Music, Padlocks and the Commons

Maître Stéphane Desrochers*

Étude présentée au Professeur Ysolde GENDREAU

Avril 2000

* L.L.M., Maîtrise en droit, axe technologies de l'information, Université de Montréal

Table of Contents

Introduction

De la musique avant toute chose,
Et pour cela préfère l'Impair,
Plus vague et plus soluble dans l'air,
Sans rien en lui qui pèse ou qui pose.
Paul Verlaine

1. Did Verlaine envision the digital World ahead? Perhaps. Perhaps not. He did put the finger on a truth so plain it took the invention of the Internet for most of us to figure it out. Music is gaseous. It weighs nothing. Present an opening and it seeks to escape whatever vial we have put it in.

2. The MP3 music compression format has caused something of a revolution. Brokers in pirated tunes began mushrooming throughout the Internet. College students went into a frenzy of illegal activity. Suddenly, abruptly, music was released into the masses for all to copy and to enjoy. The recording industry despaired. But the recording industry, with help from its parent electronics and information technology industries is building a better vial. Recognising the potential of online distribution of music and sound recordings, the industry is moving toward a secure platform for distributing its products. Collectively referred to as "Trusted Systems", various technological countermeasures are being developed to put a stop to digital piracy. The Trusted Systems architecture also promises greater access and significantly reduced prices for the consumer. Imposed technologically and contractually, Trusted Systems challenge the hegemony of copyright law in many ways. Immutable settings programmed in the trusted software and hardware will give copyright owners total control over the uses of the works.

3. This essay is set out in three sections. The first examines the technologies that led to the "liberation" of music in the Internet. It focuses mainly on copyright law's efficacy in this period of technological change. The second part poses the analytical framework for regulating copyright law in cyberspace. In it we discuss how technology - in this instance Trusted Systems - can substitute for the law and afford copyright owners protection on a level they have never known in the physical World. This, we suggest, threatens the public's rights to use works of music fairly under current legal doctrine. In the third section we argue that Trusted Systems form an integral part of a larger "Maximalist Agenda" of copyright, which would ultimately diminish the intellectual property *commons.*

Part I – Technological Change and Copyright Law Efficacy

a) Digital technology and open networks: threats to copyright?

4. It is widely believed that digital technology and the Internet pose a grave threat to copyright owners. Allegedly, counterfeit works are massively reproduced, zipped around the Internet in seconds, downloaded onto the hard drives of non-paying users, where they remain, to be read, listened to, visualised again and again, or to be altered to suit the tastes of the user, or to be engraved onto discs for convenient carry. This, copyright owners tell us, entails for them economic losses on a large scale, and translates, for the law-abiding, fee-paying consumer, into higher prices. An all around bad deal for authors, and the consuming public.

5. Other technologies have come along in the past – the tape recorder to name just one - which have also been called copyright unfriendly. To be sure, such infringement enablers have caused much hardship to owners and authors alike. But the Internet is different. Commentators from all sides of the legal-technological spectrum have foreseen the death of copyright! A question then begs to be asked: how is the Internet so different that, as we are now on the footstep of a new, IP fuelled, economy, many serious and respected scholars are converting to copyright doomsayers?

6. Indeed the Internet raises novel concerns regarding copyright enforcement. Andy Johnson-Laird, for one, has described the Internet as the 'global copying machine', noting that '[…] One is hard pressed to describe anything on the Internet that is the "original" of a work'[1]. Generally speaking, there are four features of the Internet that imperil copyright owners' rights to control the distribution of their works and to derive revenues thereon[2].

7. Perfect copies. Contrary to analog technologies, copies of digitised works are in every way identical to the 'original' file, with no degradation of quality. Absent the consideration of preserving quality, there are no compelling incentives for the consumer to seek out the legitimate source – whether the author or titleholder - of the work.

8. One-to-one communication. , The Internet allows for one-to-one communication, (e.g. cutting out the middlemen). This is sometimes referred to as the 'disintermediation effect'. Thus, contrary to distributing physical CDs - a complex enterprise which presupposes organized networks, physical outlets, transportation, time – digitised music can be distributed through the Internet instantaneously, on a very large scale, and at zero marginal cost.

9. Anonymity. Because of the accelerated growth of the Internet, measuring its size is at best an arduous task layered with obstacles, and likely to yield only approximate figures. A compounding problem is the lack of a central registration authority, so that carrying out a census would be improbable. The resulting boon for users is relative anonymity. We say relative since every computer connected to the Internet is tagged with an electronic address. Not much of a deterrent for savvy copyright pirates however. Owing to the size and transnational aspect of the Internet, pirates are notoriously hard to track down across the cyber landscape. To complicate things, services such as *anonymous remailers* make it possible to conceal one's computer's electronic identifiers through a readdressing/rerouting scheme. Of course, near perfect anonymity is possible by using robust encryption software – the Pretty Good Privacy (PGP) freeware is the premier example of this - which scrambles communications thereby rendering copyright piracy undetectable.

10. Lack of consumer education. As is the case with the general public, Internet users are blissfully ignorant of IP laws and unknowingly engage in micro-infringements. While someone who downloads a

[1] JOHNSON-LAIRD, A., "The Anatomy of the Internet Meets the Body of the Law", 22 *U. Dayton L. Rev*. 465, printemps 1997, p. 1.

[2] SCHLACHTER, E., "The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet", 12 *Berkeley Tech. L.J.*, 1997, p.4, available at: <http://www.law.berkeley.edu/journals/btlj/articles/12_1/Schlachter/html/reader.html>.

copy of a Web page when browsing onto his or her computer cannot by any stretch be labelled a pirate, widespread micro-infringements, particularly on the scale of the Internet, presumably amount to considerable losses in the copyright owners' hands.

b) The MP3 revolution: the need for speed

11. The Internet's rapid growth is well documented. With connections well exceeding 100 million and fast rising, the obvious drawback is the correlative congestion of the infrastructure, which, as anyone logging on during "rush hours" knows, was not built initially to carry so much traffic. In Internet speak, congestion equals slower connections or, worse, halted connections.

12. Internet performance is volume sensitive and files containing music, in comparison to text files, are much larger. Transferring music files takes up a lot of "bandwidth" e.g. space on the info-highway. Downloading a three-minute song, using a now standard 56K modem, may easily take two hours, let alone an entire album. To make things worse, downloading music files consumes precious disk space on one's computer. Clearly discouraging.

13. Enter the MP3 format. MP3, which stands for MPEG 1 (Moving Picture Experts Group 1), audio layer 3, is a file format for compressing digitised music files, enabling fast and space efficient downloading. In the wake of MP3, new technologies have been developed to harness this new potential: software that converts CD recordings into MP3 files, portable MP3 players, MP3 search engines…

14. Notably, the MP3 format has spawned numerous pirate sites, which compile and make available without charge an array of recordings in MP3 format. Claiming rampant illegal copying of its copyrighted materials, the *Recording Industry Association of America* (*RIAA*) has instituted suits against the notorious *MP3.com* and, more recently, against *Napster.com*, both being charged with facilitating infringing activities. An excerpt of *RIAA*'s complaint against *Napster.com* is particularly telling of the perceived damages entailed by owners:

> "*Napster is similar to a giant online pirate bazaar: users log onto Napster servers and make their previously personal MP3 collections available for download by other Napster users who are logged on at the same time. Napster provides its users with all the facilities and means to engage in massive copyright infringement. For example, Napster provides users with a hub of central computer servers to which they connect; a continuously updated database of "links" to millions of pirated recordings; software that allows fast, efficient identification, copying and distribution of the pirated recordings; and a host of other services -- all of which enable and encourage Napster users to download millions of pirated songs as well as make available their own music library for others to copy. Because Napster creates its links from the personal MP3 collections of Napster users, without Napster, these infringements would not be taking place at all*."[3]

c) Efficacy of copyright law

15. The Internet/MP3 combination apparently has sent the copyright regime reeling. Many question its relevance, pointing to seemingly insurmountable practical obstacles in enforcing it. The issues so often raised commonly pose a central question, that of the efficacy of copyright law in the Internet age. Efficacy of law is not to be confused with the effectiveness of law, that is, its propensity to produce foreseeable and unforeseeable effects. The efficacy of law can be explained as a measure of attainment of the law's goal of tailoring behaviours toward socially desirable results. Professor Harry Jones posited

[3] RIAA press release, Washington, December 7, 1999, available at <http://www.riaa.com/piracy/press/120799.htm>.

that the efficacy of a law is measured negatively by gauging five types of failures, four of which have been deemed relevant in our analysis[4]:

16. Failures of communication. According to Jones, a law fails to communicate when the persons subjected to the law are not positively forewarned of its precepts or simply do not comprehend them subjectively[5]. As regards the application of copyright law to the Internet context, the failure of communication arises not only from the obscurity of the law but often from the technology itself. For instance, the simple act of browsing the Web can naturally be assimilated to the act of flipping through the pages of various magazines in a convenience store. In fact, when opening a Web page, the client software requests that the server transfer a copy of the file for immediate storage into the client computer's memory, which in turn displays the page on the screen. A copy has been made within the meaning of the copyright law[6].

17. One of the Web's foremost characteristics is the ability to create hypertext links to outside websites, thereby enriching the text with external views or sounds or images or graphs. Hypertext linking offers limitless possibilities for creativity and is a core value of electronic editing. Yet a United Kingdom court has granted injunctive relief to a newspaper requesting that a competitor refrain from linking to its website on grounds of copyright infringement[7]. Who Knew?

