

Submission to the Standing Committee on Canadian Heritage on the Section 92 copyright review

Matthew Skala*

October 17, 2003

1 Introduction

This submission is made in response to the Standing Committee on Canadian Heritage Section 92 review of Canada's copyright laws. I am a computer scientist and concerned citizen. I believe my views are typical of those held by my colleagues in the academic and hobbyist communities, but I am not officially speaking for any organisation. My perspective on copyright draws from my perspective on freedom of expression, which I consider to be the overriding concern in any discussion of copyright.

Copyright law exists for the purpose of supporting freedom of expression. For instance, Canadian copyright law in its modern form descends from a 1709 law called the Statute of Anne, whose title begins "An Act for the Encouragement of Learning". [1] As one of my previous submissions detailed, similar goals have been consistently stated as the motivation for modern copyright laws around the world. [2] Society benefits from the creation of books and other expressive work, so policy-makers create a special monopoly privilege for authors, to encourage them to produce expressive work. Everything we do in the realm of copyright must be examined from the point of view of encouraging and supporting expression.

Copyright is two-edged, however, because it is a privilege of limiting others' actions. Copyright law allows privilege holders to say "no" to publications that would otherwise be lawful. Therefore, if the copyright privilege is extended too far, it can harm its own goal by allowing privilege holders to block valuable expression. Currently proposed reforms threaten to do just that, and so motivate this submission.

Many participants in the debate on copyright claim that new developments in technology, such as the Internet, have changed the copyright balances and that the law should change in reaction; as a computer scientist, such changes are directly within my field and concern me a great deal. This submission examines the three issues in copyright reform

*<mailto:mskala@ansuz.sooke.bc.ca>

that concern me most at this time, as well as clarifying some technical points on the limitations of what computers can do, which are not widely understood outside the computer science community.

As well as making my own comments here in this submission, which is released to the public domain, I also support the position of the Balanced Copyright Coalition as described in their 15 September 2003 submission, which I have attached. [3]

2 Technological Protection Measures must not be privileged

Technological Protection Measures (TPMs) must not gain special status in Canadian law. The use of TPMs is questionable for a number of reasons: they block legitimate use of copyright and even public-domain content; they block legitimate use deliberately, by design, instead of merely by accident; and they fail to block the illegal copying they are claimed to target. Furthermore, the flaws of TPMs are inherent in the entire concept; they are not minor oversights that could be “fixed” in legislation or technology.

It is theoretically impossible to prevent the copying of digital data. I discuss this in more detail later in this submission. The basic facts of computer technology dictate that if I can see or hear a file, then I can record it. One traditional saying, often attributed to Bruce Schneier, is that “The only secure computer is one that is turned off, locked in a safe and buried 20 feet down in a secret location, and I’m not completely confident of that either.”¹ Schneier also noted that “Digital files cannot be made uncopyable, any more than water can be made not wet.” [4]; and my own remarks on the subject were cited in one of Heritage Canada’s commissioned studies of TPMs. [5]

Since it is impossible to block copying directly, TPMs operate indirectly, by attempting to regulate use in such a way as to make copying ineffective or undesirable. For instance, one of the protection measures on DVDs is designed to prevent discs sold in one part of the world from being playable elsewhere—the discs can be freely copied, but the copies are supposed² to be difficult to use. Restricting location of viewing is not a traditional copyright privilege. The copyright holders on a book are not allowed to say “You may not read this book overseas.” But allowing the TPM, and legally protecting it from challenge, effectively creates that new copyright privilege. It allows privilege holders to re-write copyright law to suit themselves.

Because computers and other technological devices cannot read human minds and make delicate legal distinctions, TPMs necessarily block legally acceptable conduct. A DVD player, for instance, cannot know whether I am playing a disc to view it (legal), to record

¹I was unable to find the original source in which Schneier said this; it may be apocryphal. Various people in the security community have expressed similar views for a long time.

²The protection can in fact be trivially disabled with readily-available software tools.

it on a VCR and then sell unauthorised copies (illegal), or to record it on a VCR for purposes of academic research (legal). Similarly, TPMs may well be applied to content that is not subject to copyright at all, or that has had its copyright expire—DVDs of public domain movies from the earliest days of cinema are nonetheless subjected to the same TPMs that apply to more recent, copyrighted, material. The publishers are claiming a right to restrict use beyond what is granted them by the Copyright Act.

