Info, Comm & Ethics in Society (2004) 2: 1–

The Implications of Digital Rights Management for Privacy and Freedom of Expression

Ian Kerr and Jane Bailey

Faculty of Law, University of Ottawa, Ontario, Canada
Email: {iankerr,jbailey}@uottawa.ca

ABSTRACT

This paper aims to examine some of the broader social consequences of enabling digital rights management. The authors suggest that the current, mainstream orientation of digital rights management systems could have the effect of shifting certain public powers into the invisible hands of private control. Focusing on two central features of digital rights management – their surveillance function and their ability to unbundle copyrights into discrete and custom-made products – the authors conclude that a promulgation of the current use of digital rights management has the potential to seriously undermine our fundamental public commitments to personal privacy and freedom of expression.

"The best agencies for improving the masses of the people," Andrew Carnegie once said, are those that "give nothing for nothing" (Rub, 1985). Carnegie had tremendous and unrelenting faith in public institutions such as the library. So much so that he redirected substantial wealth from the private sector in support of such institutions. His belief in them was premised on his view that:

> They only help those who help themselves. They never pauperize. They reach the aspiring and open to these chief treasures of the world – those stored up in books. A taste for reading drives out lower tastes. (Rub, 1985)

Sadly, it is becoming increasingly difficult for our public institutions to live up to Carnegie's vision. Not because of slashed budgets to our library systems, to the arts and humanities. Not because of diminishing literary standards. Not even because of a diminished taste for reading in correspondence to the advent of television, movies, computers and digital media. Rather, one of the most significant challenges faced by our libraries and other public institutions these days stems from a particular vision held by many powerful private institutions about how to maintain corporate control over the economics of intellectual property. Our public institutions are being threatened by *new forms of social control* through which private institutions such as our cultural industries now "reach the aspiring."

These new forms of social control – known now as digital rights management[1] – are said to be a necessary response to the network environment and its many opportunities for the rapid and inexpensive dissemination of digital content.[2] Concerned that the digital milieu will enable consumers

KEYWORDS

Digital Rights Management

Privacy

Freedom of Expression

to undermine the economics of intellectual property, the strategic basis of digital rights management is to leverage encryption technologies as a powerful, automated alternative to the traditional, cumbersome and somewhat ineffectual protection offered by copyright law. As Barlow so poetically captured the model during its early stages of development, it commences with the proposal "that all new intellectual creations will be put in cryptographic bottles" and concludes with the transformation of "a market where wine is sold in bottles from which everyone may drink infinitely – as is the case with books – into a market where all wine is sold by the sip. Forever."[3]

Poetry aside, it is clear that our publishing industries seem more and more to prefer safeguarding digital content through technological protection measures rather than social or legal norms. In many jurisdictions, they have successfully lobbied for additional legal measures to protect these digital rights management systems.[4] Among other things, such legislation creates new rights for those who employ such technologies against those who attempt to circumvent them (Kerr *et al.* (2002).

This paper aims to examine some of the broader social consequences of enabling digital rights management. In it we suggest that the current, mainstream orientation of digital rights management systems could have the effect of shifting certain public powers into the invisible hands of private control. Our paper begins with a basic description of digital rights management systems, the motives typically associated with their creation and a brief account of the means by which they achieve their objectives. Focusing on two central features – their surveillance function and their ability to unbundle copyrights into discrete and custom-made products – we conclude that a promulgation of the current use of digital rights management has the potential to seriously undermine our fundamental public commitments to personal privacy and freedom of expression.

1. DIGITAL RIGHTS MANAGEMENT SYSTEMS

Digital rights management systems operate as 'electronic fences',[5] which can be used to control a digital work. Two well-known technologies used to carry out this function are passwords and cryptography.[6] Both of these allow copyright owners to exclude others from obtaining unauthorized access to digital materials subject to copyright. Cryptographic techniques also allow copyright owners to control subsequent uses of digitized works. Some of the forms of control that they provide are novel. For example, up until recently, when a person bought a paperback, the copyright owner had no means of controlling whether she would copy portions of it or lend it to another person. Today's digital rights management systems allow a copyright owner to control these things in the case of e-books and other digital versions of the published work.[7]

Why would copyright owners wish to assert these new forms of control?

Although there is never a single answer to such questions, the usual rejoinder offered by mainstream proponents of digital rights management is that these new forms of control are a measured response to the cultures and communities that have developed alongside network technologies. Despite a decade of co-existence, the norms of cyberspace still do not correspond to those in real space. Although many people would never steal CDs or DVDs from their local record shop, millions of them use Kazaa and other peer to peer applications to the same effect.[8] According to the current mainstream proponents of digital rights management, an unimpeded ability to duplicate and distribute digital content *en masse* through file-sharing applications could undermine the very existence of our entertainment industries.[9] Digital rights management, they argue, is necessary to combat the "free beer" mentality of those who cloak their desire to get stuff for free under the guise of a principled response to a business model that is said to force them to buy an entire album when all they really want is a song or two.

