Comments Regarding the Ministry of Economic Development's

Discussion Paper on

Digital Technology and the Copyright Act of 1994

I. Executive Summary

The Electronic Frontier Foundation submits these comments in response to the Discussion Paper on Digital Technology and the Copyright Act of 1994 ("Discussion Paper") prepared by the Ministry of Economic Development ("Ministry"). These comments will primarily address three of the issues considered in the Discussion Paper: (1) the reproduction right in the digital environment (Question 5); (2) legal protection for technological measures (Question 12); and (3) the liability of network intermediaries, such as ISPs (Question 11).

With respect to the reproduction right, EFF is concerned that the expansion of the right to make copies to include temporary and incidental digital copies (e.g., RAM copies) will (1) upset the copyright balance by creating a new "exclusive right to read" in favor of copyright owners and (2) make necessary an ongoing project of ad hoc judicial and legislative exceptions in order to protect legitimate user interests. In light of these concerns, we recommend:

Proposal: Amend the Copyright Act to clarify that temporary and incidental digital copies are not included within the definition of "copies" for purposes of the Act.

With respect to legal protections for technological measures, we urge the Ministry to preserve two important public policies: (1) the historical balance between the interests of the public and copyright owners, as reflected in the rights and exceptions contained in the Copyright Act; and (2) the values of free expression and scientific progress. In light of these concerns, we make the following recommendations:

Proposal 1: Consider whether any changes to the Copyright Act are required by the WIPO Copyright Treaty.

Proposal 2: Any circumvention prohibition should be limited to circumventions undertaken for the purpose of infringement.

Proposal 3: Any circumvention prohibition should include a "legitimate purpose" exception.

Proposal 4: Any circumvention prohibition must include protections for "innocent circumventors."

Proposal 5: The knowledge requirement contained in current Section 226(2) of the Copyright Act should be retained unchanged.

With respect to any limitations on copyright liability for network intermediaries, we urge the Ministry to be ensure that any such safe harbors: (1) create a regime that respects the privacy and free expression rights of Internet users; and (2) preserve and foster the end-to-end architecture that has made the Internet such an successful platform for innovation and competition. In light of these goals, we make the following recommendations:

Proposal 1: Amend the Copyright Act to make it clear that temporary and incidental digital copies do not implicate the reproduction right.

Proposal 2: No affirmative obligation to monitor Internet users.

Proposal 3: Notice and take-down should be limited to materials residing on the ISP's own computer systems.

Proposal 4: Notice and take-down procedures should reasonably preserve user anonymity.

Proposal 5: Any notice and take-down process should include a non-waivable affirmative counter-notice provision in favor of Internet users.

Proposal 6: Anyone performing ISP functions, including the transmission and routing of network transmissions, hosting or caching, should be entitled to whatever safe harbor is ultimately adopted.

II. The Commenting Party

The Electronic Frontier Foundation is the leading nongovernmental organization devoted to protecting free expression, civil liberties and individual rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression, privacy, and openness in the information society. EFF is a private, nonprofit, member-supported organization based in San Francisco, California, U.S.A., and maintains one of the most linked-to websites in the world: http://www.eff.org.

III. The Reproduction Right in the Digital Environment

Question 5 of the Discussion Paper asks:

> a. Is there a need to amend the definition of “copying” in the Act to take account of incidental and temporary copies that are automatically made by computers and computer networks as part of technical processes?
>
> b. If so, should the definition of “copying” be amended to:
>
> - include the making of temporary or incidental copies in all circumstances;

- include the making of temporary or incidental copies, but excuse liability for infringement where the copying is automatically undertaken as part of a technical process in a computer system; or
- exclude copying that is automatically undertaken as part of a technical process in a computer system?

The EFF urges the Ministry to adopt the last option—amend the Copyright Act to clarify that the making of incidental and temporary digital copies ("RAM copies") does not constitute "copying" that infringes a copyright owner's reproduction right. The U.S. experience demonstrates that treating RAM copies as potentially infringing (1) upsets the copyright balance by creating a new "exclusive right to read" in favor of copyright owners and (2) makes necessary an ongoing project of ad hoc judicial and legislative exceptions in order to protect legitimate user interests. These burdens are particularly difficult to justify to the extent copyright owners may protect themselves against unauthorized uses in the digital environment under existing copyright principles.