18. Does forwarding a copy of a privately sent email to others constitute copyright infringement? More to the point, is an electronic message in the form of an email a work under copyright law? These are tricky questions raised in courts of law, hardly within the grasp of the common user.

19. Failures to enlist supportive action[8]. Copyright law is private law. It establishes a series of exclusive proprietary rights, with means to publicize and contract them away. It also provides for recourses including injunctive and compensatory. Naturally, in a proprietary framework such as that of copyright law, the responsibility for enforcing the rights lies with the copyright owner.

20. In a context of massive infringement activities, failure on the part of the copyright owners to enlist supportive action, that is to seek and obtain redress, gravely reduces the efficacy of the law. That, in a word, is the *raison d'être* of copyright owners' associations such as the *Society of Authors, Composers and Publishers of Music of Canada* (*SOCAN*) and the *American Society of Authors, Composers and Publishers* (*ASCAP*) in the United States. While major battles have been won[9] and inroads made by these associations regarding webcasting[10] (e.g. the broadcasting of music via the Internet), the legal battles respecting MP3 piracy have yet to shift the tide in favour of copyright titleholders.

21. Even worse than the failure to enlist supportive action is the mounting of highly publicized legal campaigns which yield little tangible results. The all powerful *RIAA*, at times dubbed the "Evil Empire" in

---

[4] JONES, H. W., "The Efficacy of Law", *Rosenthal Lectures*, Evanston, Illinois, Northwestern University Press, 1968, p. 14.
[5] *Ibid.*, p. 15.
[6] POST, D. "Plugging In – New Wine, Old Bottles : The Evanescent Copy", *The American Lawyer*, Vol. XVII, No. 4, p.2, available at <http://eon.law.harvard.edu/h2o/property/alternatives/post.html>.
[7] *The Shetland Times* v. *Wills*, Court of Sessions, Edinburgh, October 24, 1996, available at <www.shetlandnews.co.uk/opinion.html>.
[8] See JONES *supra*, note 4, p. 21.
[9] See the Copyright Board of Canada's ruling on Tarif 22, regarding the Statement of Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Musical or Dramatico-Musical Works, issued October 1999. The Board ruled that SOCAN was entitled to collect royalties for the performance of musical works by webcasters via the Internet.
[10] WIRED NEWS REPORT, "Musicians Finally See Net Gains", *Wired News*, March 21, 2000, <http://www.wired.com/news/technology/0,1282,35085,00.html>. ASCAP has entered into a partnership with Audiosoft regarding a technology which permits the monitoring of webcasting activities on the Internet. ASCAP has already licensed some 1500 webcasters, who will use the technology henceforth to report their activities to ASCAP.

the rebellious cyber community, has launched suits in four directions, the results of which professor William Fisher of Harvard Law School has characterized as "inconclusive"[11]. The learned professor has provided valuable insight into the murky waters of the *RIAA*'s suits against the "copyists"[12], the "Equipment Manufacturers"[13], the "Pirate Sites"[14], and the "Search Engines".

22. First, the legal case against a "copyist", a person who downloads an MP3 of a copyrighted song without permission, is doctrinally sound. But, notes professor Fisher, practical impediments render it almost impossible to make any marked gain on this front since 1) copyists are difficult to locate amidst the Internet galaxy; 2) suits against individuals are bad from a PR standpoint; 3) a large number of suits is needed to attain critical mass and really have an impact.

23. Second, the legal basis for attacking the "Equipment Manufacturers" on contributory infringement grounds is shaky, especially in light of the 1984 decision in the Sony Betamax case[15]. In addition, the *RIAA*'s failed suit against Diamond Multimedia, the manufacturer of a portable MP3 player, where the Court of Appeals for the Ninth Circuit held that the Audio Home Recording Act did not apply to its device, should cool off litigious ambitions in this direction[16].

24. Third, pirate sites seem particularly vulnerable to infringement suits and would be rather easy pickings for the *RIAA*. Through the use of letters enjoining pirate sites to cease operations, the *RIAA* has succeeded in scaring away a good number of sites. While this strategy has to a degree produced encouraging results, MP3 pirate sites have not fallen into extinction just yet notes professor Fisher. As sites are shut down, new ones just keep popping up.

25. Fourth, legal challenges aimed at "Search Engines", especially *Napster.com*, which poses the greatest threat to the *RIAA*'s copyrighted assets, have recently been instituted. *Napster.com*, unlike regular search engines, allows the user to download the *Napster* freeware. This software enables users logging on to *Napster.com* at the same time to pool together their MP3 music files and form a huge selection of works. The individual user can then download the pieces that interest her onto her hard drive. An important point of fact here is that *Napster* enables the pooling of all varieties of works, including copyrighted works, voluntarily unprotected works and works in the public domain. While one may convincingly argue that *Napster* facilitates infringing activities, clearly it also enables the permissible copying of freely available works. Hence, the contributory infringement claim against *Napster* is weakened.

26. Failures of enforcement. To borrow from Jones, enforcement "[…] *is the imposition of sanctions by or at the instance of some public prosecuting authority*"[17]. The crux of the enforcement question is the deterrent effect of punishment. True to Benthamian tradition, Professor Jones has highlighted two conditions of effective deterrence: the *certainty* and the *proximity* of the punishment[18]. Certainty here refers to the more or less high order of probability that an offender will face sanctions, while proximity relates to the frequency and regularity of sanctions in proportion to threats.

27. The Internet transcends territorial boundaries. An offence committed in cyberspace is plausibly committed in every jurisdiction within the Internet's reach, but committed nowhere in particular. Assuming that a given behaviour were criminalized in every Internet jurisdiction, the problems of jurisdictional attribution, collecting evidence, locating offenders, ensuring their presence in court,

---

[11] FISHER, W., "Digital Music : Problems and Possibilities", March 19, 2000, available at <www.law.harvard.edu/Academic_Affairs/coursepages/tfisher/Music.html>.
[12] *Ibid.*, p. 3.
[13] *Ibid.*, p. 3.
[14] *Ibid.*, p 4.
[15] *Sony Corp.* v. *Universal Studios, Inc.*, 464 U.S. 417 (1984).
[16] *Recording Industry Ass'n of America* v. *Diamond Multimedia Systems, Inc*., U.S. 9th Circuit Court of Appeals, docket number 9856727, June 15, 1999.
[17] See JONES *supra*, note 4, p. 30.
[18] *Ibid.*, p. 32.

securing convictions, to name just a few, gravely undermine the precepts of certainty and proximity. More to the point however, with respect to copyright law the assumption made above does not hold true in every jurisdiction. Some countries, namely Middle Eastern and Far East countries are notoriously lax toward copyright infringement, while others even promote it, under feigned denials, as a tourist attraction[19].

28. Another problem concerning enforcement by public authorities is that of resources already spread thin[20]. Considering the order of volume of the infringement offences presently taking place on the Internet, the few attempts made call to mind a fencing bout against a windmill. Furthermore, prosecuting copyright offenders obviously presupposes choices in allocating policing resources, choices that are inherently political. Whether there exists such a political will to eradicate malevolent copying remains unclear to date, largely due we assume to the difficulty of the task at hand and the already inconclusive results obtained on the civil front.

29. Failures of obligation. Failures of obligation are deeply rooted in the ever-fluid notion of the law's legitimacy. Failures of obligation go directly to the perceived ideas of what is right and what is wrong, but also to the fear instilled in people's mind that non-compliance will bring sanctions. Jones writes: "[…] most people obey most of the law most of the time either because they feel in their hearts that they should, or because they are apprehensive of possible punishment if they do not, or for both reasons at once"[21].

30. Aside from the technological advances that have made copyright infringement simple and practically cost and risk free, perhaps the gravest danger copyright law faces, more now than in the past when serial copying technologies were introduced, is a legitimacy crisis. Strangely, at a time when more and more of the world's wealth is accrued through intellectual output, changes in technology and cultural values are leaguing together to erase copyright law's practical and moral foundations.

31. Eric Schlachter has correctly asserted that the "Internet culture" quietly accepts the flouting of copyright law[22]. His insightful look inside the Internet sociology tells of a space originally populated by academics and technologists, who were primarily motivated by the sharing of the fruits of their intellectual labours, with an implied understanding of likewise reciprocation. The second wave of Internet settlers comprised of persons in the under-thirty age segment. Accustomed throughout their lives to having easy, unimpeded and free access to informational goods of all kinds, notably with the use of various copying devices such as audio and video tape recorders, the photocopying machines and the computer, this population segment does not even remember a time when information was proprietary and scarce.

32. The Internet culture offers a glaring paradox. Staunchly libertarian, the "netizens", as they are sometimes referred to, firmly believe in the freedoms associated with property rights. Things highly valued are the freedom of expression on one's web site and the right to the sanctity of one's email inbox in regards to unsolicited email. On the other hand, the property of others posted on the Web is decidedly fair game, open to limitless copying and distribution. Schlachter makes this interesting point:

> "*More generally, the combination of the Internet culture and the general effect of technological evolution may be affecting our collective attitudes toward intellectual property. We have become a culture largely comfortable with serial micro-infringements. Generally, we want to respect other people's intellectual property rights, but we also want to run our lives in a way that ultimately results in numerous minor, almost trivial, but still theoretically*

---

[19] MANN, C., "Who Will Own Your Next Good Idea?", *The Atlantic Monthly*, September 1998, <www.theatlantic.com/issues/98/copy.html>.
[20] See JONES *supra*, note 4, p. 33.
[21] *Ibid*., p. 78.
[22] See SCHLACHTER, *supra,* note 2, p. 16.

actionable infringements. The effect of trying to try to apply copyright laws (or worse, to try to strengthen them) to overcome this attitude would likely be regressive."