The free rider problem said to accompany the "free beer" mentality is perhaps the most popular public conception of what is at stake in the digital rights management debate. Without question, an unimpeded ability of teens and twenty-somethings to thwart traditional copyright rules *en masse* raises an important set of issues for intel-

lectual property lawyers.[10] But it is crucial to recognize that there are other important issues at stake in this debate besides the economics of intellectual property and its financial implications for the music and movie industries. To better comprehend the broader motives for asserting these new forms of control and what else is at stake requires a slightly more robust understanding of digital rights management systems and their possible applications.

Typically, a digital rights management system consists of two components (Gervais, 1990). The first component is a database containing information which, among other things, utilizes various authentication technologies to identify: (i) the contents of a particular work subject to copyright; (ii) the various rights holders associated with the work; (iii) the individual consumers who seek to access or use a work; and (iv) the consumers' computers and associated software. The second component is a licensing arrangement, which establishes the terms of use for the associated work by way of contract (Hugenholtz, 2000).

The database component enables the automated collection and exchange of various kinds of information among rights owners and distributors about particular users, their habits, and their particular uses of the digital material subject to copyright. The information that is collected and then stored in these databases can be employed in a number of different ways. As already mentioned, it can be employed to promote the authorized use of an e-book by restricting access only to those who have paid to use the work, or by restricting their ability to subsequently distribute it to others who have not. Other related applications of the database usage information include the ability to identify the user's machine in order to prevent use of the material on other machines or to restrict the total number of times that the work can be accessed by that machine.

The surveillance features associated with the database component of the system are crucial to the technological enforcement of the licensing component. It is through the collection and storage of usage information that digital rights management systems are able to "authorize use" in accordance with the terms of the licensing agreement and thereby "manage" copyrights (Cunard, 2001). Without the surveillance features of the database component, all that remains is a souped-up standard form contract. Together, the database and the license allow owners of digital content to unbundle their copyrights into discrete and custom-made products.

Although there is a growing literature explicating the various technologies that underlie digital rights management and what they expect to achieve,[11] it is unnecessary to go into further detail here. The extremely rudimentary aspects of digital rights management presented above are sufficient to uncover two extremely important sets of issues that have received surprisingly little consideration in comparison to the vast attention that has been paid to the legal questions concerning the circumvention of technological protection measures and the rhetoric associated with the free beer, free rider characterization of what is at stake. The first set of issues concerns the surveillance aspect of the database component of such systems and its impact on personal privacy. The second set of issues concerns the ability to unbundle copyrights in a manner that excludes various forms of public access to a digital work, and the ultimate effect that this may have on freedom of expression.

2. PERSONAL PRIVACY

Although relatively scant academic attention has been devoted to the subject thus far,[12] it is no exaggeration to say that one of the central features of digital rights management is its ability to monitor and meter its customers' use of its products. Digital rights management systems allow an unprecedented degree of surveillance of consumers' reading, listening, viewing and browsing habits. While we refer to them as "rights management" systems, what these databases *really* manage is information – information about users, which can be gathered 24/7 by way of automated, often surreptitious surveillance technologies that are an integral part of many digital rights management databases. The information that these systems track, collect and then store is subsequently used to enforce rights either by technological or legal means. Perhaps a more appropriate label for some DRMs would be *digital rights monitoring systems*.

As mentioned in the preceding section, the surveillance features associated with the database component of DRMs are crucial to the technological enforcement of various aspects of a given license. Some kinds of surveillance are necessary not only to authorize access to a work and to authenticate the identity of legitimate users but also to clear rights, to enable the payment of royalties for uses or public performances of works, or to facilitate the pursuit of unauthorized users for the purposes of a lawsuit (Barlas and Isherwood, 2002).

If – as many are predicting – DRMs become a primary means of enforcing copyright, it is not difficult to see that privacy protection becomes an increasingly significant consideration. One of the questions which we will be forced to grapple with is: what limits ought we to place on the surveillance operations of a DRM? This, in turn, will require further consideration about what counts, or ought to count, as privacy invasion in the age of networked digital technologies (see Cohen, 2003).

monitoring systems are becoming our more constant companions, wherever we go

There is a growing consensus that the digital age compels us to confront possibilities that transcend privacy's traditional "right to be let alone" (Brandeis and Warren, 1890). More and more, scholars and jurists are coming to grips with the consequences of a broader concept of "informational privacy." Some courts, for example, have recognized that

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected (*R. v. Dyment*, 1988: 2 S.C.R. 417, 429–430).

