10, 27.

critical issues currently under discussion in the on-going effort to establish international protection norms in the e-commerce domain.[18]

I. AUTHENTICITY, FRAUD REDUCTION AND PRODUCTIVE BALANCES

In the IP world, similar to the world of e-commerce, we are concerned about authenticity, reducing fraud, and using the benefits of digital communication to provide for a more effective product distribution system, while assuring adequate protection for the contents of such digitally distributed goods and services. The protection of the distributional rights granted under IP regimes, however, is not limited merely to protection of distributed content but also assures competition by balancing the protection of such content against the needs of others to utilize such works in creating new (and presumably competitive) works.[19] This distributional right seems to mirror the fair competition concerns at the heart of much commercial regulation.

Guarantees of authenticity in intellectual property regimes are generally associated with trademark laws and geographic indications.[20] Yet the truth is such concerns extend to issues of copyright authorship[21]

---

18. I do not mean to suggest that intellectual property is not a part of what is generically referred to as the law of e-commerce. To the contrary, much of the goods and services which are the subject of the electronic commercial transactions that give rise to the digital protection issues that are the subject of this symposium contain intellectual property or implicate intellectual property in their creation. These goods include such well-known e-commerce staples as books, movies, music, software and photographs.

19. Thus, for example, copyright law has a strong fair use right that allows unauthorized third parties to use another's copyrighted work, even for commercial purposes under certain circumstances. *See* 17 U.S.C. § 107 (1992); *see generally* notes 60-67 and accompanying text *infra*. Similarly, patent law provides a limited scope of protection based on the claims themselves in order to permit workarounds. It also provides limited experimental use rights. *See, e.g.*, Madley v. Duke Univ., 307 F.3d 1351 (Fed. Cir. 2002), *cert. denied*, 539 U.S. 958 (2003) (rejecting an automatic experimental use exception even for academic research).

20. Although the particular nature of the source identifying function of a trademark has been debated, see, e.g., Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE L.J. 1687 (1999); Barton Beebe, *The Semiotic Analysis of Trademark Law*, 51 UCLA L. REV. 621 (2004); Stacey Dogan & Mark Lemley, *The Merchandising Right: Fragile Theory or Fait Accompli?*, 54 EMORY L.J. 461 (2005) (draft version *available at* http://www.chicagoip.com/dogan.pdf); Doris Estelle Long, *Is Fame All There Is?: Beating Global Monopolists at Their Own Marketing Game*, 40 GEO. WASH. INT'L L. REV. (forthcoming 2007) (copy on file with author), there is no doubt at least some of the information which consumers receive from such trademarks and other source designators including geographic indications, relate to the authenticity of the product or service in question.

21. In addition to the requirement that authors be the ones who "originate" the work,

and patent inventorship as well. Thus, for example, in addition to the well known struggles over the scope of rights to be granted authors over the use of their copyrighted works by others,[22] debates have also arisen over the scope of moral rights to be enjoyed by performers in connection with their digitally transmitted performances, including the right of performers and authors to be credited in subsequent uses of such works.[23] While the right of patrimony is generally associated with concerns over copyright authenticity,[24] international regimes require that inventorship also be recognized.[25] Concerns over "fraud" include not only legal prohibitions against the reproduction and distribution of counterfeit and pirated goods, [26] but extends to the use of commercial symbols and source designators that confuse the public about the true source or quality of the goods in question.[27] Such source designating

---

see, e.g., *Feist Publications Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991), the moral right of patrimony further assures that creators receive credit for the works they have created. *See, e.g.*, 17 U.S.C. § 106A (2000) (granting the author of a work of visual art the "right to claim authorship of that work"); Berne Convention for the Protection of Literary and Artistic Works, art. 6*bis*, Sept. 9, 1886, as revised at Paris on July 24, 1971 and amended in 1979, S. Treaty Doc. No. 99-27, 1161 U.N.T.S. 3 (granting authors the "right to claim authorship of the work," "independently of the author's economic rights") [hereinafter Berne Convention].

22. *See, e.g.*, Long, *Dissonant Harmonization*, *supra* note 6 and works cited therein. *See also* COOMBE, *supra* note 6; VAIDHYANDATHAN, *supra* note 6; MCLEOD, *supra* note 6; LITMAN, *supra* note 6.

23. *See, e.g.*, 17 U.S.C. § 106A (2000) (granting the author of a work of visual art the "right to claim authorship of that work."); Berne Convention, *supra* note 21, art. 6*bis* (granting authors the "right to claim authorship of the work," "independently of the author's economic rights").

24. *See, e.g.*, Berne Convention, *supra* note 21, art. 6*bis* (requiring countries to protect the right of authors to receive credit for their works); WIPO Performances and Phonograms Treaty, art. 5, Dec. 20, 1996, 36 I.L.M. 76 (1997) (granting patrimonial rights to performers in their performances) [hereinafter WPPT].

25. *See, e.g.*, 35 U.S.C. §§ 115, 118 (2002) (requiring that the inventor be named in patent application "as such"); Paris Convention, art. 4*ter*, revised at Stockholm July 14, 1967, 21 U.S.T. 1583, 828 U.N.T.S. 306 [hereinafter Paris Convention] (same).

26. *See, e.g.*, 17 U.S.C. § 511 (2002) (providing criminal penalties for the unauthorized distribution of copyrighted material); 18 U.S.C. § 2319 (2005) (same); 18 U.S.C. § 2320 (2006) (providing criminal penalties for the "traffick[ing] in goods or services and knowingly us[ing] a counterfeit mark on or in connection with such goods or services").

27. *See, e.g.*, Johnson & Johnson v. Carter-Wallace, Inc., 631 F.2d 186 (2d Cir. 1980) (regarding a claim of implicit false expressions about moisturizing nature of a depilatory with baby oil actionable under Section 43(a) of the Lanham Act); R.J. Reynolds Tobacco Co. v. Loew's Theatres, Inc., 511 F. Supp. 867 (S.D.N.Y. 1980) (passing off); Radio Today, Inc. v. Westwood One, Inc., 684 F. Supp. 68 (S.D.N.Y. 1988) (mislabeled products); Baskin Robbins Ice Cream Co. v. D&L Ice Cream Co., 576 F. Supp. 1055, 1060 (E.D.N.Y. 1983) (unbranded ice cream in branded cups); New Line Cinema Corp. v. Easter Unlimited, Inc., 17 U.S.P.Q. 2d 1631, 1633 (E.D.N.Y. 1989) (false merchandising sponsorship; Freddy Krueger gloves).

regulations include prohibiting spam,[28] the use of domain names intentionally selected to confuse the public or divert traffic onto a competitor's website,[29] and phishing.[30]

II. A TALE FROM THE DARK SIDE OF MUSIC

On the IP side of the fence, we have struggled to decide if the modes of protection established for commerce in intellectual property-based works in the hard goods world are sufficient, or even applicable, to the electronic marketplace. Technology has opened the possibilities of global commerce as a result of the new business models available through the internet. From a simple communication medium, the internet has developed into a global marketplace whose very existence has altered the nature of commerce itself. From "long tail" opportunities[31] to collaborative enterprises and Web 2.0,[32] the internet has changed both the opportunities for commerce and the challenges to protecting these new commercial opportunities from being usurped by the underground, unregulated market that flourishes alongside legitimate portals. There may be no better evidence of the potentialities and dangers of the electronic marketplace than the well-known history of the impact of technology and the internet on the music industry.

---

28. *See, e.g*, Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q. 2d 1020, 1026 (N.D. Cal. 1998). *See also* Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 552 (E.D. Va. 1998) (improper spam mailing held to tarnish plaintiff's mark because of use of "aol.com" on the header led to 50,000 subscribers' complaints).

29. *See, e.g.*, 15 U.S.C. §1125(d) (granting relief for the bad faith use or registration of a domain name that is confusingly similar or diluting of another's trademark). *See also* Google, Inc. v. American Blind & Wallpaper, 2007 WL 1159950 (N.D. Cal. 2007) (use of competitor's mark in metatag or for key word buy prohibited as confusing). *But cf.* FragranceNet.com, Inc. v. FragranceX.com, Inc., 493 F. Supp. 2d 545 (E.D.N.Y. 2007) (use of mark in key word buy was not considered actionable "use in commerce" under the Lanham Act).

30. Most identity thefts using the internet also employ false sponsorship or fake websites that can also be challenged under trademark doctrines. *See generally* Long, *Strategies*, *supra* note 5.

31. ANDERSON, *supra* note 2.

32. Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY NETWORK, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html; TAPSCOTT, *supra* note 3.

A. From Warez to BitTorrent: A Lack of Vision?

In the initial stages of commerce on the internet, music distribution sites were largely limited to websites owned by 'brick and mortar' companies who offered hard goods versions of legitimately distributed music for sale.[33] In short, the internet was perceived largely as an advertising medium or alternative distribution site for hard goods items. Warez sites that offered illegal copies of copyrighted works often at no charge quickly arose, but the large size of digital music files and the lack of adequate compression technology limited early warez sites to software.[34] The development of faster reproduction and compression technologies combined with Shaun Fanning's notorious development of an effective digital distribution system for music – the infamous Napster[35] – changed the commercial landscape for music and the internet virtually overnight. While legitimate sites offering lawful copies of music for download were relatively slow to develop, the creation of the iPod and its companion music download site iTunes helped fuel a renewed legitimate market in downloadable music.[36]

---

33. Probably the clearest examples were the offer for sale of music through websites for such well-known record distributors such as Tower Records.

34. *See generally No Electronic Theft Act: Hearing on H.R. 2265 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 104th Cong. (1997) (Statement of Kevin V. DiGregory, Assistant Attorney General, Criminal Division, U.S. Dept. of Justice) (describing current and future piracy issues raised by the development of warez sites and compression technologies, including methods of distribution of the same).

35. *See, e.g.*, JOSEPH MENN, ALL THE RAVE: THE RISE AND FALL OF SHAWN FANNING'S NAPSTER (2003). *See also* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (the software at issue allowed individuals to download musical compositions and sound recordings of copyrighted artists in MP3 format; it also allowed users to search and download MP3 files from any other user logged onto the internet, using a search index contained on the Napster website). The ultimate impact of peer to peer technology on the shape of copyrights in the digital age remains hard fought. While the Supreme Court most recently held the distributors of P2P software might be held contributorily liable for actively inducing end users to infringe music copyrights, see *Metro-Goldwyn Mayer Studios, Inc. v. Grokster Ltd.*, 545 U.S. 913 (2005), issues about the scope of a personal use right under fair use doctrines, remain hotly contested.