33. Of course one of the great lures of the Internet is all the free stuff. Some of the Internet's Crown Jewels – *Yahoo!*, *Hotmail* and now *Napster* - were built on the offering of services, content or software without charge. Schlachter notes that "*In this environment, users become very reluctant to pay for intellectual property, since they know that free substitutes are likely to be available elsewhere*"[23]. In this frame of mind then it could be asserted that by releasing MP3 samplers to stimulate interest in their chargeable products, the recording companies are to a certain extent adding weight to the collective "*conditioning to expect freebies*"[24]. One comes very near to suspecting that, for the all the industry uproar, the MP3 phenomenon has actually increased the sales of music CDs[25].

34. Copyright law has come increasingly under criticism since the creation of anti-copyright advocacy groups whose precepts are gaining momentum in the wired community. Certainly the Open Source Movement has recruited many soldiers for the cause. But Open Source is not anti-copyright per se, since it relies on copyright to guarantee certain fundamental Open Source freedoms; freedom to make and distribute copies of the program, freedom of access to the program's source code and freedom to improve the program[26]. Legalities aside, the Richard Stallmans[27], Eric Raymonds[28] and Linus Torvalds[29] of the cyberworld speak liberating words for a new age of IP Renaissance. This is guruism at its brightest.

35. And then he came. The Barbudo Maximo, the Internet Che, shouting the *Revolucion.* John Perry Barlow, the former Grateful Dead, retired cattle rancher, cyberspace visionary, leads the philosophical battle against copyright, against ownership of works and against ownership of creators under a corporate dictatorship. His now famous essay "*The Economy of Ideas"* reads like a manifesto against the IP legal regime[30]. Stressing the point that IP laws were conceived during a time in which creating value meant creating physical things, and that this time has long passed, he explains how IP laws, like crutches for the healed, have fallen into irrelevance. He writes:

"*Whenever there is such profound divergence between law and social practice, it is not society that adapts. Against the swift tide of custom, the software publishers' current practice of hanging a few visible scapegoats is so obviously capricious as to only further diminish respect for the law.*

Part of the widespread disregard for commercial software copyrights stems from a legislative failure to understand the conditions into which it was inserted. To assume that systems of law based in the physical World will serve in an environment as fundamentally different as cyberspace is a folly for which everyone doing business in the future will pay.

---

[23] *Ibid.*, p. 16.
[24] *Ibid.*, p. 16.
[25] Forrester Research Inc. has recently published a report indicating a connection between young consumers' browsing habits and increased sales of CDs and other entertainment ticket items offline. See the press release "The Internet Is A Friend To Offline Entertainment, According to Forrester Research", available at <www.forester.com/ER/Press/Release/0,1769,264,FF.html>.
[26] PERENS, B., "The Open Source Definition" in Chris DiBona, Sam Ockman and Mark Stone (eds) *Open Sources: Voices >From the Open Source Revolution*, Sebastopol (CA): O'Reilly and Associates, Inc., 1999.
[27] Founder of the Free Software Foundation, <http://www.fsf.org/fsf/fsf.html>.
[28] Programmer and author of the famous essay "The Cathedral and the Bazaar" available at <http://www.tuxedo.org/~esr/writings/cathedral-bazaar/>.
[29] Father of the Linux operating system, which he released into the Internet to be further developed in open source.
[30] BARLOW, J.P., "The Economy of Ideas", *Wired*, 2.03, Mars 1994, <www.wired.com/wired/archive/2.03/economy.ideas_pr.html>.

As I will soon discuss in detail, unbounded intellectual property is very different from physical property and can no longer be protected as though these differences did not exist. For example, if we continue to assume that value is based on scarcity, as it is with regard to physical objects, we will create laws that are precisely contrary to the nature of information, which may, in many cases, increase in value with distribution."[31]

[31] *Ibid.*, p. 5.

Internet, an unregulated space?

36. In the early years of the Web, lawyers and legal scholars alike commonly believed that cyberspace was largely unregulated, perhaps even impervious to any attempts at regulating it. Transnational issues, jurisdictional issues, practical issues all seemed to take on a complexity unparalleled in the physical World. Most cyber denizens embraced the newfound freedom, enjoying the anonymity and cultural openness it provided. This, they thought, was no place for governments to meddle in.

37. Some proposed the idea of recognising cyberspace as an altogether place. The virtual border already exists, since booting up the computer and connecting to the Internet imply positive actions dictated by a will akin to psychologically crossing into another realm. This, it is claimed, would surely attenuate the legal frictions caused by transnational communications. For copyright law, recognising cyberspace as a place would stimulate doctrinal incursions into uncharted conceptual waters[32].

38. There are self-regulation and market forces faithful who believe that the Internet should be left alone to police itself. Conduct codes, *netiquette*, standards, labelling schemes and other such normative manifestations owed to legal pluralism are expected to rise to the challenge of regulating cyberspace. With the impetus placed squarely on good citizenry and preserving one's reputation, the perceived futility of trying to enforce positive rights becomes a non-issue.

39. As we shall see in part II of the essay, these assumptions regarding cyberspace regulation were naive.

[32] JOHNSON, D. & POST, D., "Law and Borders – The Rise of Law in Cyberspace", 48 *Stanford Law Review*, 1367, 1996, available at <http://www.cli.org/X0025_LBFIN.html#4>. Copyright Law.

Part II – A Lessigian Theoretical Framework for Enforcing Copyright in Cyberspace

a) A theoretical framework for regulating cyberspace

40. Lawrence Lessig, the Berkman professor for Internet and Society, has provided us with the theoretical foundations for the study of Internet regulation. He rejects the common view that the Internet's very nature, its design, shields it from regulatory efforts. Acknowledging that the Internet's original design made it extremely resistant to regulation, he deconstructs the notion that this design is forever unchanging, that in fact cyberspace is fast becoming more *regulable* and more regulated than any physical space has ever been[33].

41. Indeed the design of the Internet, what Lessig calls *code*, can be changed. *Code*, that is the body of protocols, software and hardware that make up the Internet's architecture, can be transformed either to coerce behaviour or to become more easily *regulable*. Government can direct *code* in certain directions through certain regulatory techniques.

42. In the Lessigian conceptual canvass, there are four types of constraints that regulate behaviour in cyberspace: law, social norms, markets and *code*. These four types of constraints are interrelated and interact to produce a net regulatory effect on the object of the regulation. The regulatory technique involves finding an optimal dosage of direct regulation (for instance law prohibiting a behaviour) and indirect regulation (for instance law creating a new tax to raise prices and discourage a behaviour).

43. Law, as understood by positivists, applies to the Internet on principle. Copyright law has not been repealed following the creation of the Internet. That a law may be unenforceable for practical reasons does not make it any less applicable[34]. Social norms also dictate behaviours, with the difference that enforcement relies solely on the denunciation of the reproachable conduct by the community. Offenders of social norms expose themselves to being shunned, denied access to influential circles, and stripped of their reputational capital. Markets constrain behaviour through the instrument of price, which determines choices between economic opportunities. Finally, *code* determines whom may have access and on what conditions[35]. For example, *code* can be written such as that a website offering pornographic material will not grant access unless a digital certificate authenticating the age of the visitor is produced. Filtering software will determine the scope of students' rights to access information when logging on to the university's network. Encryption software, if available, will secure their right to communicate confidentially.

44. Lessig posits that in Cyberspace *code* is the dominant constraint. In a sense, the "legislative" power in Cyberspace is concentrated within the hands of the *code* writers. Of course the power of *code* may be harnessed; in other words laws can dictate the parameters of *code* to achieve a regulatory objective. The Audio Home Recording Act of 1992, which provides at s. 1002 that manufacturers of audio devices must incorporate copying controls, offers an example of how law could constrain *code* writers to develop software that functions on a secure format, thereby rendering impermissible copying and distribution impossible, or at least very difficult[36]. As we shall see, *code* can also have an effect on law.

b) Coding the law: Trusted Systems

45. Realising the implications of massive copyright infringement for corporate interests and sensing that "there's gold in them thar hills" for whomever devises a workable solution, technologists have rushed to develop ways and means to secure the assets. Collectively referred to as "Trusted Systems", a term

[33] LESSIG, L., "The Law of the Horse : What Cyberlaw Might Teach", *Harvard Law Review*, fall 1999, p. 6.
[34] *Ibid.*, p. 9.
[35] *Ibid.*, p. 10.
[36] Audio Home Recording Act of 1992, 17 U.S.C. §§1001-1010

coined by Mark Stefik[37], new technologies purport to protect the informational assets of copyright owners, while drastically lowering costs of accessing information. Trusted Systems, it is claimed, offer the promise of liberating the full potential of the Internet as the world's universal library, since creators will gladly publish their material online once they are assured of being rewarded for it.

46. Musicians and music lovers alike would benefit from the secure distribution of works on the Internet. By connecting directly the publisher and the consumer, thereby eliminating the middlemen, Trusted Systems would bring prices down to a fraction of what they are offline[38]. Perfectly efficient distribution would be achieved through network distribution since the wasteful stockpiling of CDs based on approximate demand forecasts would be eliminated. Trusted Systems would also make possible optimal pricing through "price discrimination", the technique that consists of pricing a good or a service incrementally in order to reach a wider range of consumers depending on willingness to pay.

47. Stefik, understandably, sees a bright future for Trusted Systems. As he points out, automated copyright management systems could provide round-the-clock access to high quality works from any point on the globe[39]. Unlike the MP3 apostles who prophesies the irrelevancy of copyright owing to the near impossibility of enforcing the law, the people in the Trusted Systems camp see automated enforcement spelling the demise of copyright. Different scenarios, similar result. Below we sketch some of the inner workings of Trusted Systems.