Although the above remarks were contemplated in the context of search and seizure law, the threat to informational privacy is by no means restricted to police or other public sector surveillance techniques. DRMs and other technologies adopted by the private sector further displace the adage that one's home is one's castle. The moats are long gone. And it is no longer sufficient to draw the blinds. Like other internet applications, digital rights monitoring systems enable surreptitious surveillance within what was once the seclusion of our homes. With an increasing reliance on automation and wireless technologies, these monitoring systems are becoming our more constant companions, wherever we go.

Although many moral philosophers and legal scholars are in the process of trying to better understand the implications of privacy in a digital age,[13] it is important to recognize that these are not *merely* issues of ethics or law. While ethical and legal norms will operate in accordance with their usual roles – defining the scope of individual rights, correlative obligations and the like – the means by which ethics and law achieve their ends must cease to ignore the quasi-regulatory apparatus that has been co-opted by the private sector through DRMs.

How should our social institutions respond to private sector automation technologies that are capable of circumventing the protections administered by information and privacy commissioners, data protection officers and the like? How should these oversight bodies respond to DRMs' potential to undo the balancing mechanism between private rights and the public interest? What is the appropriate regulatory response if it turns out that DRMs are used to shift public powers into the hands of private control? Although questions such as these have received much attention within the domain of intellectual property scholarship, their analysis in the context of broader social values such as privacy and freedom of expression are only now beginning to come to the fore.

In the privacy context, answering such questions must commence the same way that it did in the intellectual property field. That is, it begins with the recognition that software can be used to regulate social conduct and that a number of the value choices underlying the chosen means of regulation (some of which transgress existing

forms of regulation such as established ethical and legal norms) are often hidden within the architectures of DRM software (Lessig, 1999; Burk and Cohen, 2001). In the attempt to lay bare such value choices, one would most certainly find that the information collected, used, or disclosed by a DRM does not always comport with established fair information practices.[14]

Consider, for example, a DRM that meters the number of times a digital product is used by an identifiable purchaser from a known demographic within the first three weeks that the product is purchased. Assume that an intelligent and aware purchaser has carefully read the product's terms of use, which indicate that product's use might be monitored at any time for "statistical purposes" (whatever that means). Anxious to use the product and, in any event, knowing that she lacks the bargaining power to alter the terms of use, the purchaser clicks "I agree" when installing the product. How can it be said in any meaningful way that she provided consent (let alone an informed consent) if she has no idea about the kinds of information that are or could have been collected, when the information would be collected, why, for how long the surveillance would take place, or for how long the information that was collected would be used or stored? By what means can she safeguard the accuracy of her data profile (i.e. how can she ensure that a DRM is monitoring and recording only her specific use of the product rather than, say, some unauthorized person's)? How might she ensure that the information collected is not being used for purposes beyond that for which it was originally collected?

Uncovering the structure of particular DRM architectures that violate fair information practices is an important first step for lawyers and policy makers – but it is *only* a first step. The next important step would be to encourage those who design and implement DRMs (ACM, 2003) to work with ethicists, lawyers and policy makers in developing more robust privacy standards within the very design of DRM software. Some such projects are currently underway (Kerr, 2004).

The development and implementation of privacy protocols are particularly poignant in light of the concern expressed by a number of authors that an unfettered use of DRMs could mean an end to the privacy of reading (Cohen, 1996; Greenleaf, 2003). As Cohen so eloquently stated the problem more than half a dozen years ago:

> In truth, however, the new information age is turning out to be as much an age of information *about* readers as an age of information *for* readers. The same technologies that have made vast amounts of information accessible in digital form are enabling information providers to amass an unprecedented wealth of data about who their customers are and what they like to read. In the new age of digitally transmitted information, the simple, formerly anonymous acts of reading, listening, and viewing – scanning an advertisement or a short news item, browsing through an online novel or a collection of video clips – can be made to speak volumes, including, quite possibly, information that the reader would prefer not to share.

Some scholars are only just now beginning to take up this problem set. Greenleaf, for example, has recently responded by arguing that "privacy's relationship to copyright is that the right to experience intellectual works in private – free from surveillance – is part of the public domain aspect of copyright works" (Greenleaf, 2003).

Arguments such as Greenleaf's recognize that there exists a clear link between copyright, privacy and freedom of expression. The manner in which we experience an intellectual work – in absolute solitude or under the camera's eye – must surely have an impact on our thoughts and whether we will choose to express or suppress them. DRM surveillance techniques – which have the ability to monitor what we read or listen to, when, how often, with whom we communicate about them and other related activities – are therefore inextricably tied to our ability to express ourselves freely. A closer look at freedom of expression and its associated policy choices in light of DRMs is therefore in order.