36. *Legal Music Downloading Leaps in 2005*, CBC, Jul. 13, 2005, http://www.cbc.ca/story/arts/national/2005/07/13/Arts/DownloadsUp_050613.html. *See* Mary Madden & Lee Rainie, *Music and Video Downloading Moves Beyond P2P*, PEW INTERNET & AMERICAN LIFE PROJECT, Mar. 23, 2005, http://www.pewinternet.org/pdfs/PIP_Filesharing_March05.pdf (describing the increase in numbers of individuals visiting sites that offer legitimate downloads of digital music).

Just as new business models for the commercial distribution of music have developed, new methods for increasing consumer demands for music have similarly been fueled by the appearance of a wide variety of social networking websites, such as YouTube[37] and MySpace,[38] where end users can post music, videos and other copyrighted works to "share" with visitors to these sites. These social networking sites not only encourage the posting of unauthorized versions of copyrighted works, they have encouraged the posting of end user created musical collages, parodies, pastiches and other derivative versions of third party music. The rapid creation and dissemination of such works has placed serious pressures on existing commercial music licensing techniques. Compulsory licensing has long existed for the *performance* of copyrighted music.[39] Similarly, numerous collective rights organizations have developed in the hard goods world to license the performance, broadcast and synchronization of music.[40] Collective rights organizations have even been developed to license the performance of *performers* in digital audio transmissions over the internet.[41] Yet, to date, no legitimate collective rights organization has developed to license the creation of third party derivative works for

---

37. YouTube, www.youtube.com (last visited Oct. 26, 2007).

38. MySpace, www.myspace.com (last visited Oct. 26, 2007).

39. 17 U.S.C. §§ 110, 114, 115.

40. In the United States, these organizations include American Society of Composers, Authors and Publishers (ASCAP), Broadcasting Music, Inc. (BMI), SESAC and Harry Fox. The first three are private collective rights organizations that authorize the broadcast of licensed music, the last one is a private collective rights organization that authorizes the synchronization of licensed music ("mechanical rights"). *See generally* The American Society of Composers, Authors, and Publishers (ASCAP), http://www.ascap.com/index.html; Broadcast Music, Inc. (BMI), http://www.bmi.com/; SESAC, http://www.sesac.com/index.aspx?flash=1; Harry Fox Agency (HFA), http://www.harryfox.com/index.jsp. In the digital world, in addition to the above organizations offering performance licenses for the internet, new licensing mechanisms have been developed to meet the challenges of licensing music for the Internet Age. *See generally* M. WILLIAM KRASILOVSKY, ET AL, THIS BUSINESS OF MUSIC (10th ed. 2007); Andrew Sparrow, MUSIC DISTRIBUTION AND THE INTERNET: A LEGAL GUIDE FOR THE MUSIC BUSINESS (2006); Soundies, http://www.soundies.com (last visited Oct. 26, 2007) (offering branded music for hard goods and digital distribution).

41. SoundExchange is one example of a digital audio performance collective licensing society. *See, e.g.*, http://www.soundexchange.com (last visited Oct. 26, 2007). Under U.S. copyright law, music performers are given the right to authorize the performance of their copyrighted performances "by means of a digital audio transmission." 17 U.S.C. § 106(4) (2002). They have no right to control the broadcast of such performances. *See id.* §106(4) (failing to include "sound recordings" among the covered works for which performance rights are granted).

posting on the internet.[42] The closest licensing mechanism that may presently exist is the Creative Commons license which allows the creator of a copyrighted work to pre-grant third parties the right to create derivative works, even in some cases for posting on the internet, subject to the limitations which original authors may place on such uses, including, for example, appropriate credit.[43] Worse, the problem of legal liability for the webcasting of music already authorized for broadcast in the hard goods continues to remain uncertain.

U.S. copyright law and international regimes governing intellectual property have long recognized that the transmission of a digital performance requires the consent of both the composer of the performed copyrighted composition *and* the performer of the music in question. Although in the hard goods world, performers are only granted the right to control the reproduction of their performances under U.S. copyright law,[44] in the digital world, performers' rights have been significantly expanded. With the enactment of the Audio Home Recording Act,

---

42. I do not mean to suggest that hard goods world collective rights organizations do not currently exist which can be used to authorize the digital transmission of music in webcasts. To the contrary, at least in the U.S., ASCAP, BMI and SESAC all offer internet licensing possibilities for the *musical compositions* within their catalogue. Similarly, there are collective rights organizations such as SoundExchange (www.soundexchange.com) which license *performances* for non-interactive webcasting. What is lacking, however, is any domestic or global licensing methodology that would allow the distribution of musical recordings through personal websites, or the creation and transmission of musical collages, mash ups and samplings through internet transmissions. In short, absent individually granted licenses, such as those which are currently negotiated between content providers and YouTube, no such licensing mechanism for the posting of end user created works exists. *See, e.g.*, WILLIAM FISHER, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT (2004). While some uses *may* be subject to a fair use defense, see, e.g., *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994) (rap parody of musical composition "Pretty Woman" held to constitute fair use under US copyright law), the presence of a global licensing mechanism might reduce the present lack of clarity over the scope of such rights. I do not necessarily support the development of such a global compulsory licensing mechanism. Given the administrative difficulties involved, I have serious reservations about the effectiveness of such a system. Nevertheless, clearly some form of collective licensing is required to meet the challenges of lawful internet use of copyrighted works. Furthermore, such licensing mechanisms should be transparent, easy-to-understand-and-comply-with, and competitive to assure adequate protection of authors' and performers' rights.

43. *See* Creative Commons, http://www.creativecommons.org. The most common limitation placed on a Creative Commons license appears to be the requirement that the author of the original source work be given credit.

44. *Compare* 17 U.S.C. § 106(1) (providing a reproduction right for all works) *with* 17 U.S.C. § 106(4) (failing to include "sound recordings among the covered works for which performance rights are granted).

Congress granted performers the right to control the digital audio transmission of their performances.[45] Similarly, at the international level, the WIPO Performances and Phonograms Treaty (WPPT) recognized the right of performers to control the fixation, reproduction and broadcast of their live performances.[46]

Despite the growing legal regime to grant performers and copyright owners rights to their musical works on the internet, the intersection between rules crafted for the hard goods world and their cyber application remain open questions. Thus, for example, the simple issue of the extent to which separate royalties for the simultaneous webcast of an authorized radio or television broadcast are required has been the subject of extensive litigation. Based on the position of the U.S. Copyright Office, webcasting requires additional royalties beyond those paid for hard goods broadcasting.[47] Royalty rates continue to drop as the parties struggle to find an equitable balance between authorial compensation and business needs.[48] However, part of the difficulty, at least for US based webcasters, lies in the fact that under U.S. law both performers and composers are entitled to compensation in the digital world.[49]

---

45. *Id.* § 106(6) (granting performers the right to authorize the digital audio transmission of their performances). Under Section 101, "to 'perform' a work" is defined as "to recite, render, play, dance or act it either directly or by means of any device or process" and necessarily includes the webcasting of recorded musical performances. *Id.* §101.

46. WPPT, *supra* note 24, art. 6-8 (granting performers the right to authorize the fixation of their live performances and to further authorize the reproduction and "making available" of such fixations). Article 2 of the WPPT defines performers as "actors, singers, musicians, dancers and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore," and clearly includes musicians and singers within its purview.

47. These additional fees are due to the need to compensate performers for their digital audio transmission rights under Section 106(6) of the US Copyright Act. 17 U.S.C. §106(6). *See also* notes 44-45.

48. *See, e.g.*, Small Webcaster Settlement Act of 2002, Pub. L. No. 107-321, 116 Stat. 2780 (codified at 17 U.S.C. § 114) (allowing for, inter alia, Sound Exchange, the designated collective rights society, to establish lower fees for qualifying webcasters).

49. By contrast, radio and television broadcasters are only required to compensate the composer of broadcasted music. *See supra* notes 44-47. The WPPT also recognizes that producers of phonograms have a right to remuneration for the "direct or indirect use of phonograms published for commercial purposes for broadcasting or for any communication to the public." WPPT, *supra* note 24, art. 15(1). It further acknowledges that parties may establish as a matter of domestic policy that the producer and performer share the remuneration. *Id.* art. 15(2) ("Contracting parties may establish in their national legislation that the *single* equitable remuneration shall be claimed from the user by the performer or by the producers of a

The opportunities presented by the digital marketplace for music have been undeniably matched by its regulatory problems. At the heart of the technological and regulatory dance that is the present history of the music industry and the internet are the same critical issues facing the regulation of other forms of e-commerce. The answers may differ depending on the policies to be struck. Thus, for example, the regulation of intellectual property exploitation and use on the internet raise questions beyond those regarding the protections required to protect the commercial aspects of such transactions, including, critically, the balance to be struck between rights holders compensation and end user access to information.

B. The Lost Opportunity of the AHRA

The decisions made in determining the extent to which, if any, we need additional modes and norms of protection for internet based uses are simultaneously complex and critical. But we clearly cannot just hide our heads in the sand and hope the answers will present themselves. Instead, it is critical to consider the question from as many different points of view possible, in order to determine the most practicable regulations necessary. Evanescent solutions are not helpful. The embarrassing "solution" posed by the hard goods response to digital audio technology represented by the Audio Home Recording Act (AHRA)[50] is a case study in the wrong way to resolve the technological challenges of the Digital Age.

Briefly, faced with the advent of digital audio tape, Congress raced to craft legislation to protect copyrighted works in the face of such new reproductive technology. With inadequate consideration of the policy implications, it obligated digital audio recording equipment manufactured or distributed in the United States to conform to the copyright holders' Serial Copy Management System (SCMS) or face

---

phonogram *or both*.") (emphasis added). Interestingly, it does not provide for a single equitable remuneration to be divided between performers and composers. The absence of such treatment would appear to require that *both* performers and composers are compensated for all such broadcasts. Either composers will receive reduced compensation so that performers can share in established rates *or* royalty rates will necessarily rise. The only reason the rise has been felt most clearly for webcasters is because under U.S. law, they are the only ones who must currently compensate performers as well as composers.