48. Comprehension will be done a service by going through the basics of how Trusted Systems function. Firstly, late generation Trusted Systems rest on a number of constitutive elements:

49. Protocols. For machines to recognise trustworthy machines, they must speak the same language. Protocols are neatly defined sets of propositions and replies enabling data interchange between two or more computers. Trusted Systems rely on protocols for authenticating that the client software or hardware says who it says it is and can be trusted. The protocols must also allow content providers to set the level of security of the transaction[40].

50. Encryption. The science, some would say art, of scrambling messages to render them unintelligible is a pillar of Trusted Systems technology. In short, encryption allows for "hacker proof" transactions; encrypted materials are useless in the hands of those who are unable to speak the perimeter password. Encryption is also used to preserve the rights of consumers to confidentiality and to personal data privacy.

51. Micropayments. To accommodate a wide range of services, including for example the reading of a single newspaper article, or listening to a song occasionally, a workable technology to permit payments in the order of dimes and quarters is needed.

52. Watermarks. Watermarks are the functional equivalents of radio beacons for the Internet. With watermarks, uses of the copyrighted materials are monitored so that unlawful uses would be detected and reported back to the content provider. Invisible or inaudible, watermarks act as electronic tags that contain specific details respecting the identity of the purchaser and the type of Trusted Systems with which a file is compatible. Scattered illegal copies of a work bearing a watermark will ultimately point to the source of the copying, the initial purchaser[41].

53. Databases. The widespread use of Trusted Systems will generate huge amounts of data that will be stored and managed with the help of databases. These oceanic pools of data will present the content

---

[37] Principal scientist in the information sciences and technology laboratory at the Xerox Palo Alto Research Center.
[38] STEFIK, M., "Trusted Systems", *Scientific American*, March (1997), p. 2, available at <www.sciam.com/0397issue/0397stefik.html>.
[39] *Ibid.*, p. 8.
[40] *Ibid.*, p. 4.
[41] *Ibid.*, p. 5.

providers with some concerns as well as opportunities. On the one hand, consumers will demand that their right to read, listen, and view anonymously be respected. The correlative duty of the providers will be to take the necessary steps to safeguard their clients' sensitive information. On the other hand, powerful data mining technologies applied to the databases would likely unlock precious marketing knowledge, to the point that the databases themselves might constitute assets more valuable than the copyrighted content. Essentially, the databases would become a commodity.

54. Secondly, on the premise that function follows form, a better understanding of how Trusted Systems work can be gained by comparing them to a better-known technology. The CD, triumphant over the vinyl record and the tape cassette, we assume is familiar to most. The table below attempts to add clarity.

COMPACT DISC	TRUSTED SYSTEMS
Physical object. The physicality of the CD is perhaps its most differentiating feature. Purchasing a CD procures the right to a physical object, not to the music itself. That object is then under the custodial power of the owner, whom can use it any way he pleases: he may decide to listen to it intensively for a time, then lend it to a friend, or exchange it for another CD. He may also sell it or donate it to the local library.	**Internet service** When subscribing to an Internet music service, one becomes party to a licence enumerating certain conditional rights. Everything not specifically listed is impliedly prohibited. Permissible uses may or may not be chargeable. For example, viewing the title of the song and listening to a 10-second sample may be granted with no charge. Listening to an entire song may be granted subject to payment of a fee. Cutting out an excerpt of the song, or copying it, or sending it by email to a friend is generally prohibited[42].
Inanimate A CD is a CD!	**Smart** Trusted Systems are designed to facilitate data interchanges. To do so, there must be an initial gathering of information, which must then be authenticated through some form of cross-referencing. Decisions to grant, or grant conditionally, or deny certain uses are made automatically in accordance with a defined set of parameters. Data is stored in databases, maybe even data warehouses, where it is mined to form customer profiles and extrapolate consumer trends.
Mobile A CD fits neatly inside a coat pocket.	**Fixed** Trusted Systems deliver music to a specific IP address. The music file is attached onto the hard drive where it remains. Unless it has been affixed onto a portable computer or, eventually, a hand held device, carrying music around is problematic.
Autonomous A CD is self-contained.	**Networked** Trusted Systems are communicational by nature. A client – server relation must be established. The "Universal Jukebox" model, whereby a subscriber pays a monthly fee to gain unlimited access to tracks listed in the provider's catalogue, marvellously illustrates

[42] CHICOLA et al. "Digital Rights Architectures for Intellectual Property Protection: Legal/Technical Architectures of Cyberspace", available at <http://cyber.law.harvard.edu/ltac98/trustsys.html#_Toc437906319>.

	this point. Where permission is granted to transfer via email a song to a friend's computer, the trusted file bearing a watermark will relay the transaction information to the server.
Refundable Got a scratch on it!? Return it.	**No** Online services are licensed rights to use. Usage is provided linearly in time. Terminating the contract does not give rise to a claim for services consumed in the past.
Untraceable Any pirated CD is safe from prying eyes in the privacy of the home.	**Traceable** Watermarks remember!

c) Shrinkwrap, Clickwrap, Shoobidoowrap

54. As we have discussed above, Trusted Systems rely on a series of basic technological components. But Trusted Systems incorporate a legal component as well: the copyright licence. As more and more people get pulled into the Internet vortex and become accustomed to experiencing culture in cyberspace, the pervasiveness of Trusted Systems will bring on a generalization of copyright licences to the detriment of sales of CDs. Naturally, licences in cyberspace take on the form of "clickwrap" licences.

55. Clickwrap licences get their name from their offline precursors "shrinkwrap" licences, who owe the appellation from the commercial practice of packaging software, either diskettes or a CD-ROM, in a box recovered by plastic of cellophane "shrinkwrap". The particularity of shrinkwrap licences is that the terms and conditions of the licence are generally set out in a booklet inside the box. After the consumer has purchased the product, the mere act of tearing off the shrinkwrap plastic automatically binds her to the terms of licence. In other words the purchaser gives her consent without having had the prior leisure of reading the licence terms.

56. The validity of shrinkwrap licences has been the object of judicial challenges and the early rulings on the matter refused to uphold their enforceability. A 1996 ruling by a United States Court of Appeals in the *ProCD* v. *Zeidenberg* case reversed the initial doctrinal position, and held that shrinkwrap licences were valid provided that their terms are not objectionable on grounds applicable to contracts in general[43]. To date, this decision stands as the definitive authority.

57. Clickwrap licences are similar to their offline siblings in the sense that an Internet consumer can purchase an informational service just by clicking on a button, without the knowledge of the terms of the licence. Currently, the United States is studying the possibility of amending its Uniform Commercial Code in order to enact article 2B, which, among other things would codify the validity of both shrinkwrap and clickwrap licences.

58. *ProCD* also bore other more far-reaching implications. The facts of the case are rather plain. *ProCD* had compiled onto five CD-ROMs the telephone listings contained in over 3,000 telephone directories. *ProCD* held a copyright on the software, which enabled rapid queries of the huge databases. The CD-ROMs were packaged together and were priced at roughly $150 for the general public. *ProCD* did not have a copyright respecting the listings since these did not qualify as "works". The crux of the matter concerned one of the provisions stipulated in the licence which read:

> "*You will not make the Software <u>or the Listings</u> in whole or in part available to any other user in any networked or time-shared environment, or transfer the <u>Listings</u> in whole or in part to any computer other than the computer used to access the <u>Listings</u>*"[44]. (Underlining ours)

[43] *ProCD* v. *Zeidenberg* 86 F.3d 1447 (7th Cir. 1996).
[44] *ProCD,* 908 F. Supp. at 645.

59. Clearly, *ProCD* extended its reach by requiring that users purchasing its CD-ROMs waive their rights to freely use listings, which were information in the public domain. As one author has noted "[…] *the Court had to decide whether contractual restrictions that broaden the bundle of rights granted by copyright law placed by copyright owners on the use of their information are enforceable*"[45].

60. The governing principle here is freedom of contract; two parties entering into a contract are free to bargain away certain rights in order to obtain a correlative consideration deemed valuable enough. Therefore, users contracting to gain access to copyrighted materials should be free to waive their rights guaranteed under copyright law. The question remaining to be answered is whether there exists an overriding principle of public policy justifying a curtailment of the users' freedom of contract. That overriding principle is the balance of rights struck by copyright law, which grants the copyright owner a monopoly over his or her work that is subject to certain limitations, namely the first sale and fair dealing doctrines, the fixed duration of the copyright and things falling into the public domain.

61. The judges sitting in appeal in the *ProCD* case did not see it that way and held that "*Competition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy*". Nevertheless, what the *ProCD* case illustrates is that a copyright owner – in this case the owner of a computer program – can leverage the power of his monopoly to licence the uses of information outside the strict purview of his copyright, thereby thwarting competition[46].

62. What exactly are the implications of the *ProCD* decision for online consumers of musical works? For one, the consumer will obtain licensed usage rights to musical works by simply clicking on an icon in a Web interface, unbeknownst to her that she is quite possibly renouncing certain rights owing to her under copyright law. Second, this waiver of rights will be forced on the consumer since the uniqueness of a musical work (e.g. the absence of a substitute) gives the copyright owner complete and utter control of the market for that work. To put it differently, the consumer's choices in the market are reduced to this: either accept the copyright owner's terms of licence, or altogether forego access to the work[47].