A. The Copyright Balance and an "Exclusive Right to Read"

As the Discussion Paper recognizes, New Zealand's Copyright Act is premised on a balance between the rights of creators and the interests of users.[1] The Discussion Paper further recognizes that the balance contained in the present legislation should generally be preserved in the digital world. "Legislative provisions should apply consistently across the digital and analogue/print environments."[2]

Acceptance of the RAM copies doctrine, however, would fundamentally upset the legislative balance represented in the present Copyright Act. Under the Act, copyright owners are granted a limited roster of exclusive rights.[3] The public remains free to engage in any activities that do not run afoul of these rights. So, for example, an owner of a book may, without fear of legal action, read the book in any manner, at any time, and as many times as he may please. Similarly, he may tear out pages, write in the margins, and ask a friend to read a passage over his shoulder. In fact, in the balance represented by the present Copyright Act, virtually *all* everyday private uses of a book fall outside the reach of copyright owners.

The recognition of RAM copies as actionable copyright infringement upsets this aspect of the copyright balance in the digital world. Since computers must make RAM copies in order to function, suddenly *every* private use of a digital work would come within the exclusive control of the copyright owner. Under this view, for example, the legitimate owner of a DVD movie would be making potentially infringing reproductions each time he played the DVD on a computer.

---

[1] Discussion Paper, paragraphs 49-52.

[2] Id.

[3] Copyright Act 1994, Section 16 (setting out exclusive rights granted to copyright owners).

The RAM copies doctrine would thus effectively create an "exclusive right to read" in favor of copyright owners.[4] Every display or performance of a digital work, whether public or private, would implicate the reproduction right, and thus be subject to the control of copyright owners. This breathtaking expansion of owners' right in the digital world is at odds with copyright's historical concept of balance.

B. The Mischief of Ad Hoc Exceptions

Of course, to the extent the RAM copies doctrine spawns a sweeping "exclusive right to read," new exceptions may be legislatively or judicially crafted to re-create the copyright balance contained in the current Copyright Act. For example, courts might interpret "fair dealing" to privilege owners of DVDs to make RAM copies in order to enjoy the works they have purchased, or may fashion an "implied license" theory to accomplish the same ends. New statutory exceptions could also be enacted to permit private use of legitimately purchased digital works.

The creation of ad hoc exceptions to the reproduction right, however, cannot hope to keep pace with the pace of computer innovations. All computers, whether used for email, web browsing, network communications, or e-commerce, depend on temporary, incidental RAM copies in order to function. Virtually all electronic communication, moreover, involve data that may be the subject of copyright. As a result, exceptions to the RAM copies doctrine will be necessary to accommodate every new facet of computer technology. This process is sure to be a cumbersome one.

The U.S. experience illustrates the problem. The U.S. Congress already has had to fashion three exceptions to the reproduction right as a result of the uncertainties created by the RAM copies doctrine. First, the U.S. Copyright Act was amended to make it clear that software owners were entitled to make RAM copies in the course of utilizing the software they purchased.[5] Second, the U.S. Congress fashioned a "safe harbor" to insulate ISPs from liability for temporary copies made on their systems.[6] Third, Congress amended the Copyright Act to permit computer hardware maintenance companies to make temporary copies of computer programs in the course of rendering services.[7] Recently, the U.S. Copyright Office recommended the adoption of yet another exception, this time for temporary copies made during the course of music webcasting.[8]

---

[4] The term "exclusive right to read" was coined by American copyright scholar Jessica Litman. *See* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENTERTAINMENT LAW JOURNAL 29 (1994).

[5] Copyright Act of 1976 section 117, 17 U.S.C. § 117(a).

[6] Id. at section 512, 17 U.S.C. § 512(a).

[7] Id. at section 117, 17 U.S.C. § 117(c).

[8] *See* U.S. Copyright Office, DMCA SECTION 104 REPORT at 141-47 (August 29, 2001) (available at http://lcweb.loc.gov/copyright).

Not only is this ad hoc approach cumbersome, but it may also interfere with the dynamism of the technology sector. If computer-related businesses in New Zealand are required to await legislative exceptions to the RAM copy rule before they are able to confidently launch new digital technologies, they will be at a competitive disadvantage. Asking technology companies to proceed without a legislative exception is to ask them to depend on uncertain defenses (whether "fair dealing" or an "implied license" defense) should litigation be brought. These choices, even if they do not deter all technology companies, will certainly reduce investment in this important sector of the economy.

Instead of turning the copyright balance on its head by recognizing RAM copies as reproductions for copyright purposes, it makes more sense to exclude RAM copies from the scope of the reproduction right and preserve the current statutory scheme. As the Discussion Paper points out, the primary justification for the RAM copy doctrine is the fear of widespread piracy in a networked digital world. If copyright owners are concerned about opportunities for piracy in the networked world, those concerns are better addressed in the context of the "make available to the public" right required by the WIPO Treaties. Such an approach would preserve private uses and leave technologies unrelated to transmission free from the unnecessary encumbrances of copyright law.