50. Audio Home Recording Act of 1992, Pub. L. No. 102-563, 106 Stat. 4237 (codified at 17 U.S.C. §§1001-1010).

civil liability.[51] Unfortunately, the AHRA contained a cramped definition of the affected equipment. It defined "digital audio recording device" as a machine capable of making "a digital audio copied recording for private use."[52] A "digital audio copied recording" was defined as "a reproduction in a digital recording format of a digital musical recording, whether the reproduction is made directly from another digital musical recording or indirectly from a transmission."[53] The AHRA, however, specifically exempted from the definition of a covered "digital musical recording" any material object in which "one or more computer programs are fixed."[54] Even in 1992 when the statue was enacted, personal computers were already being used to record and store digital music from CDs, yet Congress failed to deal with the issue. The result was a statute which had a self-life of approximately seven years until the Ninth Circuit recognized the loophole and essentially nullified the practical application of the statute in the emerging digital marketplace.[55] This failing might be seen as simply another anecdote of a race to legislate too soon. But the failure to deal effectively with the issue meant that a potential fair use exception for media shifting contained in Section 1008 that might have added some clarity to the problem of personal use copying was also largely stillborn.

Section 1008 expressly exempted from the obligations of the AHRA claims "based on the non-commercial use by a consumer of [a covered] device or medium for making digital musical recordings or analog musical recordings."[56] The legislative history of Section 1008 indicates

---

51. 17 U.S.C. §§ 1002(a), 1009.

52. *Id.* § 1001(3).

53. *Id.* § 1001(1).

54. *Id.* § 1001(5)(B).

55. *See* Recording Indus. Assn. of Am., Inc. v. Diamond Multimedia Systems, 180 F.3d 1072 (9th Cir. 1999) (holding that computers are not obligated to comply with AHRA requirements even if they are used to record digital audio music).

56. 17 U.S.C. § 1008. Specifically, section 1008 provides that no action can be brought under copyright "based on the manufacture, importation or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device or an analog recording medium or *based on the non-commercial use by a consumer of such a device or medium* for making digital musical recordings or analog musical recordings." *Id.* (emphasis added). Admittedly the language is not a model of clarity since it fails to define what would qualify as an acceptable "non-commercial" consumer use. The legislative history of the Act indicates that such non-commercial use was intended to include media shifting by consumers. *See* S. REP. NO. 102-294 (1992) (suggesting that copying a CD to be played in the car for one's children is permissible activity). Yet there is little guidance as to the intended parameters of such "non-commercial" use. For example, must the "media shifted" music be owned by the

that it was intended to protect consumers' rights in making personal use copies. In explaining the scope of acceptable activities, the Senate Report explained:

> [F]or purposes of illustration, the making of an audiogram [audio digital recording] by a consumer for use in his or her home, car, or portable tape player, or for a family member, is protected by the prohibition against copyright infringement actions contained in this legislation. In determining whether the making of audiograms is for 'direct or indirect commercial advantage,' the relevant inquiry is whether a person makes audiograms for the purpose of commercial advantage, rather than whether the person making them acquires devices, media, or music from a commercial enterprise or in a commercial transaction.[57]

Given this history, section 1008 *might* have formed a viable focus for debates over media shifting with the rise of MP3 compression and digital downloads for so-called "personal uses." Yet any such resolution disappeared when music which had used computers in connection with their recording were exempted from the AHRA.

III. TEN "LESSONS" FROM THE IP WARS

As we struggle to define the scope and types of regulation which should be established to assist in the protection and development of electronic commerce on a global basis, I would urge that the lessons learned from other areas of contact with the global digital environment be considered. They may provide important insights or at a minimum highlight important issues that should be considered. For that reason, this Article outlines some of the critical lessons we have learned in the decades-long battle over intellectual property rights on the internet. I do not represent that these "lessons" are exhaustive, nor that they represent settled solutions, or even the most significant issues facing the complex question of intellectual property protection on the internet. What they do represent is my opinion of what are the most useful lessons we have learned to date which should inform any debate over the regulation of commercial activities on the internet.

---

consumer in question, or can a consumer record borrowed music? Does the implied Section 1008 fair use apply to consumer recording of pirated music for personal use? The statute is silent.

57. S. Rep. No. 102-294 (1992) (discussing the identical provision in a previous version of the bill that was finally enacted as the Audio Home Recording Act of 1992).

Lesson ONE: Don't Stop Asking The Question "What's The Difference Between Digital And Hard Copy Information Needs?"

On the IP side, it became readily apparent that the application of many of the traditional "rules" we had developed for the print media got a little fuzzy around the edges when it came to the digital marketplace. In fact, when it comes to such crucial issues as fair use and what actually qualifies as protectable speech, we are still struggling to figure out where the balance should be struck. There may be no more critical a question than the extent to which rules governing the acceptable, unauthorized use of copyright protected works need to be changed in light of the technological advances of the Digital Age. We are constantly asking ourselves where the needs of end users and the ability of technology should trump what was considered powerful authorial rights in the hard goods world.[58] For example, under copyright, the owner is entitled to the exclusive right to do or authorize six acts, including the reproduction, adaptation, transmission and distribution of their works.[59] These exclusive rights are, of course, subject to the well known "fair use" exception codified in Section 107 of the 1976 Copyright Act.[60] Because fair use in essence grants an unauthorized third party the right to use a work without compensation and without authorization, it has been, and continues to be a hotly contested battle ground.

In 1994, in a non-internet related case involving the right to create unauthorized parodies of previously recorded songs, the Supreme Court recognized that "transformative" uses were more likely to qualify as a fair use.[61] The precise nature of the "transformation" to qualify for such

---

58. For a brief discussion of the debate, see Long, *Dissonant Harmonization*, *supra* note 6. *See also* works cited in *supra* note 6.

59. 17 U.S.C. § 106.

60. *Id.* § 107 (providing that uses which qualify as fair ones are "not an infringement of copyright"). The parameters of fair use and the debates regarding the scope of such rights are far too broad to be covered adequately in this Article. For a brief overview of the history of its development, see WILLIAM A. PATRY, THE FAIR USE PRIVILEGE IN COPYRIGHT LAW (2d ed. 1995). For a selection of the articles which I believe are on the cutting edge of the debate, see Long, *Dissonant Harmonization*, *supra* note 6, at notes 84-87.

61. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994). The "transformation" rationale for fair use exceptions derived from a critical case dealing with an earlier generation of technology – the Sony Betamax case – where the Court faced the issue of whether the unauthorized taping of copyrighted broadcast programs qualified for a fair use. Despite the fact

protection, however, remains unsettled as courts struggle to understand the commercial demands of the digital marketplace. In the seminal case, *Kelly v. Arriba Soft Corp.*,[62] the owner of various posted photographs challenged the right of a search engine to copy thumbnails of those photographs without the permission of the copyright holder.[63] Given the increasing significance of search engines to the effective operation of the web, you could almost bet that the use in question would be found to be a fair one. Courts have frequently made adjustments in copyright law when faced with technological opportunities that would otherwise be stopped (or severely curtailed) without such adjustments.[64] Here the use of thumbnails was considered a sufficient "transformation" to support the fair use defense. The court stated:

> This case involves more than merely a retransmission of Kelly's images in a different medium. Arriba's use of the images serves a different function than Kelly's use-improving access to information on the internet versus artistic expression. Furthermore, it would be unlikely that anyone would use Arriba's thumbnails for illustrative or esthetic purposes because enlarging them sacrifices their clarity. Because Arriba's use is not superseding Kelly's use but, rather, has created a different purpose for the images, Arriba's use is transformative . . . . The thumbnails do not stifle artistic creativity because they are not used for illustrative or artistic purposes and therefore do not supplant the need for the originals. In addition, *they benefit the public by enhancing information gathering techniques on the internet.*[65]

Just when it appeared that the courts had established a new fair use line in the sand in light of the demands of the internet, the *Perfect Ten* case proved how movable lines in the sand may be in the digital world. Quite simply, *Google, Inc. v. Perfect Ten*[66] presented facts that were

---

that the entire work was recorded, the court found such home taping to be acceptable, in part because such non-commercial issues did not pose a significant likelihood of harm to either the potential market value of the recorded programs due largely to the absence of any market substitution. *See* Sony Corp. of Am. v. Universal Studios, Inc., 464 U.S. 417 (1984). This absence of market substitutability underscored the Court's acceptance of the "transformative" use of the Pretty Women song in *Campbell*.

62. 280 F.3d 934 (9th Cir. 2002).

63. *Id.*

64. Thus, for example, in *Sega Enterprise Ltd. v. Accolade Inc.*, 977 F.2d 1510 (9th Cir. 1992), the Ninth Circuit upheld as "fair" the unauthorized reproduction of a competitor's copyrighted computer source code where such reproduction was used solely to obtain access to unprotected functional code in order to support the creation of a final program that did not infringe the Sega's copyrights.

65. *Kelly*, 280 F.3d at 941-942 (footnotes omitted) (emphasis added).

66. 416 F. Supp. 2d 828 (C.D. Cal. 2006).

strongly similar to *Kelly*. Google's search engine provided unauthorized thumbnail versions of photographs posted by the plaintiff on its adult content websites. The district court found Google's use in *Perfect Ten* highly commercial, more so than in *Kelly,* due mainly to Google's AdSense program, which allowed Google's server to place advertisements on designated websites and then share the proceeds with the website owner. This program made Google's thumbnails both transformative *and* consumptive.[67] Additionally, in contradistinction to *Kelly*, the court noted that in 2005 Perfect Ten leased the right to distribute reduced-size versions of its images for use on cell phones to Fonestarz Media Limited.