But this kind of overly broad blocking is not merely an accident. It is part of a deliberate campaign by corporate privilege holders to gain economic privileges the law does not allow them to claim directly. Recent history, especially in the U.S.A., has shown that privilege holders can and will deliberately use legally protected TPMs and expanded copyrights to attempt to block lawful activities they don't like. [6, 7, 8]

Copyright law requires that sometimes, work can be used directly against the wishes of the privilege holders, for important reasons of criticism, research, public debate, and parody. Legally protected TPMs attempt to enforce the privilege holder's wishes, not the law; they are part of the deliberate and insidious effort to confuse “unauthorised use” with “illegal use”. Unauthorised use is sometimes, and in important cases, perfectly lawful.

Legally protected TPMs are also threatening because “protection” of TPMs is usually expanded to include prohibition on the mere discussion of circumvention—placing a chill on the entire field of security research. In recent history, papers have been withdrawn in response to lawsuit threats [7], and researchers have boycotted conferences due to hostile laws in the conference locations [9]. One researcher was recently threatened with a lawsuit just for publishing the fact that a particular TPM scheme could be thwarted by holding down the Shift key on a computer keyboard. [10, 11] The company that made the threats promptly backed down when it realised what a public relations fiasco it was headed for. [12]

So TPMs on the one hand block some legitimate users—and do so deliberately. On the other hand, as cases like the abortive Shift-key lawsuit show, TPMs are often useless in blocking copying anyway. Since illicit users may have much stronger business interests in circumvention, and bigger budgets, the same TPM may be simultaneously useless against illicit users, and insurmountable to legitimate users. Furthermore, because computers fundamentally cannot distinguish legal and illegal uses, and because of the nature of digital files which ultimately are always subject to copying, the idea of effective and appropriate TPMs is fundamentally unworkable.

2.1 TPMs and the Library and Archives of Canada Act

The Committee's recent review of the Library and Archives of Canada Act [13, Bill C-36] raises a uniquely Canadian issue: how do TPMs relate to the archiving requirements imposed by the Act? There was heated debate over whether unpublished material should have its copyright term extended, and if so by how much; protected TPMs allow the holders of creative material to create such an extension for themselves, without the Committee's participation, and claim a copyright in practice that they could not claim in law.

Suppose books or other media are routinely published in a form that is intended to limit the number of readings or viewings. For instance, SpectraDisc has attempted to market “time-limited” DVDs, which break down under the influence of the player’s laser, so that they can only be viewed for a few days after the first viewing. [14] Such discs would of course be useless for archival purposes. Other TPMs depend on using a personal computer to run software that decrypts the content—which may be difficult to do, even without a deliberate time limitation, decades in the future when technology has changed and present-day computers are no longer available. In one typical example, a digital time capsule—created, it should be noted, without even using any TPMs and for the express purpose of preservation—became useless due to technological changes in just a few years, and required elaborate restoration efforts. [15] The situation would be even worse with a deliberately restricted work.

If the Library and Archives builds a collection of digital material encumbered by TPMs, it may find in the future that the collection has become as useless as a collection of moldy, improperly preserved paper books. It is important that the Library and Archives of Canada must archive works in their most accessible and historically useful form—without allowing copyright holders to deliberately or inadvertently booby-trap the archive with TPMs.

3 Court orders must be issued by courts

The U.S. Digital Millennium Copyright Act (DMCA) creates a bizarre regulatory system I call the *Alice in Wonderland* regime: “Sentence first—verdict afterwards.” [16, 17] The DMCA allows plaintiffs in copyright cases to write their own restraining orders, and thereby punish defendants, without needing to bother with going before a judge or presenting any evidence. Canada must avoid creating a similarly inverted system.

In more detail, the DMCA introduces what has also been called a “notice and takedown” system for enforcement of copyright complaints. Anyone who claims to hold the privileges on a document posted on the Web, can file a complaint with the operator of the server that stores the document, the “sysadmin” in technical parlance. Then, regardless of the merits of the complaint, the sysadmin is required to remove the document from distribution—to “take it down”—or face liability. Only after the document has already been taken down, does the poster have a chance to go to court and argue for returning the material to public distribution. The burden of proof has been neatly shifted to the accused party; and the punishment of taking down the Web site, which may be harmful or fatal to a small business even if later reversed, [18] is carried out before any court proceedings have even begun. Sentence first, verdict afterwards.