63. As the discussion above has endeavoured to show, the one-two combination or Trusted Systems and contract law dramatically shifts the balance of power in the hands of copyright owners. In Lessigian language, *code* affects law in a way that raises questions about lawmaking generally. To quote from the eminent professor once again: "*Where architecture displaces the values of the law, lawmakers will face a choice, whether to reinforce the law, or allow the change*"[48]. Before we explore how these fundamental questions have been dealt with, let us examine first how *code* may soon come to set aside certain important precepts of copyright law.

d) Effects of Trusted Systems on Copyright Law

64. Fair Dealing Doctrine. The Fair Dealing doctrine, called Fair Use in the United States, refers to a body of rules originating in jurisprudence, which create exceptions to the copyright owners' exclusive rights to use their works. In common law jurisdictions, these exceptions transcend copyright philosophy. Utilitarian in spirit, the copyright law aims to promote the greater good of the community; authors' rights must give way to higher pursuits such as public education, the furtherance of knowledge and the search for truth. While copyright law sets up the legal framework to kindle the creative drive of authors, it also implicitly recognises that users must be allowed to build on the wealth of past works. The underlying principle is that creativity naturally spurs on more creativity.

[45] ELKIN-KOREN, N., "Copyright Policy and the Limits of Freedom of Contract", 12 *Berkeley Technology Law Journal*, 111 (1997).
[46] *Ibid.*
[47] *Ibid.*
[48] See LESSIG *supra*, note 33, p. 24.

65. Central to the Fair Dealing doctrine is the balancing of private versus public interests, the weighing of authors' exclusive rights versus the public's rights to use the works. At least three reasons are commonly invoked to explain why this balancing of interests is unavoidable: 1) the economic rationale asserts that seeking to obtain permission for certain uses from the author or owner ensues onerous, even overwhelming, transaction costs which might lead the user to forego a socially beneficial use; 2) some uses are minimally detrimental to the interests of the author; 3) some uses are regarded as having overriding significance[49]. The best-known exceptions to the authors' exclusivity include the right to quote, the right to review, the right to parody.

66. It follows then that the copyright law does not tolerate that an author exerts absolute control over his work. And to hold the author in check, there must be an arbiter. What Trusted Systems in effect do is altogether remove the arbiter, and with it the guardian of some of the core values of copyright law. Nevertheless, some have argued that Trusted Systems may lead to freer access to quality works.

67. It has been asserted that "fair use" can simply be coded into the Trusted System scheme, on the assumption that a trusted machine can be programmed to allow a "reasonable number of free copies or quotations to be used." Another solution would be to grant special licences to students and professionals who generally rely on Fair Dealing for the accomplishment of their work[50].

68. For the most part, legal scholars are apprehensive about technological solutions to legal problems. Still, amidst the general scepticism, some have expressed the view that the change from a system of "fair use" to one of "fared use" should be a welcomed one. "Fair use", it is argued, should not be mistaken for "free use". "Fair use" carries invisible costs, not the least of which is the cost relating to the legal insecurity that comes with having to make the positive determination that a use falls within the doctrinal exceptions to infringement. Steering clear from the vaporous notion of what is fair, Trusted Systems provide much needed legal security. The ensuing reduction of transactional costs then benefits the public[51].

69. In the same line of thought, commentators have pointed to the disappearance of the economic rationale justifying Fair Dealing. Indeed, Fair Dealing exceptions are said to reflect a market failure because negotiation costs in order to obtain permission for every imaginable use would prove prohibitive and in the end the public would lose out. The very essence of Trusted Systems is to automate the granting of permissions to use copyrighted works, thus eliminating transaction costs. An efficient system of "fared use" might then replace the historical compromise of "fair use"[52].

70. On the whole, however, the majority view transcending the literature surveyed for this essay is that Trusted Systems pose a definite threat to the Fair Dealing exceptions. We the public, consumers of cultural and scientific works, need to be wary of an imminent future in which copyright owners can program what may or may not be used. A "Trusted" future would mean asking permission to quote, asking permission to parody, and asking permission to cut and paste in an essay like this one[53]. Fair Dealing curtails the monopoly of copyright to ensure the malleability of the works in the hands of the public. It is precisely this malleability, which must be preserved because it is conducive to a kind of "semiotic democracy", that is the ability for the public to engage and participate actively in the making of culture[54].

---

[49] RICKETSON, S., "General Aspects of Exceptions and Limitations to Copyright", *the Boundaries of Copyright : Its Proper Limitations and Exceptions*, (ALAI Study Days – 14-17 September 1998), p. 3.
[50] See STEFIK *supra*, note 37, p. 7.
[51] BELL, T., "Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine", *North Carlonina Law Review*, January 1998, p. 17.
[52] *Ibid.*
[53] LESSIG, L., "Reclaiming a Commons", Keynote address, The Berman Center's "Building a Digital Commons", May 20, 1999, Cambridge MA.
[54] See FISHER *supra*, note 11, p. 2.

71. First Sale Doctrine. The First Sale Doctrine is another exception to the principle of exclusivity of rights for the copyright owner. It limits the owner's control over the distribution of the work. The owner is granted complete control of the initial distribution of a particular copy of the work. After that initial distribution, presumably, the author will have been remunerated satisfactorily.

72. What this means is that once a person has purchased a CD, she has acquired ownership of that physical object and can therefore dispose of it at her will. She may loan it, sell it, give it away or barter it. In a commercial context, the First Sale Doctrine prevents the owner of the work to dictate the price that the retailer demands for the CD. The retailer is also free to display the CD as she wishes in her store, or not display it at all.

73. As we have hinted above in our comparison of two technologies that bring music to consumers, a Trusted System's architecture does away with the notion of First Sale. Music may simply be streamed directly to the consumer on a pay-per-listen basis, eliminating the need for setting a quantity of CDs to be released in the market in one co-ordinated sales campaign across the land. From a technical standpoint, one could argue that a copy of the work has been deposited in the consumer's hardware, and that this copy could be disposed of freely. Before jumping to the conclusion that First Sale may still have a hold in cyberspace, it should be kept in mind that the copy will have been made on a Trusted hardware device. The Trusted hardware is so labelled exactly because it blocks impermissible forwarding of a copy to a foreign computer or device.

74. What then may be lost? What value would be sacrificed to the God of automaton efficiency? Underpinning the First Sale Doctrine is the accessibility of information and the unrestrained freedom to circulate knowledge. The sharing of materials amongst the citizenry fulfils the essential function of shaping culture and building a common understanding in society.

75. Originality and copyright duration. Copyright law affords protection to works that meet the requisite level of originality. Under copyright law, mere facts are not works and therefore do not enjoy protection. This is why databases cannot be copyrighted. A trusted architecture would protect databases – information in the public domain – far better than copyright could have.

76. Copyright law grants the author of a work a monopoly over her creation for a limited time only. This reflects the fundamental bargain struck between the public and the author for the benefit of both. The author may draw revenues from the work for a time, after which the work reverts to the public domain. In a sense, the time limitation works to nourish the growing public domain, from which creators can borrow freely to create new works. In a Trusted System's architecture, copyright owners could exercise control over their works indefinitely.

e) Law in aid of *Code.*

77. Above we have discussed the ways that Trusted Systems – *code* – might impact the existing body of rules that make up the copyright law. Below we discuss how the copyright statute might be adapted to the pressing reality of Trusted Systems; assuming that the law should take into account the change.

78. Reviewing a number of national reports on the subject of copyright policy for the digital age, professor André Lucas has summarised the positions on how law should react to technical protections as being twofold: firstly, the law should at least be neutral and not hamper the deployment of Trusted Systems; secondly, the law should encourage the use of Trusted Systems by providing a proper legal framework[55].

79. The principle of neutrality states that legal roadblocks to technological protection systems ought to be removed. For Trusted Systems, this presupposes that technologies employing robust encryption may

[55] LUCAS, A., "Le droit d'auteur et protections techniques – Rapport général", *Le Droit d'auteur en cyberespace* (ALAI Study Days – 14-17 September 1998).

be freely exported. Encryption software and hardware are considered dual-use technologies – military and civil – under the Wassenaar arrangement. The signatory countries have agreed to pose stringent controls on exports of encryption products and services[56]. Loosening these controls appears inevitable if Trusted Systems are to one day pervade cyberspace.

80. Encouraging the deployment of Trusted Systems could be achieved simply by rendering them mandatory, for example by forcing hardware manufacturers to incorporate trusted capabilities into their products. Another way of achieving this would be to negate the recourses of those copyright owners who neglected to rely on Trusted Systems. But most agree that copyright owners should be free to choose the means of protection that best suit them[57].

81. There remains the question of Trusted Systems vulnerability to "hacking" or "reverse-engineering". For these eventualities the law should serve as a practical deterrent by prohibiting certain activities, the purpose of which would be to deactivate Trusted Systems. The national reports unanimously support some form of anti-circumvention measures. Illustrative of such measures are the provisions included in the Digital Millennium Copyright Act of 1998 (DMCA). Section 1201 of the Act provides:

> *a)(1) No person shall circumvent a technological protection measure that effectively controls access to a work protected under title 17.*
>
> *`(2) No person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof that—*
>
> *`(A) is primarily designed or produced for the purpose of circumventing a technological protection measure that effectively controls access to a work protected under title 17,*
>
> *`(B) has only limited commercially significant purpose or use other than to circumvent a technological protection measure that effectively controls access to a work protected under title 17, or*
>
> *`(C) is marketed by that person or another acting in concert with that person for use in circumventing a technological protection measure that effectively controls access to a work protected under title 17*[58].