Despite acknowledging the harm to internet development, a decision in Perfect Ten's favor might entail a recalibration of previous fair use factors. Ultimately, the district court concluded that no fair use applied:

> Although the Court is reluctant to issue a ruling that might impede the advance of internet technology, and although it is appropriate for courts to consider the immense value to the public of such technologies, existing judicial precedents do not allow such considerations to trump a reasoned analysis of the four fair use factors.[68]

While the difference in the courts' decisions regarding thumbnails might be seen as contradictory, in reality, the two arguably demonstrated that despite the relative proximity in time, we have gained more experience with searches. More significantly, the courts are beginning to understand the economic impact of internet search engines, both on the ones who sponsor such searches (and charge for keyword buys), and on website owners themselves who pay for such buys to enhance their positioning in search results.

Recently, the Ninth Circuit in *Google v. Perfect Ten*[69] reversed the district court's determination that Google's use of the thumbnails was too commercial to qualify as a transformative use. In reversing the ultimate conclusion, however, the court did not disagree with the lower court's recognition that the consumptive use was problematic. Instead, it determined that the district court had failed to adduce sufficient evidence of the nature of the allegedly consumptive use to warrant rejection of Google's fair use defense. The court stressed that "the

---

67. *Id.* at 848-49.
68. *Id.* at 851.
69. 487 F.3d 701 (9th Cir. 2007).

significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case,"[70] which the court described as "incidental"[71] and "minor."[72] While skeptics might claim that the court's reliance on the public benefit of Google's search engine indicates a technology-trumping vision of fair use transformation that no amount of consumptive use could overcome, such skepticism ignores the court's plain recognition that in the face of significant evidence of such use the result would have differed.

As commerce intrudes ever more completely into what used to be mere communicative activity, the lines between communication and commerce in cyberspace become more difficult. Even such straight forward commerce-related issues as what qualifies as challengeable trademark use in the context of internet searches and advertising has proven difficult. Under federal trademark law, to qualify as actionable infringement a third party must use a confusingly similar word or symbol *as a trademark.* Non-trademark uses are expressly excluded from liability.[73] In the hard goods world the issue of non-trademark use has been used largely to strike the balance between regulatable commercial speech (represented by trademark use) and other forms of speech, including political speech, criticism and parody.[74] In the electronic marketplace, the balances become more nuanced. Just as search technology has raised issues under copyright fair use doctrines, such search technology (or, more precisely, the economic gamesmanship search technology encourages in search listings) has raised issues under the trademark equivalent of fair use.[75] Early in the

---

70. *Id.* at 723.

71. *Id.*

72. *Id.*

73. Subject matter jurisdiction under the Lanham (Federal Trademark) Act requires use of a trademark in interstate commerce. *See* 15 U.S.C. §§ 1114, 1125(a), 1127.

74. The clearest example of this distinction is the statutory exception to federal trademark dilution protection contained in Section 43(c). 15 U.S.C. § 1125(c). Despite the broad scope of protection purportedly granted under dilution doctrines, including protection despite the absence of either competition or likely confusion, see *id.* § 1125(c)(1) (providing for civil relief against dilution "regardless of the presence or absence of actual or likely confusion, or competition, or of actual economic injury"), such relief does *not* extend to "any noncommercial use of a mark." *Id.* § 1125(c)(3)(C).

75. I am using the term "fair use" in the broader sense than traditional trademark doctrines. To qualify as a fair use traditionally the mark must be a descriptive term and must be used "in good faith only to describe the goods or services of such party, or their geographic

debates, in *Playboy Enterprises Inc. v. Netscape Communications Corp.*,[76] the court held that use of terms "playmate" and "playboy" as key words in a search engine, which could be purchased to run certain banner ads when the terms were used, qualified as a non-trademark use.

Similarly, in *1-800 Contacts, Inc. v. WhenU.com*,[77] the Second Circuit held that use of plaintiff's mark to trigger a pop-up ad did not trigger trademark liability because the defendant had made no commercial use of the mark. The court explained: "A company's internal utilization of a trademark in a way that does not communicate it to the public is analogous to an individual's private thoughts about a trademark. Such conduct simply does not violate the Lanham Act . . . ."[78] Yet in *Government Employees Ins. Co. (GEICO) v. Google, Inc.*,[79] the court declined to dismiss GEICO's suit for trademark infringement based on Google's use of GEICO's trademark to create sponsored links on its web searches. The district court concluded that Google's use of the GEICO trademarks could falsely identify a business relationship or licensing agreement between Google and GEICO. It also found that using GEICO trademarks to sell advertising links qualified as a use in commerce that implied that Google had permission to do so. The court recognized a potential use in commerce since the marks were used as source identifiers in the advertising links posted on Google's search results page.

At the heart of all of these disputes is the critical issue of the extent to which competition on the internet requires different regulation than in the hard goods world. In short, what are the limits of fair competition and compensable trademark use in cyberspace where domain names are arguably limited to one mark and one domain name, and where money can be earned simply by offering search services that rely on metatags and keyword buys that may contain another's trademark? Given the constantly changing nature of commercial activities on the internet, and

---

origin." *Id.* § 1115 (b)(4). It cannot be used as a trademark or source designator. *See, e.g.*, Zataran's Inc. v. Oak Grove Smokehouse, Inc., 698 F.2d 786, 791 (5th Cir. 1983) (finding "fish-fri" could be used by defendants even though it had attained secondary meaning because they were using the term in a descriptive sense). The fair use doctrine has been expanded in recent years to acknowledge a nominative use of trademarks where source designating terms are used to describe accurately the goods or services related to or referring to such goods or services. *See, e.g.*, New Kids on the Block v. News Am. Publ'g, Inc., 971 F.2d 302 (9th Cir. 1992).

76. 55 F. Supp. 2d 1070, 1086-88 (C.D. Cal., 1999), *aff'd*, 202 F.3d 278 (9th Cir. 1999).

77. 414 F.3d 400, 409-11 (2d Cir. 2005).

78. *Id.* at 409.

79. 330 F. Supp. 2d 700 (E.D. Va. 2004).

our growing understanding of the economics involved in such commerce, no matter what methods or norms are established, the balance between hard goods and cyberspace must be constantly revisited.

Lesson TWO: You Need Both Law And Technology To Protect Internet Content

Some people would argue that cyberspace isn't really a separate economic "space" at all, but merely the hard goods world transformed into a digital version of itself. Certainly the multiplayer game Second Life[80] is the epitome of this argument, as well its proven exception. On the one hand, life in a digital environment, and its legal problems, seem to reflect the hard goods world. Shopping, rock concerts, housing acquisitions, and even trademark infringement all occur in the digital world of Second Life.[81] But apart from the digital reflection Second Life provides are the cyber-problems that we do not have in the hard goods world, such as the lack of a permanent identity, the ability to supposedly craft your own appearance, make up your own avatar, and to a large extent live by your own rules. A lot of the social norms that exist in the hard goods world do not yet appear part of the cyberworld, including for example, sexual equality.[82] In cyberspace you can participate in rape fantasy games.[83] In the real world, acting out such fantasies should get you put in jail.[84]

---

80. Second Life, http://www.secondlife.com (last visited Oct. 27, 2007).

81. *See, e.g.*, Matt Belloni, *Case Filings: Copyright on sex in Second Life?*, HOLLYWOOD REPORTER, Aug. 23, 2007, http://www.hollywoodreporter.com/hr/content_display/business/law/e3ic3c981a927197a172b0b0830c5ea7f62; Phil Davis, *Virtual Sex Software Spawns Lawsuit*, ASSOCIATED PRESS, Aug. 10, 2007, *available at* http://www.msnbc.msn.com/id/ 20214184/wid/11915829?GT1=10252.

82. *See, e.g.*, Ann Bartow, *Some Peer-to-Peer, Democratically, and Voluntarily-Produced Thoughts*, 5 J. TELECOMM. & HIGH TECH. L. 449 (2006) (faulting Benkler for ignoring race and sexual equality issues on the internet); LISA NAKAMURA, CYBERTYPES: RACE, ETHNICITY AND IDENTITY ON THE INTERNET (2002) (describing racial and ethnic stereotyping that occurs in cyberspace, even in the creation of avatars); BETH E. KOLKO ET AL., RACE IN CYBERSPACE (2000) (same).

83. *See, e.g.*, Ann Bartow, Presentation at Virtual Women Conference at Thomas Jefferson Law School (Feb. 9, 2007). So long as these rape fantasy games contain digital avatars, even if the activity would generally qualify as obscene or pornographic under hard goods regulations, they have avoided such legal strictures. The presence of such virtual pornography, however, raises serious concerns about the alleged role of cyberspace as a democratizing space. *Cf.* Doris Estelle Long, *Electronic Voting Rights and the DMCA: Another*

If the old legal rules appear to have little applicability to cyberspace, one potential solution to the problem is to rely on technological fixes. To turn Larry Lessig's well known conclusion that in cyberspace *code is law* on its head,[85] what do we need law for when we have code? Instead of creating new laws whose efficacy is questionable at best, perhaps we should instead simply rely on what got us into this fix in the first place – technology. On the electronic commerce side, such a solution would suggest that the protection of authenticity in transactional documents, websites and other commercial activities should largely be resolved through the development of acceptable encryption technologies. Unfortunately, in the IP wars, while we've learned that law alone won't prevent infringement or unfair competition,[86] technology alone as a solution has similarly proven relatively ineffective.

For every unbreakable code that someone creates, we seem to have a hacker willing and able to break it. More problematic for those in the digital content industry, such as music, films and software, hackers are not only capable of hacking any code created to date; they are also more than willing to share their knowledge with everyone on the planet. Thus, for example, recently touted technology regarding copy code used to

---

Blast from the Digital Pirates or a Final Wake Up Call for Reform?, 23 J. MARSHALL J. COMPUTER & INFO. L. 533 (2005); Bartow, *supra* note 82.

84. I do not want to stretch the analogy of the "wild frontier" of cyberspace too far. While individuals have the ability to create their own images, including cross-gender and cross-racial ones, the sad reality appears to be that the people in cyberspace bring their prejudices and biases with them. Thus, while people craft their own nationalities, these nationalities seem to reflect the same racial stereotyping that has bedeviled the hard goods world. *See, e.g.*, NAKAMURA, *supra* note 82; Bartow, *supra* note 82.