Last session, Parliament passed Bill C-15A, which created a regulatory system for removal of another class of undesirable content from the Web, namely child pornography. [19] The C-15A regime is essentially the same thing that some participants in the copyright debate refer to as “notice and notice”: the police can send a complaint to the sysadmin of

a computer alleged to contain child pornography, the poster of the material has a chance to respond, then there is a court hearing and if appropriate, the court can issue an order to require the material to be taken down. Notably, the takedown does not happen until a court order has issued.

Privilege holder groups in the present consultation have claimed that notice and notice is insufficient for copyright infringement cases. Because illicit material can be copied so quickly and easily, any delay in the takedown would harm the effective suppression of the material. Thus, there is no time to wait for a court; no time to waste on due process. I suggest that if Parliament cared enough for the Constitutional right of freedom of expression, that it allows even alleged child pornographers a court hearing before punishing them, then the Committee should be similarly careful of the rights of accused copyright infringers. Copyright infringement should not be treated as a worse crime than distribution of child pornography.

That much would be true even if all complaints were legitimate; but the DMCA notice and takedown system also invites flagrant abuse, punishing activities that are not copyright infringement and not illegal at all. Anyone who objects to a document on the Web, for any reason, may have it removed simply by claiming to be a wronged copyright holder and issuing a takedown notice. Such a claim, if false, would eventually catch up to the complainant—but by the time it did, they could have long since achieved their goal of suppressing a critic or punishing an enemy. As one recent example, the Church of Scientology has used DMCA complaints to have its critics' Web sites removed from the search engine Google, by claiming that it owned the copyrights to the critics' original Web site content, and that Google listing the Web site in its directory somehow made Google subject to a takedown order. [8]

Even without such a regime of our own, Canada is already experiencing problems resulting from the *Wonderland* regime in the U.S.A. At one of the Section 92 public hearings, representatives of U.S. television distributor DirecTV openly admitted to sending DMCA takedown notices to Canadian Internet Service Providers (ISPs), never mind that the notices had no legal force in Canada. [20] They apparently thought that sending such notices was perfectly legitimate; they even expressed disappointment that only 3% of the recipients had complied. Michael Geist, a law professor from the University of Ottawa, turned it around in a subsequent intervention: given that we are a supposedly independent nation, isn't it upsetting that as many as 3% of Canadian ISPs were willing to take down customers' Web sites on the strength of a complaint made under a law that doesn't apply here? [21]

4 Researchers must be free to make bibliographic citations

Academic research hinges on citation of previous work. Every research paper contains citations to previous related papers, with information on how to find the previous work typically collected in a section at the end called “references” or the “bibliography”. This very submission contains many citations, and most of the entries in my bibliography include addresses to retrieve the documents over the World Wide Web. The standard format for citations varies depending on the field; in this submission I am loosely following a format popular in computer science journals. Legal professionals use a different format for citations of existing material in court documents—and the law, just like academic research, hinges on citation of previous documents.

Links on Web sites serve exactly the same purpose as the bibliographic citations in academic and legal documents. Links are just citations in a standardised form convenient for computers. Just as a reader like me, trained in the citation practices of computer science, can easily look up the references from a journal article, so a reader equipped with a Web browser can easily look up the references from an online document. The electronic version of this submission even has clickable bibliography entries, so that when I post it on my Web site it will be hard to say whether they should be called traditional “bibliographic citations” or new-media “hyperlinks”. The two concepts are not meaningfully distinguishable.

It is absolutely critical that there be no restrictions on citation; and that means no restrictions on links. I am free to make bibliographic citations to material that is offensive or flat-out illegal [22, 23, 24, 25]; and I am free to make citations without any permission from, and even directly against the wishes of, the authors or privilege holders of the material I cite. These freedoms are absolutely fundamental and necessary to discourse in the academic and legal realms. What makes freedom of citation reasonable is that by citing a document I need not be in any way endorsing, or endorsed by, the document or whoever wrote it. I might cite a document I agree with [3] or one I disagree with [22]; and one that I created myself [2] or one I took no part in. [7] Citation, by itself, does not create any specific kind of relationship between me and the document I cite.