FREEDOM OF EXPRESSION

Public commitments to freedom of expression are integral to democracy. In addition to the intrinsic self-fulfillment associated with the ability to freely express oneself,

freedom of expression is instrumental in the search for truth and to informed democratic participation (Mill, 1947; Meiklejohn, 1965; Emerson, 1963). Though commentary on freedom of expression often focuses on the right to speak, listeners' access to information is also a critical component. Access provides not only a platform for informed decision-making; it can also transform listeners into speakers contributing ideas inspired by the expression of others.[15] As Moon has written,

> The creation of meaning is a shared process, something that takes place between speaker and listener. A speaker does not simply convey a meaning that is passively received by an audience. Understanding is an active, creative process in which listeners take hold of, and work over the symbolic material they receive, locating and evaluating this material within their own knowledge or memory. ...Freedom of expression is valuable because in communicating with others an individual gives shape to his or her ideas and aspirations, becomes capable of reflection and evaluation, and gains greater understanding of her/himself and the world. It is through communicative interaction that an individual develops and emerges as an autonomous agent in the positive sense of being able to consciously direct his or her life and to participate in the direction of his or her community. [Footnotes omitted] (Moon, 2000)

In this way, both the freedom to speak and the freedom to access information and ideas are foundational to freedom of expression. Copyright law, by creating and enforcing privately held rights of exclusivity in relation to the expression of ideas, seems quite inconsistent with a public commitment to free expression. Copyright endows rights holders with a distinct advantage in the marketplace, allowing them to impose limits on the use of their expression, thereby creating barriers to participation by unempowered players in the marketplace of ideas. Nevertheless, many jurisdictions otherwise committed to maintaining a healthy marketplace of ideas have chosen to establish and protect private rights of exclusivity.[16] Many argue that the legal protection of this private right can be reconciled with the public commitment to freedom of expression because copyright can act as an "engine of" free expression. Relying on an economics-based analysis, they assert that by ensuring that copyright holders enjoy a degree of exclusivity that allows them to charge for use of their expression, copyright provides the economic incentive necessary to encourage creation and dissemination of ideas – thereby enhancing and enriching the marketplace of ideas available to all.[17]

Even if one accepts the marketplace model and the theory that some degree of exclusivity is necessary to stimulate expression and creation, determining what degree of exclusivity is actually necessary is key to fair implementation. The law that protects copyright should not, and does not, protect it absolutely. Rather, it strives to afford the degree of private exclusivity necessary to incent creation, without unduly trenching on public access and use. Restrictions on the duration of copyright, its applicability to expression only (and not to ideas or facts themselves), protection of certain "fair uses" of or "fair dealing" with expression, and other limitations are used to restrict the scope of exclusivity and attempt to balance the interest of copyright holders in economic reward with the general public interest in access to information.[18]

Unregulated privately-implemented digital rights management systems need not and, in some cases are not technologically capable of, honouring the balance of public and private interests struck in public policy (Kerr *et al.*, 2003). Deciding whether access to or a particular use of content is legally permissible can be a difficult task, often involving subtle, contextual distinctions. Digital rights management systems are not currently technologically capable of analyzing these fundamental textured distinctions. Perhaps even more disturbing, digital rights management systems can be used to control access to and use of works that are otherwise part of the public domain and therefore not legally subject to copyright restrictions (Lessig, 2002).

Widespread adoption of digital rights management systems could lock up digital content according to the private economic interests of rights holders, with little regard for the fundamental public interest in facil-

itating a healthy marketplace of ideas through access to and use of the expression of others. In addition to erecting cost barriers to accessing and using content (which need not reflect public efforts to balance interests), digital rights management systems could stifle innovation if used to protect outdated modes of content delivery (Lessig, 2001), and discourage participation in the marketplace by those who wish, as Greenleaf put it, "to experience intellectual works ... free from surveillance" (Greenleaf, 2003).

How might a public commitment to freedom of expression inform a decision about whether to extend the public force of law to protect these private mechanisms of social control? The answer may be informed, in part, by how the "free" in freedom of expression is conceptualized.

Jurisdictions that have accepted that some degree of exclusivity is necessary to foster incentives for creation will be reluctant to accept that the "free" in "free expression" means "at no cost", as it might be conceptualized under the "free beer" mentality.[19] Nevertheless, policy makers ought to be open to the possibility that less exclusivity may be required to incent creation in a network environment characterized by comparatively lower costs of production and distribution.[20] Viewed differently, "free"dom could also be conceptualized as "government-free" or "control-free" – each potentially leading to different understandings of policy makers' responsibilities.