85. LESSIG, CODE, *supra* note 8.

86. The widespread use of peer to peer software to download and distribute illegal copies of films, music and software despite the fact that such unauthorized reproduction and distribution violates domestic copyright laws has, to date, failed to stop end users from engaging in such activity. Even when the RIAA began its largely successful campaign in 2003 to hold end-users accountable for such activities, internet piracy figures remained high. It was only when a business alternative to such illegal activities, in the form of iTunes and other legal digital download sites for music, developed that piracy figures began to decline. While some of this downloading activity might be attributable to ignorance of the law, after the well-publicized Napster and Grokster cases, *A&M Records, Inc.*, 239 F.3d 1004; *Metro-Goldwyn Mayer Studios, Inc.*, 545 U.S. 913, and subsequent campaigns by the music industry to advertise the issue, a claim of ignorance is far less tenable. To the contrary, the widespread continued P2P file trading in music and films must be due to a disregard of legal obligations. In the face of such widespread disregard of legal norms, if the norms are to be maintained, something more is required. This "something more" in the digital era necessarily includes better copy protection technology.

protect lawfully authorized digitally downloaded films from unauthorized duplication has already been hacked, and the solution was posted on the internet for anyone who would care to seek it out.[87] Despite my admitted techno-scepticism,[88] I do not mean to suggest that technology can serve *no* significant role in protecting authentication methodologies, such as digital signatures and the like. However, the lesson we have learned from the IP Wars is that technology *alone* will not resolve all the challenges posed by electronic commerce. Without an appropriate legal regime to protect such technologies, any technological solution will prove evanescent at best.[89]

The other major problem with a technological solution to content protection is the apparent lack of agreement over the existence of any such technology. One of the critical legal issues which has arisen in the realm of intellectual property is the border-related question of how to enforce local content regulation in the face of the "borderless" internet. Numerous countries regulate content on the internet. Such content regulation is not limited to copyright, but includes laws that require content to be in the national language,[90] or that regulate hate speech or the nature of goods which may be sold over the internet.[91]

---

87. *See, e.g.*, Ina Fried, *Hackers Crack Apple, Microsoft Music Codes*, CNET NEWS, Sept. 1, 2006, http://www.news.com/2100-1027_3-6111530.html (hackers have circumvented both Microsoft Windows Media DRM and Apple's Fair Play and posted hacks on the internet).

88. *See* note 10 and accompanying text.

89. The other major problem with a technological solution to content protection is the apparent lack of agreement over the existence of any such solution. One of the critical legal issues which has arisen in the real world is the extent to which filtering or other such technological measures are actually *effective*. Thus, for example, in the debate over potential liability for facilitating the sale of prohibited Nazi paraphernalia in France, experts as well known as Vint Cerf disputed whether any effective technological methods existed to allow the French subsidiary of Yahoo to prevent the sales to customers in France of prohibited items, including *Mein Kampf*. Ultimately the court found that such technology existed. *See* La Ligue Contre Le Racisme et L'Antisemitisme (LICRA) v. Yahoo! Inc., No. RG 00/05308 (November 20, 2000) (Tribunal de Grande Instance de Paris) (available at http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi-paris_201100.htm). In what I believe was an exercise of sound judgment, the court did not require that such technology be fool-proof to be acceptable but recognized the some leakage was inevitable, setting that leakage at approximately 90% based on filtering and geographic location technologies. *Id. See also* note 93 *infra* and accompanying text.

90. One such law is the *Loi de Toubon* which requires, inter alia, that websites which are directed toward French citizens be in the French language. The website for a campus which Georgia Tech operated in France ran afoul of this law, resulting in charges being filed. The case was ultimately dropped. *See generally* Anne Swardson, *French groups sue to bar English-only Internet sites*, WASH. POST, Dec. 24, 1996; *French Ban on Use of English in French Web Sites*,

In a well-known case involving French law, which prohibits the sale of Nazi paraphernalia, Yahoo.com and its French subsidiary were sued for violating this law by facilitating, inter alia, the purchase of copies of *Mein Kampf* by French customers.[92] One of the critical issues before the French court was the question of the extent to which technology existed that would permit internet service providers to comply with French legal requirements. The testimony before the court is notable for the vehemence of the disagreement between so-called technology experts on the extent to which technology would allow Yahoo France to prevent its French customers from using its services to access Yahoo.com and purchase prohibited works.[93] In the face of dueling experts, the court accepted that present technology may not support perfect compliance and accepted a technological fix consisting of, inter alia, "the use of geographical identification and declaration of nationality" which the court accepted made it possible to achieve at best a rate of filtering "close to 90%."[94]

The same debate over technological efficacy is being repeated in global challenges to the illicit use of peer-to-peer (P2P) file trading software. Thus, for example, in *Universal Music Australia Pty Ltd. v Sharman License Holdings Ltd.*,[95] the Australia court expressly found that the defendant's failure to utilize filtering software in order to filter out illegal copies of posted music on his website was a key factor in its liability determination.[96] The failure to use such filtering techniques was relied upon even though the effectiveness of such filtering techniques has been severely criticized.[97] If we cannot agree on the

---

TED CASE STUDIES, *available at* http://www.american.edu/TED/english.html.

91. See *LICRA v. Yahoo! Inc.* and note 89 for further details. *See also* notes 92-94 *infra* and accompanying text.

92. *See id.*

93. Vint Cerf, for example, in an opposing letter filed with the court did not question the existence of filtering and geographic location methodologies but questioned whether such methodologies would be "feasible" in light of both privacy and ease of application concerns. *See id.*

94. *Id.*

95. [2005] FCA 1242

96. *Id.*

97. The court itself in *Sharman* acknowledged that filtering would not be completely effective:

> It is also apparent – indeed common ground between the experts – that a keyword filter system that was tied to the title of the sound recording or the name of the artist would not be 100% effective. However, counsel for the applicants argued this was no reason to reject the view that the respondents could have used this technique substantially to inhibit copyright infringement . . . . I accept that some canny users

efficacy of technological protective measures, we assuredly cannot rely upon such measures *alone* to resolve critical protection issues in cyberspace.

Lesson THREE: No Code Is Unbreakable, No Matter How Much Money You Spend

Lesson Three is really a corollary of Lesson Two. If technology alone will not resolve the problem of protecting digital content and assuring authenticity of commerce in cyberspace, it is because technology is infinitely fallible. Despite creating what the motion picture industry hoped would be an unbeatable encryption code to protect digital content on the DVD, referred to as "CSS,"[98] Eric Corley managed to circumvent that code which he then shared in various forms, including on t-shirts, with the rest of the world.[99] The use of the internet as a communications media for "sharing" hacking techniques has proven so effective that, despite injunctions in the United States prohibiting Corley from sharing his solution with others,[100] a Finish court has recently declined to protect CSS on the grounds that DeCSS (Corley's code for breaking CSS) is so prevalent that CSS no longer qualifies as a protectable technological protection measure because it is "ineffective."[101] On the IP side of the house we have yet to face the question of unbeatable keys or the extent to which any code should be placed in escrow with a governmental organization because, as yet, we do not have encryption that seems to defeat even a yellow marker.[102]

> would devise methods of evading a keyword filter; for example, by the adoption of a nickname for the artist or a codeword for a particular song. However, this technique would allow file-sharing of the relevant works only as between people who were privy to the adopted nicknames or codewords . . . . I accept any keyword filter will not be totally effective. I also accept it may sometimes produce false positives. However, the fact that a protection is imperfect is not a sufficient objection to its adoption. Even an imperfect filter would go far to protect copyright owners, provided they were prepared to go to the trouble of providing and updating a list of keywords (titles, performers etc).

Id. at 284-94.

98. Content Scramble System.

99. *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 439 (2d Cir. 2001).

100. *Id.*

101. Helsingin Käräjäoikeus, case R 07/1004, 25.5.2007, *available at* http://www.turre.com/css_helsinki_district_court.pdf.

102. *See, e.g.*, *Post It Notes Versus Copy Protected CDs* (May 13, 2002) (discussing potential circumvention of copy protection on certain CDs using a marker); Long, *Global Solution*, *supra* note 10 (discussing diverse problems with encryption and other technological

In the face of the obvious failure of technology to resolve the regulatory problems of IP content on the internet, technology has been married to law to provide legal protection for the technological protection measures copyright holders may employ to protect their rights in the digital world. Instead of relying on legal prohibitions against unauthorized uses (including reproduction and transmission), the Digital Millennium Copyright Act (DMCA),[103] similar to its international analogues, the WCT[104] and WPPT,[105] provides strong legal prohibitions against the unauthorized circumvention of certain technological protection measures employed to protect authors' rights in the era of digital technology.[106] While this technique is not new – the Audio Home Recording Act required protection for content scramble systems used to protect digital audio tape[107] – the scope of protection afforded under the DMCA far exceeds the limited "first toe in the water" represented by the AHRA.

Under the DMCA, the making or selling of devices or services used to circumvent technological measures to prevent either unauthorized access or unauthorized copying of a copyrighted work is prohibited where such devices or services are *primarily* designed or produced to circumvent "technological protection measures."[108] Section 1201 prohibits the circumvention of technological protection measures designed to control access to a copyrighted work.[109] To qualify for protection the technological measure in question must be "effective."[110] Effectiveness, however, does not mean that the measure must be perfect or nearly impossible to break. Instead, it is sufficient if the measure "actually works" when decryption programs or other circumvention measures are absent.[111]

---

solutions).

103. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. §§ 512, 1201-1205).

104. WIPO Copyright Treaty, April 12, 1997, 36 I.L.M. 65 (1997) [hereinafter WCT].

105. WPPT, *supra* note 24.

106. *See generally* 17 U.S.C. §§ 1201-1205 (1999); WPPT, *supra* note 24, art. 18; WCT, *supra* note 104, art. 11.

107. *See* 17 U.S.C. §§ 1001-1009.

108. *Id.* § 1201 (1999). The DMCA also provides safe harbors for certain internet service providers from charges of contributory copyright infringement. *See generally id.* §§ 1201-1204.

109. *Id.* § 1201(a).

110. *Id.*

111. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000), *aff'd on other grounds sub nom.*, *Corley*, 273 F.3d 429 (2d. Cir. 2001).