Imagine the difficulties we would have prosecuting criminals if judges were forbidden to mention the documents involved in a case, either because the documents themselves were illegal and so could not lawfully be cited, or because the defendants refused permission to cite the documents. The system would fall apart. No judge would be allowed to write a document like the final written decision in *R. v. Sharpe*, because it cites illegal documents and documents written by hostile authors, who would withhold permission to cite. [26]

But for whatever reason, some intervenors have suggested that it would be a good idea to forbid linking under some circumstances. That would not be a good idea. There must be no automatic liability for posting a link to illicit material; and there must be

no requirement to have anyone’s permission to post a link. Links are citations and must remain as unrestricted as any other citations.

It is true that the Web is different from printed media, but the technical differences between the Web and print media are, if anything, reasons why the freedom to link is all the more important on the Web. Documents on the Web change frequently. If I post a link to, for instance, a regularly-updated news site that was completely inoffensive when I viewed it myself, the very next day they could decide to report on a series of horrific murders and publish photos that offend readers who follow my link. I cannot be blamed for that, although of course I must be free to cite it even if I did know the site was objectionable. Web sites change, unlike printed material, and so those who cite Web sites can take even less blame for the present content of the cited sites than for printed material.

It has been suggested that direct links, which “cause the immediate download” [27] of allegedly illicit material, should be treated differently from other links.³ That is a false, and dangerous, distinction. First of all, every link always causes an immediate download if it is followed at all—nothing can ever be viewed on the Web without downloading it first, as I explain in Subsection 5.2 below. At best, there may be a distinction as to whether the downloaded file will be saved indefinitely or discarded after one viewing. Second, the question of whether a file will be viewed immediately and then discarded, or saved on disk for later viewing, is determined by the reader’s browser configuration. If I post a link, I cannot control what the reader might do with it; it is unreasonable, then, to attach liability to me or not depending on a decision out of my hands. Most popular browsers make the decision between “save” and “immediate view” based on a guess as to the content type of the downloaded document (text, graphics, audio, video, and so on)—which is also by definition out of my hands when I did not post the document and the document could have changed since I made the citation. The fact that I cannot control the reader’s computer’s actions is not a technological issue that could be ever be fixed; no matter what labels I might attach to the link to tell the reader’s computer “save this indefinitely once you download it” or “throw it away after displaying it once”, the reader’s computer will ultimately follow its owner’s orders in preference to whatever I might say.

5 Limitations of computers

There is a strong tendency in the non-technical community to regard computers as magic. If ever we face a difficult problem in the human realm, someone has the bright idea that, hey, maybe the techies can solve it by “doing some of that computer stuff”!⁴ The entire concept of TPMs stems from this kind of thinking. Someone who thinks that there is a magical technical solution to the problems faced by the music and movie industries is

³The term “deep linking” has been used to describe this situation; I prefer “direct linking” because “deep linking” already has a generally accepted and quite different meaning.

⁴I think legislators are sometimes similarly expected to perform miracles.

unlikely to take “no” for an answer, no matter how many times I and my colleagues try to say “no”. The problem is exacerbated by the tendency of some computer professionals to tell clients “That is impossible,” when the actual situation would be better described as “That might be technically possible, but I don’t want to spend hours explaining to you the complicated and important consequences of what you have demanded.” Clients stop taking “no” for an answer when computer professionals start using it in that sense, leaving us with no way to respond when the request really is impossible.

The belief that computers are magic and can solve all our problems has caused a great deal of grief and many misunderstandings in recent years. As a theoretical computer scientist I would not wish to go so far as to declare that computers are not magic; but I would say that even magic has limits. Computers have limits, and the limits cannot be broken no matter how much the Committee or anyone else might wish that the limits could be broken. Just as physics has laws like the conservation of energy, computer science has its own fundamental laws. Some of the laws of computing are easy to understand; the copyright debate would benefit from everyone better understanding the laws of computing; and so in this section, I will attempt to describe some basic computer science in an understandable non-technical form.

5.1 Computers operate on numbers

All pieces of information inside a computer are represented as numbers, and there is only one kind of number. The numbers representing a piece of text (like this submission) are fundamentally the same as the numbers representing a piece of music or a motion picture. They only gain meaning when the computer and its human owner decide to declare that these numbers represent a document, those numbers represent a song, and some other numbers over there represent a movie. At any moment we could decide to instead treat them merely as generic numbers.