82. Lucas notes that there are two possible approaches to anti-circumvention: those who justify legislative action on the necessity of protecting copyright's entitlements, and those who hold that the law ought to reinforce Trusted Systems irrespective of copyright considerations[59].

83. Under the first approach, an act of circumvention will have been committed only where an attempt to violate the copyright law can be demonstrated. This approach recognises the interests of users who may legitimately assert a Fair Dealing claim or wish to access works in the public domain. Circumvention acts for these intended purposes pose no threat to exclusive copyright entitlements. Accordingly, the law has no interest in punishing them. The counter assertion is that a legitimate claim to a use does not negate the freedom of service providers to employ whatever means available, including Trusted Systems, to deliver informational goods in a secure environment. In the same way, the fact that a work is no longer copyrighted does not entitle users to demand that service providers hand over the keys to the lock[60].

84. The second approach presumes that prohibiting all acts of circumvention has more teeth and is simpler to administer. On the facts of any given case, sanctions could be made distinguishable

---

[56] The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, <http://www.wassenaar.org/>.
[57] See LUCAS *supra*, note 54, p. 8.
[58] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).
[59] *Ibid.*, p. 9.
[60] *Ibid.*, p. 10.

depending on whether a copyright violation was intended or not. Attention would properly focus on the effects without weakening the whole anti-circumvention edifice.

85. Lately the anti-circumvention provisions have come under heavy fire from critics. Predicting a "continuing technological struggle between content providers, their customers, their competitors and future creators", Professor Boyle describes the deployment of Trusted Systems as the erecting of technological "fences". He writes:

> "*The technical means to do this can be thought of digital fences. Sometimes those fences will be used to stop clear violations of existing rights. Sometimes they will be used to enclose the commons or the public domain. Thus by making it illegal or impractical for me to go around through or over the fence, the state adds its imprimatur to an act of digital enclosure. The Internet trinity tells us that information wants to be free and that the thick fingers of Leviathan are too clumsy to hold it back. The position is less clear if that information is guarded by digital fences which themselves are backed by a state power maintained through private systems of surveillance and control*".[61]

86. Commenting on the DMCA's anti-circumvention provisions, Professor Samuelson notes that the statute pays no heed to many important and legitimate reasons to permit lawful circumvention acts. Of particular concern, is the fact that the statute lacks a provision enabling courts to exempt acts of circumvention engaged in for legitimate purposes. While the statute does permit circumvention acts in some limited instances, unwittingly giving unprecedented standing to hackers, it defuses legitimate circumvention exceptions by outlawing devices that do just that[62]. One step forward, one step backward.

87. Generally, the anti-circumvention provisions raise concerns of the law's over-inclusiveness. As it was shown above, Trusted Systems have the potential of overreaching the strict letter of copyright law in many ways. The law's concern with protecting the Trusted Systems, through airtight anti-circumvention measures, has led professor Lessig to conclude correctly that "[…] The law protects the *code,* then, more than the law protects the underlying copyrighted material". He thus goes on to conclude that the law protects "[…] schemes whose ultimate effect may well be to displace the balance that copyright law strikes."[63]

f) Efficacy of Copyright in the Year 2015

88. Earlier in this essay, much musing was spent on trying to measure the efficacy of copyright law in the context of the wild, regulation-resistant Internet. That was the Internet of old. But this is the Year 2015 and things have changed. Like the telephone and the television before it, the Internet has become pervasive in most developed countries. So too have Trusted Systems. The CD has succumbed to the same fate as its physical predecessors. Most music is experienced via the Internet. Those children born at the turn of the millennium, now teenagers, have never known what it is to purchase an album at a record store.

89. The future is now and the future is "pay-per-hear". Interestingly, back in the glory days of the now defunct MP3 format, some had foreseen the coming of the "pay-per-hear" era. Some came frighteningly close in their prediction. In his timeless piece, Jonathan Zittrain offered this half comical half disturbing vision of music distribution online:

> "*Songs are not "sold" in even the colloquial sense of the word; rather, they are "licensed"—both from a legal and technical standpoint. Compact discs have joined 8-tracks,*

[61] BOYLE, J., "Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors", 1997, p. 15, available at <www.wcl.american.edu/pub/faculty/boyle/foucault.htm>.
[62] SAMUELSON, P., "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised", 14 *Berkeley Tech. L.J.*, 519, Spring 1999.
[63] See LESSIG *supra*, note 33, p. 37.

cassettes, and phonograph records in the dustbin; their replacements are small, generic "jukeboxes" linked by the Net to a central repository of songs managed by a publisher.

An individual authenticates herself to a jukebox—perhaps with a fingerprint or carefully scrawled signature on its back with a stylus—and then may access specific songs that fall under her monthly payment plan. She will be granted access to the music archive only after parting with personal information about herself, including name, age, address, and phone number.

As she selects songs, her tastes are noted, allowing offers for "special" songs not included in her monthly plan to be specifically targeted to her tastes and sent to her across all media. The songs she asks for are "streamed" to her player as she listens, and do not remain there any more than a song stays inside a radio after it is over.

An inaudible signal is embedded in the music; if she holds a microphone to her headphones and thereby makes an imperfect, analog copy to an old-fashioned cassette, her name and a unique identifier will be "in" it, permitting prosecution for copyright infringement if the copy is found. Her user license agreement provides an alternative path for the music owner to pursue fast-track damages, including the sending of a signal to her jukebox that permanently disables anyone from using it until the matter is settled.

In the unlikely event that she were to abuse her access to the system by hooking up her jukebox to an amplifier and playing the music at a backyard party outside her California apartment, a cheap listening post on the beach's lifeguard chair could be monitored by ASCAP, which would use a watermark decoder to know instantly that she was behind the cacophony—and that the particular performance had only been paid for at the "portable personal use" rate rather than the "noncommercial party" rate.

A more likely event is that she will fall behind in her monthly payments, in which case her access to any music—except that which is heard over old-fashioned analog "public" radios—will be cut off automatically. (This may soon happen; her monthly rate just doubled since her graduation from college and corresponding loss of student discount status.)"[64].

90. Copyright law is still law in the books, although the sections of it which find application nowadays are mainly those concerned with searches and seizures, arrests, conduct of trial, and sentencing of circumvention felonies. Copyright lawyers describe their practice as "*your basic hacker, cracker, cipher cases; lots of subscriber identity theft, pirateware… you now, kids stuff*".

91. The recording industry is content. With cheap access to music anywhere anytime, the public is content also. To call into question copyright law's efficacy would seem odd. Let us indulge in the oddity. Recall the failures of law: failure of communication, failure to enlist supportive action, failure of enforcement, failure to forestall avoidance, failure of obligation.

92. Failure of communication. Yes. Technology can be intensely behavioural, perhaps more so than law. Contrary to the owner of a CD, who instinctively knew that she could listen to it ten times or a thousand times, play it at a party with many guests attending, loan it, sell it, exchange it, excerpt from it, the present day music lover can hardly fathom such privileges. Nowadays you simply verbalise a command to your hand-held device and a song immediately pours out, while your virtual wallet is automatically debited one electronic token. Of course there are ways to access pieces of music without charge. For instance, high school and college students can purchase "educational series" listening devices, which are registered to the student. Say a student is rehearsing a Céline Dion song for a school recital. She could freely access the song from the service provider by entering her unique digital signature into the device and arrange for her music teacher to do the same. Once the two signatures are entered, the encrypted song is unscrambled and can be listened to only on the device. Such privileges are generally understood to be administered by the school and can be cancelled for a variety of reasons, including suspicions by the service providers of "privilege abuse".

[64] ZITTRAIN, J., "What the Publisher can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication", February 24, 2000, Harvard Law School, Public Law and Legal Theory Working Paper Series, Working Paper No. 007, revised version forthcoming in *Stanford Law Review*, Vol. 52, p. 18.

93. Failure to enlist supportive action. Yes. Unaware that the copyright law entitles them to "fair dealing" uses of copyrighted materials, few persons have ever made any sort of claim based on this arcane section of the copyright law (copyright is widely perceived as a special kind of criminal statute and the idea that users could assert a claim under this law eludes most mortals). The few that have saw their actions dismissed on grounds that they had waived whatever rights they might have had when agreeing to the licence terms. Seeking an injunctive remedy to force a provider to "give away" music, even for limited purposes, rests on thin legal bases if any. Exorbitant legal fees are frequently mentioned as the main prohibitive factor. Anyway, the vast majority of copyright practitioners are either corporate cadres of the recording industry or criminalists who do not wish to stake their reputations arguing lame duck cases.

94. Failure of enforcement. No. Watermarks have proven extremely effective at locating pirated copies and the sources of those copies. "Spider" software has improved immeasurably, crawling the web in search of bootleg copies at great speed. Once an illegal copy is found on the hard disc of a computer, or in rented memory space in the Web mainframe, the spider issues a virtual indictment to which is attached a search and seizure warrant for the computer, paralysing the functionality of the machine and thereby rendering it useless. The accused may plead guilty by clicking on an icon of a gavel, after which her virtual wallet is debited one hundred tokens for a first time offence. The fine paid, she can regain the use of her computer.

95. Failure to forestall avoidance. No. Back when the framers wrote the copyright law for the next millennium, they proved to have had keen foresight. They included what were then called "anti-circumvention" provisions, which outlawed any attempt to deactivate technical protections of copyrighted materials, including the mere fact of writing software or manufacturing devices with such capabilities. These provisions, and the ensuing amendments to them, are now collectively better known as the "Zero Tolerance Clause".