In addition to prohibiting the actual circumvention of technological protection measures, the DMCA also prohibits the manufacture, importation, offering to the public, provision or other "trafficking" "in any technology, product, service, device, component or part that is *primarily designed* or produced for the purpose of circumventing a [protected] technological protection measure that either effectively controls access or protects a right of the copyright owner."[112] "Trafficking" has been broadly defined under the statute, and even includes the knowing linking to a page containing unauthorized anti-circumvention techniques.[113] Violations of these anti-circumvention provisions may be challenged by both civil and criminal actions. Successful civil litigants are entitled to a full panoply of remedies, including statutory damages of not less than $200 nor more than $2,500 "per act of circumvention, device, product, component, offer or performance of service."[114] Criminal violations require proof of willfulness and motivation for commercial advantage or private financial gain.[115]

In addition to prohibiting the circumvention of technology used to protect copyrighted content, the DMCA also prohibits the unauthorized, intentional removal or alteration of any "copyright management information."[116] It also prohibits the unauthorized distribution, importation for distribution or public performance of works from which such copyright management information has been illegally removed.[117] By definition, protected copyright management information includes the following categories:

> The title or other identifying information, including the information contained on a copyright notice;
> The name or other identifying information about the author;
> The name or other identifying information about the copyright owner of the work;

---

112. 17 U.S.C. § 1201(a)(2), (b)(1) (emphasis added).

113. *See Corley*, 273 F.3d at 442.

114. 17 U.S.C. § 1203(c)(3)(A) (1999). Additional remedies include injunctive relief, impoundment, reasonable attorneys fees and costs. *Id.* § 1203(b).

115. *Id.* § 1204. First time offenders may be subjected to penalties of up to $500,000 in fines and/or imprisonment for not more than 5 years. Recidivist penalties are significantly elevated. *Id.*

116. *Id.* § 1202(a).

117. *Id.* The DMCA also prohibits knowingly providing false copyright management information or distributing or importing for distribution false copyright information "with the intent to induce, enable, facilitate or conceal infringement." *Id.*

> With the exception of public performances of works by radio and television broadcast stations, the name or other identifying information about the performer whose performance in fixed in the work;
> In the case of audio-visual works, with the exception of public performance of works by radio and television broadcast stations, the name and other identifying information about a writer, performer, or director credited in the work;
> The terms and conditions for use of the work (such as licensing contact information); and
> Any other information which the Register of Copyright may require.[118]

Similar to the anti-circumvention provisions, violations of rights management information integrity may be challenged in both civil and criminal actions.[119] The DMCA imposes higher penalties for information integrity violations[120] than for unauthorized circumventions of technological protection measures,[121] largely due to the usefulness of copyright management information as a tool for tracking pirated works and the subsequent harm caused by its unauthorized removal or alteration.

Despite the critical role that fair use plays in copyright policy, the access and trafficking provisions of the DMCA do *not* provide a categorical exception for "fair use" activities.[122] Thus, for example, a

---

118. *Id.* § 1202(c).

119. *Id.* §§ 1202, 1204.

120. Successful civil litigants are entitled to statutory damages of not less than $2,500 nor more than $25,000 per violation, in addition to injunctive relief and attorney's fees. *Id.* § 1203.

121. *See id.* § 1204.

122. The categorical exceptions set forth in the statute are limited to:

- Non-profit libraries, archives and educational institutions;
- Law enforcement, intelligence and other government activities;
- Reverse engineering;
- Encryption research;
- Security testing; and
- Protecting personal identification information.

See generally id. § 1201(g). It should be noted that these exceptions are not so broad as this categorical listing implies. For example, while Section 1201(g) provides an exception for encryption research, not all encryption research qualifies. To the contrary the exception has been narrowly crafted to apply only to research "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works" and further requires that such activities must be "conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." *Id.* § 1201(g)(1)(A). Moreover, the research in question must generally be "disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement." *Id.* §

teacher who seeks to circumvent technological protection measures for the purpose of obtaining *access* to materials to use in teaching activities is *not* excused from compliance, even if the use of such materials might otherwise qualify as a fair use under traditional copyright principles.[123]

Despite the numerous problems which the DMCA presents, however, the approach of seeking to provide legal protection for technology used to help prevent unauthorized or inauthentic uses of content on the internet is a valuable one. The DMCA's checkered history serves to remind us that whenever we are dealing with technological protection measures we must either paint less broadly or go back and repaint the canvass more frequently to take advantage of experiential knowledge. It is not that the DMCA was necessarily a poor idea. The balances struck, however, may need to be reconfigured in light of experience.[124]

Lesson FOUR: Craft The Language Clearly Or Your Technological Protection Laws Will Be Used To Defend Potentially Anti-Competitive Conduct

Even if technological protection laws are desirable, be careful what you wish for. What begins as a pro-competitive measure can be easily perverted in the digital world if the language is not carefully crafted. While anti-circumvention prevention seems an admirable goal at first instance – strongly reminiscent of the need in the information world for encryption keys and the like – we have discovered that any law created for one purpose may be applied to prohibit activity that was never

---

1201(g)(3). Such narrow exceptions have been criticized for excluding much present day encryption research, particularly that which is undertaken by amateur researchers.

123. While fair use exceptions are specifically excluded under the access prohibitions of section 1201(a) and the trafficking prohibitions of Section 1201(b), fair use limitations *do* apply to the circumvention provisions of Section 1201(b) which relate to the circumvention of copy control mechanisms. *See, e.g., id.* § 1201(c)(1) ("Nothing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title."); H.R. Rep. 105-551, pt 1, at 18 ("[A]n individual [should] not be able to circumvent in order to gain unauthorized access to a work, but [should] be able to do so in order to make fair use of a work which he or she has acquired lawfully"). Thus, if the technological protection measure in question is used to prevent copying as opposed to access, the previously described teacher would have the fair use right to circumvent such measure to create teaching materials. However, since trafficking is not subject to a fair use exception, the teacher would have to develop her own circumvention technique since no one else could provide it without theoretically violating the anti-trafficking provisions of the DMCA.

124. This reconfiguration should include re-consideration of the need for absolute prohibitions against unauthorized *access* to copyrighted works, as opposed to their unauthorized distribution and/or performance.

intended to be covered. Thus, in a well known case involving Lexmark printer toner cartridges, *Lexmark International, Inc. v. Static Control Components, Inc.*,[125] the DMCA was used to defend the use of an authentication sequence in smart chips on the toner cartridges that prevented the use of unbranded toner cartridges in branded printers.[126] The court rejected defendant's claim that only technological protection measures that were designed to control access to prevent digital piracy were covered by the statute despite arguable evidence in the legislative history that suggested such a limit. It affirmed: "The plain meaning of the DMCA is clear and it would be inappropriate for the Court to consider the legislative history in an effort to determine the 'true' congressional intent."[127] Fortunately, the application of the DMCA to Lexmark's toner cartridges was overturned on appeal and the makers of third party toners could continue to create cartridges that contained codes to circumvent Lexmark's recognition codes on its printers,[128] but that result hasn't prevented other manufacturers from trying to use the DMCA to protect garage door openers from interchangeability.[129]

Lesson FIVE: You Cannot Protect Digital Content Without International Standards BUT International Standards Necessarily Bring Their Own Set Of Problems

It seems obvious that the internet necessarily involves international legal protection issues. Part of the appeal of the internet for small businesses is the ready access it provides to a global marketplace. Yet

---

125. 253 F. Supp. 2d 943 (E.D. Ky. 2003), *vacated*, 387 F.3d 522 (6th Cir. 2004) (*see also* note 126 *infra*).

126. Briefly, Lexmark alleged that its toner cartridges contained software code in its smart chips which was protected by an authentication sequence that occurred between the smart chips and the printer. Defendants had allegedly circumvented this "handshake" access authentication sequence in order to assure that the printer would accept their unbranded toner cartridges. Since the authentication sequence was designed to prohibit unauthorized access to the software code, Lexmark contended its sequence qualified as a technological protection measure under the DMCA which had been illegally circumvented by defendants. *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 530 (6th Cir. 2004).

127. *Lexmark Int'l*, 253 F. Supp. 2d at 967.

128. *Lexmark Int'l*, 387 F.3d at 531-32, 546-49. Unfortunately, the reversal was based on the appellate court's determination that the software code at issue did not qualify for copyright protection because of the limited expression it contained. In the absence of such copyright status, the anticircumvention strictures of the DMCA did not apply.

129. Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004).

in order to enhance this global marketplace, regulations should be transparent and, where possible, legal standards should be harmonized to assure predictable *ordered* international commercial transactions. In the intellectual property world, the TRIPS Agreement[130] serves this purpose, establishing minimum substantive and procedural standards and requiring transparency of laws to assure an even playing field for commercial exploiters of intellectual property rights.[131]

It seems axiomatic that if you want to have legal standards applied equally on both sides of an international transaction, you need an international agreement on what those standards should be. The problem: Most of the international accords that exist in this area were created for the hard goods world. Thus, for example, on the intellectual property side of the fence, when countries tried to create workable international standards for copyrighted works on the internet, they ended up in fights over terminology. Similar to the treatment of privacy for databases,[132] the copyright community found itself struggling with cultural and legal differences over what actually qualifies as a "copy" on the internet.[133] This is a critical issue under copyright because before you can determine what rights an author should control, you need to know whether an unauthorized copy has been created, or whether the work qualifies as merely a performance or display.[134] The compromise: New terminology was developed to describe authorial rights on the

---

130. Agreement on Trade Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, Legal Instruments -- Results of the Uruguay Round, 33 I.L.M. 1125, 1197 (1994) [hereinafter "TRIPS"].

131. For a brief overview of the major provisions of the TRIPS Agreement, see Doris Estelle Long, *The Impact of Foreign Investment on Indigenous Culture: An Intellectual Property Perspective,* 23 N.C. J. INT'L L. & COM. REG. 229 (1998) [hereinafter Long, *The Impact of Foreign Investment*].

132. *See, e.g.*, Long, *Global Solution*, *supra* note 10 (discussing the cultural problems in creating an international database standard involving personal consumer information).

133. For an excellent background on the scope of the debates surrounding the difficulty of establishing this standard as part of the WCT, and the reason for the compromise "making available" language in Section 8, see MIHALY FICSOR, THE LAW OF COPYRIGHT AND THE INTERNET: THE 1996 WIPO TREATIES, THEIR INTERPRETATION AND IMPLEMENTATION (2002).