The important consequence of all numbers being of the same kind is that anything a computer can do to one number, it can do to any similar number. Saying, “Here’s a movie, and you can watch it on a computer but not copy it!” is like saying, “Here’s a number, 45, and you can add 24 but you can’t subtract 3!” Any computer scientist would laugh and say “42.” You cannot prevent anyone from subtracting 3 from 45, no matter how much you want to.⁵

5.2 Computers cannot force each other to forget things

Not only is copying numbers always possible, but copying is the fundamental operation computers perform on numbers. If we say that we have “moved” a file from one disk drive

⁵One might argue that in some sense I can’t subtract 80 from 45, but the point is that one 45 is the same as any other 45. There is no magic 45 from which 3 cannot be subtracted.

to another, that is actually a shorthand term: behind the scenes, the “move” command actually works by making a perfect copy of the file and then deleting the original. The World Wide Web is based on copying: When you view a Web document, what happens is that your browser sends a request to the “server” elsewhere on the Net, saying “Please send me such-and-such document.” The server sends a copy of the document. At each of the points along the way, the document is copied bit by bit from one machine to the next until it reaches your computer. Normally, the intermediaries destroy their copies as soon as they have finished copying them to the next machine along the path. Once there is a copy on your computer’s disk drive,⁶ you can view the document. It is important to understand that before you can see the document at all, it must have already been copied from the server to your computer. Depending on your Web browser, your own computer will usually hold onto its copy of the document, to save the trouble of requesting another one from the server if you want to look at the same document again soon. The temporary copies are stored in a place on disk called the “cache”, and usually deleted after a few days.

The general process of copying documents over a network is called “downloading”.⁷ I was disappointed to read in the Evidence of the Committee a member challenging a witness to “tell me what your understanding of sampling [archival documents from the Web] is and how it isn’t downloading[.]” [28] The member makes a good point but also misses one—of course sampling is downloading. Everything that involves looking at documents on the Web is downloading. It would be better to have the witness explain why downloading documents for the purposes of sampling, is different from downloading them for the purposes of infringement. It would be terribly unfortunate if the Committee were to decide that “downloading” is a dirty word. The Web would have to shut down.

Although all documents must be copied before they can be viewed, human beings see a difference between copying the document, looking at it, and then eventually deleting the copy; and copying the document and keeping the copy indefinitely for repeated viewing. The server does not see this difference, however. It sends the document to your computer once in either case. The only difference is whether your computer forgets the document soon, or later.

The fact that all documents on the Web must be downloaded before they can be viewed has an interesting consequence: the server cannot control whether you delete your copy after viewing it, or keep it indefinitely. That is, ultimately, the reason “pay-per-view” schemes cannot be secure: once the user’s computer has received the data once, and that must happen in order to view it at all, then the user can instruct their computer to keep the file instead of deleting it.

Suppose I were to write here, “Forget you ever read this submission.” I could write

⁶Computers have several forms of memory, some more permanent than others, but most popular Web browsers today save documents to disk, relatively permanently, immediately upon viewing.

⁷It has in some contexts been traditional to draw a distinction between “downloading” and “uploading” based on a rough concept of larger computers being “above” smaller ones, but all file transfers on the Web are generally called downloads.

that, but I could not force you to actually forget the submission. Similarly, computers cannot force each other to forget things, no matter how much you want them to.

5.3 Computers cannot read human minds

One popular complaint among computer users is that “The machine won’t do what I want, only what I tell it!” That is a fundamental limitation of computers—they cannot read minds. The practical consequence is that computers cannot act differently depending on the human reason for something. A disc-copying program, for instance, cannot permit copying for fair dealing and not for infringement; it only knows that it has received a “copy” command. At best it could ask the user, “Are you requesting this for legal purposes?” but it could not constrain the user to answer truthfully; and the existence of such a program would necessarily mean that someone else could build a similar program that would not even bother to ask.

Because computers cannot read human minds, TPMs (to the extent they can work at all, which is already narrowly limited) can never capture distinctions in the purpose of acts: they can only limit acts as such, independent of purpose. Building a copier that can only make lawful copies is like building a bullet that can only shoot bad people. Think how wonderful it would be to give those bullets to our soldiers and police! We would never have to worry about friendly fire or accidental shootings again. But it will not happen, no matter how much we want it to.