"Freedom" in liberal democracies is often conceptualized as "government-free" – "free" from government restriction.[21] Where might this conception of "freedom" lead in determining whether law should protect the technologies that protect copyright (and more)? It might suggest that governments should refrain from acting. To the extent that digital rights management systems restrict access to and use of digital content with little or no regard for the delicate balance of interests underlying public policy, they arguably undermine freedom of expression. On this view, policy makers would arguably be complicit in unduly restricting free expression if they chose to layer public legal protection on top of private technological control. They ought not to do this without a compelling demonstration from rights holders that this additional measure of exclusivity is justified.[22] Even if a compelling justification were possible, policy makers must also consider the negative social impacts of surrendering to private rights holders control over the delicate balance between public and private interests intended to protect fundamental public commitments to free expression.

The answer may be informed, in part, by how the "free" in freedom of expression is conceptualized

If "free"dom were conceptualized as "control-free", it might not be enough for governments to simply refrain from acting. Rather, one might look beyond freedom as the absence of government restraint to recognize the oppressive nature of private social control, which Mill noted "leaves fewer means of escape, penetrating much more deeply into the details of life, and enslaving the soul itself" (Mill, 1947). "Free"dom so conceptualized may require not just that governments refrain from legislating to protect the technologies that protect copyright (and more), but that they take affirmative steps to protect the public from the private imposition of unduly restricted access to and use of information. Some courts have recognized the freedom-enhancing role that government can play by limiting privately imposed restrictions, noting:

> a situation might arise in which, in order to make a fundamental freedom meaningful, a posture of restraint would not be enough, and positive governmental action might be required. This might, for example, take the form of legislative intervention aimed at preventing certain conditions which muzzle expression, or ensuring public access to certain kinds of information. (*Haig v. Canada*, 1993, 2 S.C.R. 995, 1039)

Even before the network environment, real questions existed about whether, or at least how much, private exclusivity was actually necessary to incent creativity and foster a vibrant marketplace of ideas. The prolifer-

ation of digital networks raises these issues once again, compounding them with concerns that control over the balancing of interests essential to maintaining public commitments to freedom of expression will shift away from publicly accountable political institutions to silent technological systems designed to serve the interests of rights holders.

CONCLUSION

Will digital rights management follow a path that leads to the creation of a much greater range of consumer choice and innovative new forms of privacy-friendly content delivery at greatly reduced prices? Or will the greater control afforded to the owners of digital content be used to skew copyright's delicate balance, trumping corporate rights over the public interest? The long-term consequences of our newfound ability to unbundle copyright remain unknown.

In the preceding sections we have offered a number of criticisms of the current, mainstream orientations of digital rights management with the hope of guiding it towards the first path rather than the second. We have tried to render conspicuous an important tactic underlying this approach to digital rights management: to transform the basis of control for intellectual creations from various public powers into the invisible hands of private control. We have also tried to offer a warning: these new forms of social control have the ability to threaten our fundamental public commitments to personal privacy and freedom of expression.

To express our concern in the language of Andrew Carnegie, many of today's digital rights management systems are designed to help only those who pay. They pauperize. They impede the aspiring and lock away from these chief treasures of the world – renting to them instead only brief glimpses, tracking their every move all the while. A taste for such systems drives out higher tastes.

ACKNOWLEDGEMENTS

Ian Kerr wishes to extend his gratitude to the Canada Research Chair program, to the Social Sciences and Humanities Research Council, to Bell, Canada and to the Ontario Research Network in Electronic Commerce for all of their generous contributions to the funding of the research project from which this paper derives. Thanks also to Alex Cameron and to Jennifer Manning for all of their extraordinary efforts, their brilliance, and for the high quality of research assistance that they so regularly and reliably provide.

Jane Bailey wishes to thank Bell Canada and the Ontario Research Network in Electronic Commerce for their generous support of the research initiative associated with this paper. Thanks, as well, to Alex Cameron and Jennifer Manning for research assistance and support extending well beyond the call of duty.