134. For example, in order to violate the right of reproduction, a copy must be created. *See* 17 U.S.C. § 106. If no copy is created, then subsequent distribution of the work is allowed even if the copyright owner opposes such subsequent distribution, under the first sale right. *See id.* § 109. By contrast, if the work is "performed" or "displayed," no right of further distribution exists. *Id.*

internet – "making available."[135] You know if a generally unused term appears in an international agreement to resolve a critical issue such as authors' and performers' rights on the internet – you're in trouble. Now we have a new international right, with people attaching new meanings, making protection even more problematic.

One of the fundamental assumptions of this Article is that talking across legal regimes may actually help resolve some of the conflicts we all face in dealing with cyberspace. Thus, for example, we have begun to examine the interplay between intellectual property and human rights regimes in an effort to determine where the boundaries of traditional knowledge and access to information should lie.[136] Yet in working across regimes, we have also learned the painful lesson that secret protocols or failures to include all affected parties may result in a standard that causes more problems than it solves.

If you're going to create a new international treaty that deals with prosecuting crimes using the internet, and you're going to create criminal standards that deal with already existing issues, such as the protection of copyright or privacy, it might be a good idea to get people who deal with those issues to participate in the discussion. Originally conceived as an international agreement involving the issue of international legal assistance in investigating and prosecuting international crimes on the net (LEGATS), the Cybercrime Convention by the Council of Europe[137] was largely negotiated by ministries of justice with little if any input from the IP community or the privacy community. It was also negotiated with very little public input.[138] The result – a treaty that has been harshly criticized.[139] The lessen: Don't box yourself in. You may think you're only dealing with information security, but take a second look. Better yet, be certain to include other

---

135. WCT, *supra* note 104, art. 8.

136. *See, e.g.*, Doris Estelle Long, *Traditional Knowledge and the Fight for the Public Domain*, 5 J. MARSHALL REV. INTELL. PROP. L. 317 (2006); Peter Yu, *Reconceptualizing Intellectual Property Interests in a Human Rights Framework*, 40 U.C. DAVIS L. REV. 1039 (2007).

137. Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

138. Letter from Electronic Privacy Information Center (EPIC) to Senate Comm. on Foreign Relations Regarding Cybercrime Convention (July 26, 2005) (detailing lack of transparency in process resulting in Cybercrime Convention final draft) [hereinafter EPIC Letter], *available at* www.epic.org/privacy/intl/senateletter-072605.pdf.

139. *COE Cyber Crime Treaty Debated*, TECH LAW JOURNAL, Dec. 11, 2000, http://www.techlawjournal.com/crime/20001208.asp; EPIC Letter, *supra* note 138.

regimes and communities in taking your second look. You might have missed something.[140]

Lesson SIX: Jurisdiction Is Never Easy

No matter how detailed your international agreements concerning the protection of information in cyberspace may be, lack of international jurisdictional standards can severely limit the advances these agreements may have theoretically secured. In the IP wars, we have a detailed international treaty, originally ratified by 144 countries – the TRIPS Agreement.[141] With that many countries, you would think we would have a fairly thorough international standard for protection. We do,[142] subject of course to the vagaries of language treaties always present.[143] But despite requiring "effective enforcement" of intellectual property rights[144] and providing relatively detailed procedural minimum standards for such enforcement,[145] TRIPS did not address jurisdictional issues. Given the diverse domestic standards governing jurisdiction, including choice of law problems, efforts were undertaken to create an international agreement – The Draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters.[146] As you can imagine, it crashed. First of all, people disagreed about whether

---

140. This problem of failure to include other affected regimes in initial drafting was also evident in the Draft A2K (Access to Knowledge) Treaty, where the rights of indigenous peoples were ignored in the race to free up information on the internet. *See* Long, *Global Solution*, *supra* note 10; *see also* Doris Estelle Long, Professor of Law John Marshall Law Sch., *Traditional Rights and Data Access Demands: Untying the Gordian Knot*, Address at Yale Law School Access to Knowledge Conference (April 21-23, 2006) (copy on file with author).

141. *See supra* notes 130-31.

142. The TRIPS Agreement not only establishes minimum standards of protection for covered intellectual property rights, including copyright, trademark, patents and trade secrets, but also establishes minimum standards of civil, criminal and border enforcement of those rights. *See generally* Long, *The Impact of Foreign Investment*, *supra* note 131; DANIEL GERVAIS, THE TRIPS AGREEMENT: DRAFTING HISTORY AND ANALYSIS (2d ed. 2003).

143. *See generally* Doris Estelle Long, *"Globalization": A Future Trend or a Satisfying Mirage?*, 49 J. COPYRIGHT SOC'Y U.S.A. 313 (2001) (contending that harmonized IPR standards may be less "harmonious" than anticipated).

144. TRIPS, *supra* note 130, art. 41.

145. *Id.* arts. 41-61.

146. Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters [hereinafter "Hague Convention"], *reprinted in* DORIS ESTELLE LONG & ANTHONY D'AMATO, 2002 DOCUMENTS SUPPLEMENT TO A COURSEBOOK IN INTERNATIONAL INTELLECTUAL PROPERTY 912-20 (West Group 2002).

copyright was included. The Treaty expressly covered only "patents, trademarks, designs or other similar rights."[147] Some claimed that such coverage meant that copyrights were, therefore, excluded,[148] thus removing many of the problematic issues regarding the protection of copyright in cyberspace that are raised by any treaty which attempts to establish a single point of jurisdiction for such matters. But despite this claim, the Convention covered torts,[149] and many countries treat copyright infringement as a tort.[150] Second, there is nothing so personal as jurisdiction, particularly when the internet is involved. Nor is there anything so complicated as determining when a country should be able to extend its laws to websites and activities that are geographically situated on a server or operated by an end user in another country.[151] Any effective enforcement method will eventually have to face this problem.[152]

---

147. Hague Convention, *supra* note 146, art. 12(4).

148. *See generally* Federal Register Notice on Draft Hague Convention, U.S. Patent and Trademark Office, 66 Fed. Reg. 43575-02 (Aug. 20, 2001).

149. Hague Convention, *supra* note 146, art. 10.

150. *See* Doris Estelle Long, Comments on Draft Convention, submitted in response to Federal Register Notice (October 19, 2001) (copy on file with author).

151. Thus, for example, in an attempt to establish soft law guidelines for when conflicts might arise regarding trademark use on the internet, WIPO has established the Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet which described diverse factors to be considered, including the language of the site in question. *See* Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet, art. 3 (describing when a website may be deemed to have a "commercial effect" on a given country and including language as a factor) *available at* http://www.wipo.int/about-ip/en/development_iplaw/pdf/pub845.pdf.

152. *See generally* Jane C. Ginsburg, *Global Use/Territorial Rights: Private International Law Questions of the Global Information Infrastructure*, 42 J. COPYRIGHT SOC'Y U.S.A. 318, 319-20 (1995) (questioning the complexity in litigation of a copyright infringement suit when the protected material is disseminated to many countries through electronic means, like the internet); Rochelle Dreyfuss, *The ALI Principles On Transnational Intellectual Property Disputes: Why Invite Conflicts?*, 30 BROOK. J. INT'L L. 819 (2005) (suggesting that choice of law principles are an obvious place to begin to deal with IPR international jurisdictional conflicts); Rochelle Cooper Dreyfus, *An Alert to the Intellectual Property Bar: The Hague Judgments Convention*, 2001 U. ILL. L. REV. 421 (2001) (questioning the utility of the Draft Hague Convention in connection with intellectual property disputes). For cases which demonstrate the complexity of jurisdictional disputes over cyberspace, see, e.g., *National Football League v. TV Radio Now Corp.*, 51 U.S.P.Q. 2d 1831 (W.D. Pa. 2000) (jurisdiction wherever site is accessible), *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996) (passive advertising of schedule of Blue Note Club in Missouri did not confer jurisdiction in New York), and *Insert Systems, Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D.Conn. 1996) (passive site in Massachusetts granted jurisdiction because advertising was directed to Connecticut and all other

Lesson SEVEN: Sovereignty And Sacred Principles Are Not Easily Ignored

Most countries are generally unwilling to give up their power over something as important as the ability to determine *as a matter of domestic policy* what information gets protected by law and how.[153] When that information is perceived as having a potential impact on the growth of local commercial industries, domestic policy becomes even more significant and makes the creation of international standards which may reduce such power even more difficult to achieve. When the protection of such information collides with the cultural, political or social norms of a country – what I refer to as "sacred principles" – the odds are against achieving agreement on international principles of protection. The *LICRA v. Yahoo!, Inc.*[154] case has become paradigmatic of the problems faced when sacred principles collide. At the heart of the debate over the methods for preventing the sale of illicit Nazi paraphernalia in France is a sacred principle of French law to reduce hate and race speech.[155] In the world of cyberspace, this sacred principle was put on a collision course with another sacred principle – the U.S. principle of free speech.[156] The collision was as predictable as the result.

As noted above,[157] in order to prevent the sale of illicit Nazi paraphernalia in France, the French court had ordered Yahoo France to impose certain technological measures to prevent its French users from accessing prohibited material. Since the sale of Nazi paraphernalia is not prohibited under U.S. law, the Yahoo.com website, operated out of

---

states).

153. I do not mean to suggest that countries never cede at least partial sovereignty over such information. To the contrary, for example, Article 39 of TRIPS requires protection of certain undisclosed confidential information that has commercial value. TRIPS, *supra* note 130, art. 39. I merely suggest that a willingness to cede such authority is generally obtained as part of a balance that is struck where each party perceives itself to be obtaining some advantage. *See, e.g.*, SUSAN K. SELL, PRIVATE POWER, PUBLIC LAW: THE GLOBALIZATION OF INTELLECTUAL PROPERTY RIGHTS (2003); MICHAEL RYAN, KNOWLEDGE DIPLOMACY: GLOBAL COMPETITION AND THE POLITICS OF INTELLECTUAL PROPERTY (1998).

154. *See supra* notes 89-90 for a discussion of the French law and technological protection aspects of this case.

155. *See LICRA v. Yahoo! Inc.*, No. RG 00/05308 (May 22, 2000) (Tribunal de Grande Instance de Paris), *available at* http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi-paris_201100.htm.

156. *See* U.S. CONST. amend I.