5.4 Computers cannot disobey their owners

The other side of “The machine won’t do what I want, only what I tell it!” is that within the limits of its capabilities, the computer really will do what you tell it. Assuming technical competence, owners of computers have ultimate control over their computers’ actions. That means, for instance, that even if you hand me a CD which contains, encoded onto it, instructions along the lines of “Attention, computer! Do not copy this CD!”, I am free to tell my computer, “Ignore the instructions on this disc; just copy it, anti-copying instructions and all.” And it will do so—even if you elaborate the label on the disc to say things like, “Do not copy this disc and do not ignore this label, even if your owner tells you to ignore this label, really, don’t do it!” Those kinds of TPMs appear to the computer as numbers just like any other numbers; there are no magic numbers that must be obeyed.

Even a specially-built computer which took its orders from a source other than the normal controls, would not work; if I bought one, I would simply find out which connection it used to take its real orders, control it through that, and teach other hobbyists to do the same. Witness the recent phenomenon of “Xbox hacking”, in which owners of Microsoft Xbox computers have figured out ways to use them for purposes unintended by the man-

ufacturer despite heavy TPMs designed to make that pursuit difficult.⁸ [29] You cannot force computers to disobey their owners, no matter how much you want to.

6 Biographical notes

My name is Matthew Skala. I am a PhD candidate in computer science at the University of Waterloo, and hold BSc (computer science and mathematics combined co-op, with distinction, 1999) and MSc (computer science, 2001) degrees from the University of Victoria. I am currently supported by an NSERC Postgraduate Scholarship (PGS B) and have received numerous other honours and awards including the University of Victoria Fellowship, the Paul Smith Memorial Prize for performance in the Putnam Mathematical Competition, and a “Best Student Paper” from the Government of Canada’s Communications Security Establishment. [30] I have been named an Honorary Teenager by the youth-rights organisation Peacefire. [31]

My research interests cover theoretical computer science, computer security, computing policy, and especially the intersection of these three. My best known work was on just such a topic: in early 2000 I collaborated with Eddy Jansson, in Eskilstuna, Sweden, on the critical analysis and review of a “filtering” package claimed to prevent computer users from viewing objectionable material on the World Wide Web. [32] The vendors of the software alleged that our review violated copyright law, and the resulting lawsuits made front-page news across Canada and highlighted many important issues in the copyright debates. [33, 34] Our case was cited by the U.S. Library of Congress in its later rulemaking on exceptions to the Digital Millennium Copyright Act. The Library created a DMCA exception, one of only two that were granted at all, specifically to permit critical examination of “filtering” software. [35, page 64564]

I have been involved in the Section 92 process since the public comment period of Summer 2001, when I filed a lengthy comment document (in fact, the longest from any individual or group) titled *New Media Copyright Extensions Would Harm Canada*. [2] I filed three response comments in the second phase [36, 37, 38], attended the public consultation meetings in Toronto and Ottawa and wrote reports on what I observed there, and filed an additional comment, discussing additional concerns, in April of 2002. I am active in the ongoing discussion of the Section 92 process within the academic and hobbyist communities. As well as the Section 92 process, I have participated in CRTC public comment processes on Broadcasting Public Notices 2002-32 (digital television) [39] and 2002-38 (Internet retransmission of television) [40, 41] and the Justice Department comment process on “lawful access” and wiretapping. [42] I gave an invited lecture on “lawful access” at the

⁸Here the TPMs attempt to protect yet another privilege far beyond the traditional copyright bundle—there was a time when it was taken for granted as a simple property right that if you bought something, then you owned it and were entitled to full control of it; but now the Xbox hackers are being threatened under the DMCA for attempting to gain full control of their own property.

University of Toronto in March of 2003. [43] All my submissions, and the slides from the “lawful access” talk, are available through my Web site. [44]

I would be happy to travel to Ottawa to address the Committee directly.

7 Conclusion

I have described the three most significant issues to me: that technological protection measures must not be privileged, that court orders must be issued by courts, and that researchers must be free to make bibliographic citations. Computers have limitations, and as a computer scientist it is my job to understand and explain those limitations; I have discussed some limitations relevant to copyright. Finally, in all copyright issues, freedom of expression is the most important value because copyright exists to promote freedom of expression. Freedom of expression must guide the copyright discussion.