96. Failure of obligation. Yes. The recording industry has made two historically important vows: to bring quality recordings of music and sound to the public at the lowest cost feasible, and to champion the cause of protecting the works of needy and deserving artists "associated" to it. Acquiring the copyrights to the works is done only because it is a legal prerequisite to obtaining the standing to put all the industry's financial and political clout behind the war on pirates. The recording industry is the force that guarantees the incentives to create music and preserve a rich cultural tradition.

97. The recording industry's actions speak louder than its words. Made up of exemplary corporate citizens, collectively it pays billions of dollars in taxes per year, employs hundreds of thousands, and gives generously to various charities. The recording industry has cleaned up its act and ended the practice of resorting to child labour in developing countries. It also funds important research such as the "Universal Audience Project" which has brought music enjoyment to millions of hearing impaired individuals through the advancement of neurological chip implant technology.

98. The recording industry believes in the rule of law and the sanctity of one's property. **It is not in the business of massively subsidising schools, universities and libraries through the application of economically unjustified legal doctrines such as "Fair Dealing"**. Indeed, undue meddling in the normal functioning of markets brought on by heavy-handed government regulation can only lead to market distortions and inefficiencies.

Part III – The *Commonist* Revolt

a) Lessons from the Microsoft case

99. The dust has not yet settled in the Microsoft trial. The remedial order has not been handed down, but a break-up of the largest software company in the World is entirely within the realm of possibility. Whatever the outcome, this case deserves close scrutiny from lawyers and legal scholars across the board. To characterize it only as a case about unfair competition would be downplaying its pedagogical significance. For the Microsoft case is as much a case about copyright as it is a case about competition. It raises important questions about property and power, about copyright and money, and about monopolies and markets. More generally it teaches us lessons about the information economy, and network effects, and who has the ability to control. Control. That's the gist of it.

100. Bill Gates had already enjoyed adequate remuneration for his copyright of DOS when he and the other MS strategists came up with the idea of bundling the Windows 95 operating system with Internet Explorer (IE), and force PC manufacturers, through compulsory licences, to preinstall both on every computer that rolled out of the shop. The same held true when they decided to tie IE to Windows 95/98 and make it difficult to deactivate IE without compromising the functionality of the operating system. The real question is not why they did it, but why would they have not done these things. What compelling argument of copyright law might have caused them to stop and think before they went and choked competitors in the OS and browser markets? There is none. The copyright law does not say that you must use your copyright only to further the good of human kind. Nor does it say that you should make a killing in the market. These determinations are left to the copyright owner.

101. The idea that copyright could somehow cause damage seems ludicrous to most, just in the same way that property is generally thought of as a good thing. And truth be told, copyright and property are good things. In theory property is neutral. But just as landlords of the past could tyrannise tenants, so can copyright owners exploit authors and consumers. Landowners were once free to mine, excavate, deforest, spill waste, and wreck the environment. Copyright owners are now free to enclose their property, milk the consumer market, suppress criticism, bar access to information, stifle innovation and wreck the public domain.

102. The point about the Microsoft case generally, and the point about Trusted Systems specifically, is one of private, proprietary, regulation. This essay has endeavoured to show that the Internet's design, once neutral, is rapidly changing to one of control, where corporate titans can dictate the behaviour of the masses by coding default settings in software. We have said previously that *code* is intensely behavioural. Consider the rule embedded in Windows 95/98/IE: attempt to disinstall IE to put in Netscape Navigator, and suffer the dire consequences of a buggy operating system. In a sense, Microsoft has set up the mother of all Trusted Systems; a system that secretly favours pure Microsoft *code,* or paid-for-approval-by-Microsoft *code.*

103. So the Microsoft lessons become clear and warrant positive actions. Government will step forward and assume its role of guardian of the public interest. It will strengthen defaults in the copyright law to humble copyright owners and re-establish the balance that is the very essence of the law. No. Prevailing policy rhetoric says that markets are best left alone to police anti-social behaviours. The *laissez-faire* approach counts many supporters, as does the wait-and-see attitude. The Internet is still in infancy, unpredictable, evolving. Its promise is too great to risk debilitating it with bad laws. This view is terribly skewed says Professor Boyle. He writes:

> "*In the information economy, where power is likely to be measured in intellectual property rights, the idea that the state is not somehow making choices and picking winners seems particularly obtuse. Neo-liberals should try applying the same scepticism to the process of granting and defining the state-conferred monopolies called intellectual property rights that*

they do to the state-conferred regulatory monopolies that affect certain kinds of banking business or the electromagnetic spectrum."[65]

104. Proprietary regulation differs quite substantially from the public brand of regulation. Regulation-making of the public kind obeys to strict principles, namely democratic representation, public scrutiny, accountability, and judicial review. Checks and balances in the system that reflect the duties that come with state-backed authority. The same checks and balances exist in the corporate edifice also, but mainly to protect stockholders. However, there are ways to circumvent the checks and balances imposed in the private sector. There are ways to band secretly and determine the future of online distribution of music.

105. The Secure Digital Music Initiative (*SDMI*) is "a forum that brings together the world-wide recording, consumer electronics and information technology industries to develop open technology specifications for protected digital music distribution"[66]. Its membership is "open to technology-based commercial companies that have significant direct activity in, or affecting, digital music security" and comes with a $10,000 admission fee[67]. Reading the *SDMI* mission statement, one encounters much talk about the concern for protecting the artists' rights. Paradoxically, artists do not fit the membership description and, in all likelihood, are not at the table. The Electronic Frontier Foundation (EFF) was reportedly denied participation in the ultra secretive meetings. In effect, *SDMI* seeks to round up the Tsars of the related music, electronics and IT industries to lay down the format, another word to mean *code*, to eradicate digital copying of musical works, and Fair Dealing rights for good measure. *SDMI code*, pure gobbledegook to whoever lacks an engineering degree and extensive training in the science of audio compression, would not only inhabit the Internet but also permeate offline audio devices. If widely adopted, it could alter the rights of music consumers in the coming years. Nevertheless, the public needn't be represented in the decision-making process.

106. Worse, governments are lending a hand to this form of privatization of legislation. In their rush to establish favourable conditions for the continued growth of electronic commerce and growth of the IT industry, governments are pushing forward the IP 'Maximalist Agenda"[68].

b) The Intellectual Property Land Grab

107. In her landmark paper *The Copyright Grab*, Professor Samuelson exposes the Clinton Administration's copyright policy as a handover to the publishing, cinema and music industries in exchange for financial backing in its re-election bid. She describes the eight point plan to please the Hollywood lobby: 1) give copyright owners control over every use of copyrighted works; 2) give copyright owners control over every transmission of works in digital form; 3) eliminate fair-use rights whenever a use might be licensed; 4) deprive the public of the "first sale" rights it has long enjoyed in the print World; 5) attach copyright information to digital copies of a work (watermarking); 6) protect every digital copy of every work technologically (Trusted Systems) and make illegal any attempt to circumvent that protection; 7) force online service providers to become copyright police, charged with implementing pay-per-use rules; 8) teach the new copyright rules of the road to children throughout their years at school[69].

108. Behind the accusatory language of the text, there lies a distinctly noticeable cry of distress; a motherly cry for help in saving the fast eroding sphere of the public domain. Apparently the brilliance of the flare was spent in vain and died unnoticed in the darkness of the night. The maximalist agenda continued unfettered, seeking to gain protection for databases and spilling into the law of patents. The

---

[65] BOYLE, J., "Missing the point on Microsoft", *salon-technology*, April 7, 2000, <www.salon.com/tech/feature/2000/04/07/greenspan/print.html>.
[66] Secure Digital Music Initiative, "SDMI FAQ", available at <http://www.sdmi.org/public_doc/SDMI99070809-SDMI_FAQ.pdf>.
[67] OAKES, C., "Pundits Ask: Who Owns Music?", *wirednews*, February 26, 2000.
[68] SAMUELSON, P., "The Copyright Grab", *wired*, No. 4.01, January 1996, p. 2.
[69] *Ibid.*, p. 2.

Amazon.com "one-click" patent has angered many e-commerce interests and received much media attention. The glaring absurdity of patenting Internet business methods perhaps has had the effect of discomforting the layperson with the idea of patents. Also, the fury over the issue of HMOs has put the patentability of life forms to the forefront of public opinion. The more disturbing implications of the maximalist agenda just might strike a sensitive chord in the collective psyche.

109. The maximalist agenda rests on two questionable premises: one, that the digitisation of information permits infringement activities on a wide scale and therefore threatens the livelihood of creators; two, that expanding IP rights to cover *sui generis* subject matters is needed to encourage further investment in the global information infrastructure[70]. The maximalist agenda aims to expand IP protection in a myriad ways and, as we have discussed quite sufficient in this essay, permit information proprietors to padlock their assets for safekeeping. It follows then that the maximalist agenda accepts that legal doctrines such as Fair Dealing and First Sale may succumb, unfortunate casualties in the aftermath of the Tech Wars.

c) *Commonists,* not Communists!

110. Throughout this essay, we have sought to impress upon the reader a feeling of urgency. Something really is at stake. A common front needs to be formed to halt the maximalist progression. Authoritative voices must rise above the new economy rhetorical hype and bring guidance to the unsteady information society. For what is at stake is more than the Fair Dealing rights of the public. What merits battling for is the idea of a *commons.*

111. The *commons* can be explained by its relation to property. Neither private nor state property, the *commons* represents a balance to private property[71]. The *commons* can be loosely defined as that which is there for all to enjoy and respect. It embodies the freedoms of access and of use. Its spirit is sharing and disinterested contribution. Professor Lessig gives numerous examples of what is *commons.* Listing just a few gives a better picture: a public park, streets, a mathematics theorem, HTML source code, open source software, the Internet. *Napster* is a commons.