157. *See supra* notes 89-90 and accompanying text.

the United States, became an obvious source of concern. In an effort to prevent enforcement of the order of the French court in the United States, Yahoo.com sought a declaratory judgment that such an order was unenforceable as a violation of the U.S. Constitution. The district court agreed, finding that "[a] United States Court constitutionally could not make such . . . order [prohibiting the sale of, inter alia, *Mein Kampf*]."[158] Consequently, it declined to enforce a French order requiring relief that no U.S. court could order. Stressing the critical role of sacred principles in international enforcement decisions, the court stated: "Absent a body of law that establishes international standards with respect to speech on the internet and an appropriate treaty or legislation addressing enforcement of such standards to speech originating within the United States, the principle of comity is outweighed by the Court's obligation to uphold the First Amendment."[159] While the Ninth Circuit ultimately found the first amendment determination was premature,[160] the predictable ground work has been set for the rematch.

Lesson EIGHT: Security Is A Sacred Issue

We have had no better luck establishing international standards governing internet server liability in connection with the facilitation of unauthorized P2P file trading of copyrighted works. This isn't the problem of establishing control over the ISP or even tracking the end user's identity. It's the problem of removing from governments a powerful tool for controlling content. If end users are too numerous to control adequately and websites seem to spring up overnight, the most effective pressure points for control may be the internet service providers and those who operate internet cafés. Internationally, countries routinely exempt from safe harbors those activities which are perceived to constitute threats to public order. Thus, for example, Australia prohibits activities where the content is unsuitable for

158. Yahoo! Inc. v. La Ligue Contre le Racisme, 169 F. Supp. 2d 1181, 1189 (N.D. Cal. 2000), *rev'd on related grounds*, 379 F.3d 1120 (9th Cir. 2004) (the court did not reach the First Amendment grounds for declining to enforce the order, but instead vacated the consideration of such issues as premature)

159. *Id.* at 1193.

160. *Yahoo! Inc.*, 379 F.3d at 1123.

minors;[161] Singapore makes the ISP liable if the activity is objectionable on the grounds of public order and national harmony;[162] and China imposes ISP liability for activities which endanger national security and disturbs the social order.[163] There is no country for which security is not a sacred principle (even if we may quibble over the contours of such security). Consequently, if you are creating encryption or escrow standards or any other laws, regulations, or standards that potentially impact on content or information control, there will be plenty of exceptions to whatever international standards you create, some of which may be fluid enough to make the standard evanescent at best.

Lesson NINE: Free For One, Free For All OR Act Now Or You May Not Have Information To Protect

The music industry learned the hard way that if you let people get used to downloading music without challenge, the norm you have helped develop will take on a life of its own and it will be stronger than you could ever anticipate. Despite evidence that legitimate music download sites are growing with the development of effective business models,[164] the reality is that a sizeable percentage of end users still obtain their music through illegal downloads.[165] While there may be no *single* cause, the reality is that Napster, which provided an easy-to-use and free P2P music file trading software, was launched in 1999, challenged by legal proceedings instituted that year, but was not taken

---

161. Australian Censorship Act of 1996 (WA), *available at* http://libertus.net/censor.

162. Broadcasting Act of 1996, ch. 28, § 9, cl. 2, ¶ 13(b)(i) (Singapore ISP Class Licensing Regulations), *available at* http://www.mda.gov.sg/wms.file/mobj/mobj.487.Class Licence.pdf.

163. Chinese Internet Domain Name Regulations, ch. 4, art. 19, § 2 (Sept. 30, 2002), *available at* http://www.chinaepulse.com. *See also* China's Internet Regulations, art. 15 (prohibiting the production, reproduction, release or dissemination of information that insults or slanders other people) (available in English at http://www.chinepulse.com). For a discussion of liability paradigms in general for copyright use on the internet, see Doris E. Long, *Crossing the Pond: International ISP's and the Barrier Reef of Strict Liability*, AIPLA Annual Spring Meeting (May 2004) (Published in Conference Proceedings) (copy on file with author).

164. *See supra* note 36 and accompanying text.

165. Madden & Rainie, *supra* note 36 (finding that 22% of music is downloaded from unauthorized sites and other sources; the report, however, did not attempt to determine the extent to which any such downloads might have qualified for a fair use exemption under Section 107 of the US Copyright Act and also claimed that awareness of current enforcement activity may have led respondents to underreport their use of such sites).

down until 2002.[166] By that time, P2P techniques had transformed into the Grokster model where no website indexing function was required to permit the file trading.[167] The first RIAA subpoena to an end-user for engaging in copyright infringement for P2P file trading in music did not issue until September 2003[168] – far too long to wait to bring the message to end-users that owners intended to enforce their copyrights against them. If your information is valuable, protect it in the early stages, because once people get used to having access to your information or worse to using it for free *YOU CANNOT GET IT BACK.*

The corollary to Lesson Nine is the equally painful, and equally obvious reality that *Secrets Don't Work Well on the Internet.* Our attempts to protect trade secret information from the ravages of unauthorized disclosures on the internet have not been heartwarming. The reality is once your secret formula, marketing plans, customer lists, code or even your pre-release film is posted on the internet, you usually can not get it back. Worse, we are still struggling to decide whether you lose the confidential nature of your trade secret when unauthorized parties post them.[169] If you want your authentication processes, or your encryption keys protected, pay attention to your physical protection processes. Law cannot put the genie back in the bottle no matter how hard it tries.

Lesson TEN: New Business Models May Outrun Us All

I may be a technosceptic, but I am also, I think, a technorealist. Part of the reason, I believe, we are having so much trouble enforcing intellectual property rights in both the hard goods and digital goods

---

166. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). *See also* Fanning, *supra* note 11. The site was later reborn as an authorized site for legitimate music downloads. *See* Napster, www.napster.com.

167. Metro-Goldwyn Mayer Studios, Inc. v. Grokster Ltd, 289 F. Supp.2d 1029 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *rev'd*, 545 US 913 (2005) (describing the differences between the functioning of Napster and Grokster model file sharing methodologies).

168. *See, e.g., Not-So-Jolly Rogers*, ECONOMIST, Sept. 10, 2003, http://www.economist.com/agenda/displaystory.cfm?story_id=E1_NDVDQGS (reporting on filing by RIAA of more than 250 lawsuits against end users for illegally downloading music onto their computers).

169. *Compare* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D.Va.1995) (noting that "[o]nce a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve") *with* DVD Copy Control Ass'n Inc. v. Bunner, 116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185 (Cal. App. 2004) (recognizing that not all publications on the internet automatically result in loss of trade secret status).

worlds presently is because the business models we are using, and the laws that we use to protect those models, do not accurately reflect the current real world requirements for the development of innovative and creative works. Despite our constant reconfiguration of copyright law in the Digital Era, we are still struggling to define the parameters of fundamental issues regarding the scope of rights which should remain in the hands of authors.[170] I am not suggesting that all of copyright law is inapplicable to the Digital Era. To the contrary, if these ten lessons demonstrate anything, they demonstrate that much of the policy behind the laws which we developed for the hard goods world remains equally vital today. The fundamental precepts – that copyright law is designed to promote the creation of new works[171] and that trademark law is designed to protect consumers from false designations of origin[172] – remains at the core of cyber-protection today. What we have learned, however, is that businesses models may in fact solve legal problems.

While digital piracy remains a problem, alternative business models, such as iTunes, that effectively meet consumer demands have reduced some of that problem.[173] Similarly, the negotiation between copyright owners and social networking sites such as YouTube for licenses to allow the posting of end user created adaptations has reduced some of the clamor for immediate action to resolve the legal issue.[174] Although business models still need to be protected by the appropriate legal building blocks, we must be careful not to act too quickly or in too strained a manner to make whatever legal standards we create either as evanescent as the AHRA or as cumbersome as the DMCA. In cyberspace, as in the hard goods world, whatever standards we impose for electronic commerce must be based in both the reality of the

---

170. These include, inter alia, the economic rights which should inhere to the author for new uses for her works, including the right to enter into new digital markets through "transformations" of earlier works, see, e.g., *Perfect 10, Inc. v. Amazon.com, Inc.*, 487 F.3d 701 (9th Cir. 2007), and the theory on which liability for violations of authorial rights should be imposed. *See* Reichman & Lewis, *supra* note 14.

171. *See, e.g.*, Eldred v. Ashcroft, 537 U.S. 186 (2003). *See also* U.S. CONST., art. I, § 8, cl. 8 (establishing the Constitutional purpose for federal copyright law to "promote the Progress of Science and the useful Arts").

172. *See, e.g.*, Stahly Inc. v. M.H. Jacobs Co., 183 F.2d 914 (7th Cir. 1950).

173. *See, e, g., Legal Music Downloads at 35%, Soon to Pass Piracy,* slashdotcom (June 21, 2005).

174. *See, e.g.*, Andrew Orlowski, *Universal Exec Says Goodbye to the Old Record Co.* (Jan. 20, 2007) (announcing licensing arrangement with YouTube to allow end users to post music), *available at* http://www.theregister.co.uk/2007/01/20/kenswil_license_stuff.

marketplace and the aspirational goals we establish for the fair working of such a marketplace.

CONCLUSION

Despite the appearance of cyberspace as alternatively a wild frontier or a technological battlefield, it, nevertheless, remains a potent arena for global digital commerce. Experience, including social norming demands, demonstrates that we must reconsider hard goods laws and policies in this new electronic marketplace. Yet the evanescence of technological controls and the perceived utility (or desirability) of illicit conduct in this new frontier for business make any regulation problematic at best. An examination of some of the lessons learned in the hard fought (and on-going) battles over the control of intellectual property-based goods and services in cyberspace provide useful warnings for crafting international standards to protect and promote commercial transactions utilizing the latest communication technologies. The ultimate lesson for all of us, however, may be that in crafting rules for cyber-commerce, policy must be created with a firm view toward the special nature of the internet and in maintaining its potential to level the commercial playing field to allow all countries to participate in their own economic and commercial development. Just as business has learned to constantly reinvent itself to compete in the changing environment of cyberspace, we must similarly accept that rules and policies must constantly be revisited to avoid unintended consequences of earlier visions. The value of cyberspace as a commercial medium ultimately is only as great as the fairness under which it is operated.