References

- [1] An Act for the Encouragement of Learning, by Vesting the Copies of Printed Books in the Author’s *[sic]* or Purchasers of Such Copies 8 Anne, c. 19 (1709). In Philip B. Kurland and Ralph Lerner, editors, *The Founders’ Constitution*, clause 1.8.8, no. 2. University of Chicago, 1987. Online http://press-pubs.uchicago.edu/founders/documents/a1_8_8s2.html.
- [2] Matthew Skala. New media copyright extensions would harm Canada, August 24 2001. Submission of Matthew Skala to the Intellectual Property Policy Directorate, Industry Canada, and the Copyright Policy Branch, Canadian Heritage, in response to the June 22, 2001 discussion papers. Online <http://ansuz.sooke.bc.ca/icsub.html>.
- [3] Balanced Copyright Coalition. Submission to Heritage Committee, September 15 2003.
- [4] Bruce Schneier. The futility of digital copy prevention. *Crypto-Gram Newsletter*, May 15 2001. Online <http://www.schneier.com/crypto-gram-0105.html#3>.
- [5] Ian Kerr, Alana Maurushat, and Christian S. Tacit. *Technical Protection Measures: Part II—The Legal Protection of TPMs*, page 8. Department of Canadian Heritage, 2003. Online http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/protection_e.pdf.
- [6] Plaintiff’s verified complaint in *Microsystems Software, Inc. and Mattel, Inc. v. Scandinavia Online AB, Islandnet.Com, Eddy L.O. Jansson, and Matthew Skala*, March 16 2000. Civil No. 00CV10488 EFH. Online http://www.eff.org/IP/DRM/Microsystems_v_Scandinavia_Online/20000316_verif_complaint.html.

- [7] Scott A. Craver, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. Reading between the lines: Lessons from the SDMI Challenge. In *4th International Information Hiding Workshop*, Pittsburgh, PA, USA, April 25–27, 2001. Statement read in lieu of withdrawn paper. Online <http://www.cs.princeton.edu/sip/sdmi/sdmimessage.txt>.
- [8] Matt Loney. Cult forces Google to remove critical links. *ZDNet UK*, March 21 2002. Online <http://news.zdnet.co.uk/internet/0,39020369,2107088,00.htm>.
- [9] Alan Cox. Declaration in the United States District Court for the District of New Jersey, August 13 2001. Case No. CV-01-2669 (GEB). Online http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html.
- [10] Eric Bangeman. New CD copy protection easily compromised. *Ars Technica*, October 8 2003. Online <http://arstechnica.com/archive/news/1065630292.html>.
- [11] Fred Locklear. Press “shift” to initiate lawsuit. *Ars Technica*, October 9 2003. Online <http://arstechnica.com/archive/news/1065755223.html>.
- [12] Josh Brodie. Threat of lawsuit passes for student. *The Daily Princetonian [Web edition]*, October 10 2003. Online <http://www.dailyprincetonian.com/archives/2003/10/10/news/8797.shtml>.
- [13] Sam Banks. Bill C-36: The Library and Archives of Canada Act. Legislative Summary LS-460E, Parliamentary Research Branch, September 11 2003.
- [14] Andy Patrizio. DVDs that self-destruct. *Wired News*, January 20 2000. Online <http://www.wired.com/news/technology/0,1282,33781,00.html>.
- [15] John Innes. Experts unlock BBC’s archive of life in the Eighties. *Scotsman.com News*, December 2 2000. Online <http://www.news.scotsman.com/archive.cfm?id=1340622002>.
- [16] U.S. Congress. Digital Millennium Copyright Act (DMCA). In *United States Code, Title 17*, section 1201. U.S. Copyright Office, 1998.
- [17] Lewis Carroll. *Alice’s Adventures in Wonderland*. Project Gutenberg, Millennium Fulcrum edition, March 8 1994. Online <http://www-2.cs.cmu.edu/People/rgs/alice-table.html>.
- [18] Sandy Harris. Comments in Industry/Heritage public consultation meeting, Toronto, Ontario, March 26 2002.