NOTES

1. Originally, Mark Stefik (1999) referred to this technology as "trusted systems": "[t]he term 'trusted system' came originally from military technology. It refers to computer systems that provide access to secret information for national and military purposes. In the last few years, its meaning has been broadened to include systems that protect and govern the use of digital objects and information for commercial purposes." According to Bill Rosenblatt *et al.* (2002), "the term 'digital rights management' was coined by some combination of vendors, their marketers, and industry analysts in the late 1990s."
2. As the RIAA points out on their website (www.riaa.com) under "Protecting Rights on Networks," "Unfortunately, Web sites do not always recognize the piracy concerns of content owners, sometimes allowing music to be posted for downloading in formats, such as unsecured MP3, that include no mechanism for compensating those who created it. To address this problem and to enable the development of new business models for the dissemination of music, the RIAA and its member companies founded (along with IFPI and RIAJ), the Secure Digital Music Initiative, a forum that brings together the worldwide recording and technology industries to develop open standard for specifications for protected digital music distribution..." "RIAA believes that the establishment of technological protection and management for all musical content, regardless of the media on which it resides or the method by which it is transmitted, is a central component for the expansion of both the music opportunities for the consumer and the business opportunities for the technology industry."
3. Barlow (1998). Of course, the idea that a

digital work might be protected indefinitely undermines the time-limited protection afforded by copyright law and, as Lessig (1999) has described, it is tantamount to "hardwiring the legal regime into the technology:"

4. See, for example, *The Digital Millenium Copyright Act of 1998* (DMCA, 1998). See also *Copyright Amendment (Digital Agenda) Act 2000* (Cth.). See, for example, *Japanese Copyright Law No. 48,* promulgated on May 6, 1970 as amended by Law No. 77, of June 15, 1999 and the *Japanese Anti-Unfair Competition Law (JAUCL)*. The amendments made to the JCL and to the JAUCL both came into force on October 1, 1999. See also the European Union's *Directive of the European Parliament and the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society* (2001). O.J.L. (http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/ l_16720010622en00100019.pdf – 1.30.2004).
5. Authors including Mackaay (2001) have used the metaphor of the digital fence to illustrate how intangible property may be protected.
6. Cryptography allows the communication of information in a manner that is disguised so as to keep its content hidden from unintended or unauthorized recipients. See Network Associates and its Affiliated Companies (1990–1999).
7. Burk and Cohen (2001) note that TPMs (technological protection measures), used in conjunction with other legal safeguards, "will be capable of controlling, monitoring and metering almost every conceivable use of a digital work."
8. See e.g. http://www.kazaa.com/us/index.htm. Many opponents of this point of view argue that file-sharing is not stealing. See, for example, Litman (2001).
9. As Jack Valenti (Chairman & Chief Executive Officer of the Motion Picture Association) explained "...unless there is put in place various baffle-plates of protection, we will bear witness to the slow undoing of a huge economic and creative force": Motion Picture Association of America (2003), Press Release: Valenti Testifies Before Senate Commerce Committee, Calls on Congress to Support Efforts to Protect Intellectual Property, http://www.mpaa.org/jack/2003/2003_09_17a.htm, 01.30.04.
10. These issues have already received substantial academic attention: See, for example, Gervais (2001), Ginsburg (2001), Hugenholtz. (2000), Lange and Lange-Anderson (2001), Burk and Cohen, 2001; Litman (2001), Lunney (2001) and Koelman (2001).
11. See e.g. Kerr *et al*. (2002). See, for instance, Weinberg (2000), Stefik, M. (1997), Lessig (2004), Stefik (2004) and Barlow (2004).
12. See, for example, Cohen (2003), Bygrave (2003), Greenleaf (2003), Weinberg (2000), and Cohen (1996).
13. See *Stanford Law Review* (2000). See also Walker (1999), Alfino and Mayes (2003), Bennett (2001), Marx (2001) and Nissenbaum (1997).
14. See the eight OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: 1. Collection Limitation Principle, 2. Data Quality Principle, 3. Purpose Specification Principle, 4. Use Limitation Principle, 5. Security Safeguards Principle, 6. Openness Principle; 7. Individual Participation Principle, 8. Accountability Principle, online at http://www1.oecd.org/publications/e-book/9302011E.PDF accessed 01.30.2004. See also *Model Code for the Protection of Personal Information,* CAN/CSA-Q830-96, online at http://www.csa.ca/standards/privacy/code/Default.asp?language=English accessed 01.30.2004.
15. Numerous international human rights instruments recognize the centrality of access to information in building and maintaining vibrant communities: *Universal Declaration of Human Rights*, G.A. Res. 217 (III) UN GAOR, 3d Sess., Supp. No. 13, UN Doc. A/810 (1948) 71, Art. 19; *International Covenant on Civil and Political Rights,* 23 March 1976, 999 U.N.T.S. 172, Art. 19; *Convention for Protection of Human Rights and Fundamental Freedoms,* 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S. 5, Art. 10.
16. A list of copyright legislation in various countries is at http://www.eblida.org/ecup/lex/.
17. This analysis of copyright's relationship to free expression was recently endorsed by O'Connor J. of the United States Supreme Court in *Eldred v. Ashcroft* 537 U.S. 186 (2003), p. 219.
18. In addition to the impact of digital rights management on "fair use" or "fair dealing", other of these "safety valves" are also slowly being eroded over time by measures such as copyright term extensions, and protections for databases and compilations of fact: Trosow, (2003).
19. Nevertheless, an important message to be taken from the "free beer" approach is that lower costs of use and access reduce barriers that threaten vibrancy and growth in the marketplace of ideas (Boyle, 2003).
20. See Litman (2002), Trosow (2003) and Ku (2003).
21. Liberal constitutional documents often focus on restraining government activity (e.g. U.S. Const. Amend. I), while others explicitly envision a balancing between restraint on government and permitting government to restrain private forces of control (e.g. Part I of the *Constitution Act,* 1982 being Schedule B to the Canada Act