112. Lessig, an avowed prophet of doom, nevertheless makes the important point of the tragedy of the *commons:*

> "*The problem with the commons is that there is no incentive for individuals to use it properly. Create a commons, and people will overgraze it. The commons cannot sustain itself; it, like a tragedy, is destined to die some horrible death.*"

113. Intellectual property has a *commons.* It is called public domain and it too faces a horrible death. It may face a horrible death. A trusted architecture for the Internet, we have argued, would spell the end of the public domain. To explain how this slow death might one day come, professor Boyle offers the parallel, the metaphor we could say, of the environment and how it to fell victim to rape by proprietary interests. He argues convincingly that, in the case of the environment, structural reasons led to its mistreatment and neglect. A market based conceptual framework, which presupposes a legal system centred around private property, is flawed in that:

> "*Markets would routinely fail to make activities internalize their own costs, particularly their own environmental costs. This failure would, routinely, disrupt or destroy fragile ecological systems, with unpredictable, ugly, dangerous and possible irreparable consequences*."

[70] BOYLE, J., "A Politics of Intellectual Property: Environmentalism For the Net?", p. 11, available at <www.wcl.american.edu/pub/faculty/boyle/intprop.html>.
[71] LESSIG, L., "Code and the Commons", Keynote, given at the conference on *Media Convergence*, Fordham Law School, New York, NY, February 9, 1999.

114. Similarly, market driven arguments for intellectual property will routinely fail to internalize the costs to the public domain and to the equilibrium of the information ecology. Boyle concludes that we are in need of "*popularizable analytical tools*" to build political momentum around the public domain[72].

115. The *commons* is one such tool. And, for the legally minded, perhaps another proper tool could be what Lessig calls "Cyberspace's Constitution". Lessig posits that the Internet has an unwritten Constitution comprising a "set of norms, or understandings, latent within a political culture. These norms "*were constituted by practices, and by a history, that formed the ordinary ways of a people.*"[73] This constitution was present in the minds of the original framers of the Internet and in the *code* they originally wrote. Uncovering its precepts means to go back in time and study the Internet's original design. *Code*, despite the obvious menacing connotation, can be liberating and indeed once was. In the beginning, the *code* protected privacy, freedom of speech and free access to works. Today, talking about privacy in cyberspace seems oxymoronic. Content filtering is commonplace. Trusted Systems lurk in the distance.

116. The *Commonists* hold the belief that the Constitution of Cyberspace protects the *commons.* Regulators, whether the state or private *code* writers, must abide by the precepts of this Constitution if there is to be any flourishing intellectual *commons* in cyberspace. Trusted Systems, including the *SDMI* protocol, edict rules that conflict with the *commons*. They most likely are *ultra vires* of the Internet's spiritual Constitution.

[72] See BOYLE *supra,* note 68, p. 12.
[73] LESSIG, L., "Cyberspace's Constitution", Lecture given at the American Academy, Berlin, Germany, February 10, 2000.

Conclusion

117. The MP3 revolution has challenged some intrinsic notions of copyright law. At first glance, the World seems divided between copyright abolitionists and copyright maximalists. Abolitionists claim that the Internet has ushered in a new era of “containerless” information, which has unveiled the artificialness of laws that create property interests in information. “Information wants to be free” goes the saying. The maximalist lobby seeks to widen the ambit of intellectual property, then lock-up what can be captured with technological means – Trusted Systems. The maximalists have skilfully steered the public debate on intellectual property by defining the issues as mere infringement concerns. In fact, there are much greater things at stake.

118. Trusted Systems deployed pervasively would transform the space in cyberspace. Control would become the default setting. Proprietary regulation, programmed into the Trusted Systems, would erase the historical checks and balances of the copyright monopoly, and further erode the public domain. The intellectual property *commons* would die a horrible death.

119. However, a third voice has risen. That of the *Commonists*. They warn of what could be lost and propose the conceptual tools with which to mount a political battle to preserve the public domain. They correctly affirm that the maximalists’ views conflict fundamentally with the framers of the copyright law, and even with the original values of the Internet. They ask the deeper question of whether the *commons* could represent the economic model for the information society.

Bibliography

BARLOW, J.P. “The Economy of Ideas”, *Wired*, 2.03, Mars 1994, <www.wired.com/wired/archive/2.03/economy.ideas_pr.html>.

BELL, T., “Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine”, *North Carlonina Law Review*, January, 1998.

BOYLE, J., “Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors”, 1997, available at <www.wcl.american.edu/pub/faculty/boyle/foucault.htm>.

BOYLE, J., “Missing the point on Microsoft”, *salon-technology*, April 7, 2000, available at <www.salon.com/tech/feature/2000/04/07/greenspan/print.html>.

BOYLE, J. “A Politics of Intellectual Property: Environmentalism For the Net?”, available at <www.wcl.american.edu/pub/faculty/boyle/intprop.html>.

CHICOLA et al., “Digital Rights Architectures for Intellectual Property Protection: Legal/Technical Architectures of Cyberspace”, available at <http://cyber.law.harvard.edu/ltac98/trustsys.html#_Toc437906319>.

DYSON, E., “Intellectual Value”, *Wired*, 3.07, July 1995.

ELKIN-KOREN, N., “Copyright Policy and the Limits of Freedom of Contract” 12 *Berkeley Technology Law Journal*, 111, 1997.

FISHER, W., “Digital Music : Problems and Possibilities”, March 19, 2000, available at <www.law.harvard.edu/Academic_Affairs/coursepages/tfisher/Music.html>.

FISHER, T., “Property and Contract on the Internet”, Draft Paper of June 10, 1998.

GOLDSTEIN, P., “Copyright and its Substitutes” *Wisconsin L. Rev*., 865, 1997.

GOMULKIEWICZ, R., “The License Is The Product : Comments on the Promise of Article 2B for Software and Information Licensing”, 13 *Berkeley Technology Law Journal*, 981, 1998, available at <http://eon.law.harvard.edu/h2o/property/alternatives/reading1.html>.

JOHNSON-LAIRD, A., “The Anatomy of the Internet Meets the Body of the Law”, 22 *U. Dayton L. Rev.*, 465, printemps 1997.

JOHNSON, D. & POST, D., “Law and Borders – The Rise of Law in Cyberspace”, 48 *Stanford Law Review*, 1367, 1996, available at <http://www.cli.org/X0025_LBFIN.html#4>. Copyright Law.

JONES, H. W. “The Efficacy of Law”, 1968 *Rosenthal Lectures*, Evanston, Illinois, Northwestern University Press, p. 14.

LESSIG, L., “The Law of the Horse : What Cyberlaw Might Teach”, *Harvard Law Review*, fall 1999.

LESSIG, L., “Reclaiming a Commons”, Keynote address, The Berkman Center’s “Building a Digital Commons”, May 20, 1999, Cambridge MA.

LESSIG, L., “Code and the Commons”, Keynote, given at the conference on Media Convergence, Fordham Law School, New York, NY, February 9, 1999.

LESSIG, L., “Cyberspace’s Constitution”, Lecture given at the American Academy, Berlin, Germany, February 10, 2000.

LUCAS, A., “Le droit d’auteur et protections techniques – Rapport général”, *Le Droit d’auteur en cyberespace* (ALAI Study Days – 14-17 September 1998).

MANN, C., “Who Will Own Your Next Good Idea?”, *The Atlantic Monthly*, September 1998, <www.theatlantic.com/issues/98/copy.html>.

PERENS, B "The Open Source Definition" in Chris DiBona, Sam Ockman and Mark Stone (eds), *Open Sources: Voices From the Open Source Revolution*, Sebastopol (CA): O'Reilly and Associates, Inc., 1999.

POST, D. “Plugging In – New Wine, Old Bottles : The Evanescent Copy”, *The American Lawyer*, Vol. XVII, No. 4, available at <http://eon.law.harvard.edu/h2o/property/alternatives/post.html>.

RICKETSON, S., “General Aspects of Exceptions and Limitations to Copyright”, in *The Boundaries of Copyright : Its Proper Limitations and Exceptions*, (ALAI Study Days – 14-17 September 1998)

SAMUELSON, P., “Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised”, 14 *Berkeley Tech. L.J.*, 519, Spring 1999.

SCHLACHTER, E. “The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet” 12 *Berkeley Tech. L.J.*, 1997, available at <http://www.law.berkeley.edu/journals/btlj/articles/12_1/Schlachter/html/reader.html>.

STEFIK, M., “Trusted Systems”, *Scientific American*, March 1997.

STEFIK, M., “Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge us to Rethink Digital Publishing”, 12 *Berkeley Tech. L.J.*, 137, 1997.

ZITTRAIN, J., “What the Publisher can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication”, February 24, 2000, Harvard Law School, Public Law and Legal Theory Working Paper Series, Working Paper No. 007, revised version forthcoming in *Stanford Law Review*, Vol. 52.

Audio Home Recording Act of 1992, 17 U.S.C. §§1001-1010.

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

ProCD v. *Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

ProCD, 908 F. Supp. at 645.

The Shetland Times v. *Wills*, Court of Sessions, Edinburgh, October 24, 1996, available at <www.shetlandnews.co.uk/opinion.html>.

Sony Corp. v. *Universal Studios, Inc.*, 464 U.S. 417 (1984).

Recording Industry Ass'n of America v. *Diamond Multimedia Systems, Inc.*, U.S. 9th Circuit Court of Appeals, docket number 9856727, June 15, 1999.