- [19] David Goetz and Gérald Lafrenière. Bill C-15A: An Act to amend the Criminal Code and to amend other Acts. Legislative Summary LS-410E, Parliamentary Research Branch, September 30 2002.
- [20] DirecTV, Inc. Comments in Industry/Heritage public consultation meeting, Ottawa, Ontario, April 11 2002.
- [21] Michael Geist. Comments in Industry/Heritage public consultation meeting, Ottawa, Ontario, April 11 2002.
- [22] Valerie Solanas. *The SCUM Manifesto*. Ak Press, 1997. Online (in a different edition) <http://www.ai.mit.edu/~shivers/rants/scum.html>.
- [23] Adolf Hitler. *Mein Kampf*. G S G & Associates, 1981. Translated by James Murphy.
- [24] Anonymous. Eh. Online <http://www.goatse.cx/>.
- [25] John Robin Sharpe. Sam Paloc's flogging, fun and fortitude—a collection of Kid-diekink Classics.
- [26] Supreme Court of Canada. R. v. Sharpe. 2001 SCC 2. Online http://www.lexum.umontreal.ca/csc-scc/en/pub/2001/vol11/html/2001scr1_0045.html.
- [27] David Basskin. Comments in Industry/Heritage public consultation meeting, Toronto, Ontario, March 26 2002.
- [28] Sarmite Bulte. Question to Ian Wilson. In *Evidence of the Standing Committee on Canadian Heritage*, June 3 2003. Online <http://www.parl.gc.ca/InfoCom/PubDocument.asp?DocumentID=968284&Language=E#Int-579004>.
- [29] XboxLinux Project. Online <http://xbox-linux.sourceforge.net/>.
- [30] Matthew Skala. A limited-diffusion algorithm for blind substring search. In *Proceedings of the 10th Annual Canadian Information Technology Security Symposium*, pages 397–410, Ottawa, Ontario, June 1–8 1998.
- [31] Peacefire. Honorary teenagers. Online <http://www.peacefire.org/HonoraryTeenagers/>.
- [32] Eddy L.O. Jansson and Matthew Skala. The breaking of Cyber Patrol® 4. Posted on the World Wide Web, March 11 2000. No longer distributed due to court settlement.
- [33] Chris Wood. E-commerce and the law. *Macleans*, April 10 2000. Online <http://www.macleans.ca/topstories/article.jsp?content=32979>.

- [34] CBC News Online staff. Hacker causes headache for Mattel's Cyber Patrol. *CBC News Online*, April 25 2000. Online <http://cbc.ca/cgi-bin/templates/view.cgi?/news/2000/04/24/mattel1000424>.
- [35] Copyright Office, Library of Congress. Exemption to prohibition on circumvention of copyright protection systems for access control technologies. [*U.S.*] *Federal Register*, 65(209):64556–64574, October 27 2000. Online <http://www.copyright.gov/fedreg/2000/65fr64555.pdf>.
- [36] Matthew Skala. Response to the submissions of DirecTV, Inc. and Kyle Lahnakoski, October 15 2001. Online <http://ansuz.sooke.bc.ca/icresp1.html>.
- [37] Matthew Skala. Response to the submissions of Eric R. Smith, PhD and Coridon Henshaw, October 17 2001. Online <http://ansuz.sooke.bc.ca/icresp2.html>.
- [38] Matthew Skala. Response to the submissions of Aliant Inc., et al.; Telus Corporation; DirecTV, Inc.; and Information Mechanics Ottawa, Inc., October 20 2001. Online <http://ansuz.sooke.bc.ca/icresp3.html>.
- [39] Matthew Skala. Submission in response to BPN 2002-32, August 15 2002. Online <http://ansuz.sooke.bc.ca/crtc2002-32.html>.
- [40] Matthew Skala. Submission in response to BPN 2002-38, September 4 2002. Online <http://ansuz.sooke.bc.ca/crtc2002-38.html>.
- [41] Matthew Skala. Reply comment in response to initial comments on BPN 2002-38, October 3 2002. Online <http://ansuz.sooke.bc.ca/crtc2002-38r.html>.
- [42] Matthew Skala. Protecting lawful private communications, December 16 2002. Submission to Department of Justice. Online <http://ansuz.sooke.bc.ca/lawful-sub.html>.
- [43] Matthew Skala. Protecting lawful private communications. In *Information Rights Salon*, Toronto, Ontario, March 24 2003. University of Toronto. Slides online <http://ansuz.sooke.bc.ca/20030325slides.pdf>.
- [44] Matthew Skala. DMCA de Canada. Online <http://ansuz.sooke.bc.ca/candmca.html>.