1982 (U.K.) 1982, c. 11 , ss. 1 and 2(b)).

22. Policy makers should view skeptically claims that reductions in revenue through traditional mechanisms of delivery provide sufficiently compelling justifications. See Lessig (2002).

REFERENCES

ACM (2003) *Workshop on Digital Rights Management*, Association for Computing Machinery online at http://portal.acm.org/toc.cfm?id=947380&dl=GUIDE&dl=ACM&type=proceeding& CFID=15968309& CFTOKEN=57534736 accessed 01.30.2004.

Alfino, M. and Mayes, G. R. (2003) Reconstructing the Right to Privacy, *Social Theory and Practice,* 29(1): 1–18.

Barlas, C. and Isherwood, M. (2002) Security technology and rights management information. In Kendrick, J. (ed.), *Collective Licensing: Past, Present and Future,* Maklu, p. 182.

Barlow, J. P. (1998) *Life, Liberty and the Pursuit of Copyright? Round One: Opening Remarks*. http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm, accessed 1.30.2004.

Barlow, J. P. (2004) Life, Liberty and the Pursuit of Copyright, Round Two: Response, http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm accessed 01.30.04.

Bennett, C. (2001) Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web, *Ethics and Information Technology*, 3(3): 157–169.

Boyle, J. (2003) The Second Enclosure Movement and the Construction of the Public Domain, *Law & Contemp. Probs.* 66: 33.

Brandeis, L. and Warren, S. (1890) The Right to Privacy, *Harvard Law Review*, 5: 193–212.

Burk, D. and Cohen, J. (2001) Fair use infrastructure for rights management systems, *Harv. J. L. & Tech.* 41:48.

Cohen, J. (1996) A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace, *Conn. L. Rev*. 28: 981.

Cohen, J. (2003) DRM and Privacy, *Berkeley Tech. L.J.* 18: 575.

Cunard, J. (2001) Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape, online at http://www.alai-usa.org/2001_conference/pres_cunard.doc, accessed 01.30.2004.

DMCA (1998) *The Digital Millenium Copyright Act of 1998*. Pub. L. No. 105-304, 112 Stat. 2860.http://www.copyright.gov/legislation/hr2281.pdf accessed 01.30.2004.

Emerson, T. (1963) Toward a General Theory of the First Amendment, *Yale L. J.* 72: 877.

Gervais, D. (1999) Electronic rights management and digital identifier systems, http://www.press.umich.edu/jep/04-03/gervais.html, accessed 01.30.2004.

Gervais, D. (2001) Lock-it up or license. In Hanson, H. (ed.), *International Intellectual Property Law & Policy*, vol 6, Juris Publishing.

Ginsberg, J. (2001) Copyright and Control over New Technologies of Dissemination, *Colum. L. Rev.* 101: 1613.

Greenleaf, G. (2003) IP, Phone Home: Privacy as Part of Copyright's Digital Commons in Hong Kong and Australian Law. In Lessig, L. (ed.), *Hochelaga Lectures 2002: The Innovation Commons,* Sweet & Maxwell Asia.

Hugenholtz, B. (2000) Copyright, contract and code: what will remain of the public domain, *Brook. J. Int. L.* 26: 77.

Kerr, I. (2004) Look out: The eyes have it. *Globe and Mail* (12 January 2004).

Kerr, I., Maurushat, A. and Tacit, C. (2002) *Technical Protection Measures: Tilting at Copyright's Windmill,* 34 Ottawa L. Rev. 7, pp.13–17.

Kerr, I., Maurushat, A. and Tacit, C. (2003) Technical Protection Measures: Part II – The Legal Protection of TPMs, Heritage Canada, http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/tdm_e.cfm accessed 01.30.2004.

Koelman, K. (2001) The Protection of Technological Measures vs. the Copyright Limitations, online at http://www.alai-usa.org/2001_conference/pres_koelman.doc accessed 01.30.2004.

Ku, R. (2003) Consumer Copying and Creative Destruction: A Critique of Fair Use as Market Failure, *Berkeley Tech. L. J.,* 18, 539.

Lange, D. and Lange-Anderson, J. (2001) Copyright, Fair Use and Transformative Critical Appropriation,online at http://www.law.duke.edu/pd/papers/lange-and. pdf accessed 01.30.2004.

Lee, A. and Bygrave, L. A. (2003) Digital Rights Management and Privacy – Legal Aspects in the European Union. In Eberhard Becker *et al.* (eds.), *Digital Rights Management – Technological, Economic, Legal and Political Aspects*, Springer, p. 418.

Lessig, L. (1999) *Code and Other Laws of Cyberspace,* Basic Books, p. 139.

Lessig, L. (2001) *The Future of Ideas,* Random House Inc., pp. 253–254.

Lessig, L. (2002) Free Culture, Keynote Address OSCON 2002, online at http://www.oreil-lynet.com/lpt/a/2641 accessed 01.30.2004.

Lessig, L. (2004) Architecture of Innovation, http://law.duke.edu/pd/papers/lessig.pdf accessed 01.30.2004.

Litman, J. (2001) *Digital Copyright,* Prometheus Books, p. 163.

Litman, J. (2001) The Breadth of the Anti-Trafficking Provisions and the Moral High Ground, online at http://www.alai-usa.org/2001_conference/pres_litman.doc.

Litman, J. (2002) Copyright Law as Communications Policy: Convergence of

Paradigms and Cultures: War Stories, *Cardozo Arts & Ent. L.J.,* 20: 337.
Lunney, G. (2001) The Death of Copyright: Digital Technology, Private Copying and the Digital Millennium Copyright Act, *VALR* 87: 813.
Mackaay, E. (2001) Intellectual property and the Internet: the share of sharing. In Netanel, N., Elkin-Koren, N. and Bouganim, V. (eds.), *The Commodification of Information*, Kluwer Law International.
Marx, G. (2001) Murky Conceptual Waters: The Public and the Private, *Ethics and Information Technology*, 3(3): 197–210.
Meiklejohn, A. (1965) Political Freedom, Oxford University Press.
Mill, J. S. (1947) On Liberty. In Castell, A. (ed.), *On Liberty*, AHM Publishing Corp.
Moon, R. (2000) *The Constitutional Protection of Freedom of Expression*, University of Toronto Press, pp. 23–24.
Network Associates and its Affiliated Companies (1990–1999) *Introduction to Cryptography*, http://www.pgpi.org/doc/pgpintro accessed 01.30.2004.
Nissenbaum, H. (1997) Toward an Approach to Privacy in Public: Challenges of Information Technology, *Ethics-and-Behavior,* 7(3): 207–219.
Rosenblatt, B., Trippe, B. and Mooney, S. (2002) *Digital Rights Management: Business and Technology,* Hungry Minds, Inc.
Rub, T. (1985) *The Day of Big Operations: Andrew Carnegie and His Libraries,* 173: 7 Architectural Record 81 at 81.
Stanford Law Review (2000) Symposium: Cyberspace and Privacy: A New Legal Paradigm? *Stan. L. Rev.* 52: 987, online at http://stlr.stanford.edu/STLR/Symposia/Cyberspace/index.htm accessed 01.30.2004.
Stefik, M. (1999) *The Internet Edge,* MIT Press, p. 55.
Stefik, M. (1997) Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing, *Berkeley Tech. L. J.* 12: 137, online http://www.law.berkeley.edu/journals/btlj/articles/vol12/Stefik/html/reader.html accessed 01.30.2004.
Stefik, M. (2004) Life, Liberty and the Pursuit of Copyright, Round One: Opening Remarks, online at http://www.theatlantic.com/unbound/forum/copyright/stefik1.htm accessed 01.30.04.
Trosow, S. (2003) The Illusive Search for Justificatory Theories: Copyright, Commodification and Capital, *Can. J.L. & Juris.* XVI(2), 217: 220–221.
Walker, D. (1999) Privacy in the Digital Age: Encryption Policy – A Call for Congressional Action. *Stan. Tech. L. Rev.* 3.
Weinberg, J. (2000) Hardware-Based ID, Rights Management, and Trusted Systems. *Stan. L. Rev.* 52: 1251, online at http://cyber.law.harvard.edu/ilaw/Contract/Weinberg_Full.html accessed 1.30.2004.

Corresponding Authors

Ian Kerr and Jane Bailey
Faculty of Law, University of Ottawa, 57 Louis Pasteur St., PO Box 450, Stn. A, Ottawa, Ontario K1N 6N5, Canada
Email: iankerr@uottawa.ca