C. Proposal

In light of the considerations detailed above, EFF proposes the following:

Proposal: Amend the Copyright Act to clarify that temporary and incidental digital copies are not included within the definition of "copies" for purposes of the Act.

In light of the negative consequences of the RAM copies doctrine, the Ministry should study carefully the possibility that the valid piracy concerns of copyright owners would be better addressed though a "making available to the public" right, rather than through an unprecedented expansion of the reproduction right.

IV. Legal Protection of Technological Measures

Question 12 of the Discussion Paper asks:

> a. Are existing legal provisions sufficient to protect the interests of copyright creators and owners concerning the use of technological protection mechanisms and electronic rights management information in relation to copyright works?
>
> b. If existing legal provisions are not considered adequate, what changes or additions should be made? In particular, which of the following non-exclusive approaches should be examined in more detail:
>
> - expanding the existing copy-protection provisions in the Act;
> - introducing new provisions in relation to electronic rights management information;

- providing that suppliers of circumvention devices, means or information be liable for infringement where they ought reasonably to have known that the device, means or information would be used for circumvention purposes;
- introducing criminal sanctions in relation to prohibited activities relating to technological protection measures and/or electronic rights management information; and/or
- prohibiting the actual circumvention of technological protection measures and/or interference with electronic rights management information.

EFF believes that New Zealand's current Copyright Act is sufficient to protect the interests of copyright creators and owners concerning the use of technological protection mechanisms. If the Ministry concludes that some additional protections are necessary, EFF urges the Ministry to tailor such additional protections to preserve two important public policies: (1) the historical balance between the interests of the public and copyright owners, as reflected in the rights and exceptions contained in New Zealand's Copyright Act of 1994 as amended; and (2) the public values of free expression and scientific progress. The U.S. experience with "anti-circumvention" provisions, however, suggests that the Ministry should refrain from broadening the scope of the existing provisions in the Copyright Act, lest the important values identified above be undermined.

A. Preservation of the Copyright Balance

As the Discussion Paper recognizes, one of the major objectives of New Zealand's Copyright Act is "to ensure a proper balance between the protection provided to authors and owners of copyright and the ability of users to access copyright material."[9] Because this balance aims to reconcile important competing public policy priorities, the crafting of the copyright balance has properly rested in the New Zealand Parliament and the judicial process.[10]

The balance is reflected in the Copyright Act by a broad grant of certain exclusive rights to copyright owners for a limited time, on one hand, and a number of exceptions and limitations to preserve access for the public, on the other.[11] Each of the limitations on the scope of a copyright owner's exclusive rights reflect a deliberate legislative conclusion that "Parliament has determined that the wider public interest or the interests of particular groups makes it necessary to restrict or limit the rights granted to copyright owners."[12] For example, several elements of the Copyright Act reflect recognition of the critical roles played by libraries, archives and museums in ensuring that a repository of

[9] Discussion Paper, paragraphs 21, 170.

[10] Id, paragraphs 27-28. *See, e.g.,* Copyright Act, section 43 (determination of fair dealing for research or private study involves judicial balancing of competing factors).

[11] Id, paragraphs 26-28.

[12] Id, paragraph 27.

knowledge and culture remains accessible to all citizens.[13] The public's side of the balance also includes "fair dealing," which includes the right to make uses of copyrighted works for research or private study, without fear of unwanted scrutiny from copyright owners.[14] Other provisions recognize the special needs of educational institutions[15], individuals with print disabilities[16] and certain activities of the Crown.[17] Further provisions recognize the importance of public access to works for use in cultural activities,[18] for private non-commercial uses in daily life,[19] and the public value in the dissemination of information.[20]

The adoption of broad anti-circumvention provisions could supplant entirely this careful copyright balance in the digital realm, replacing it with a one-sided legal regime that accommodates only the interests of rights holders. The danger from overly broad anti-circumvention protections is plain: if new provisions are introduced to prohibit the act of circumvention and to expand the range of technological measures under the existing copy-protection provision, rights holders will be able to prohibit what the Copyright Act would otherwise permit.[21] For example, under an overly-broad anti-circumvention provision, a use that would otherwise be permitted as "fair dealing" under the Copyright Act would no longer be permissible where the use required circumvention of a technological protection measure. Suddenly, the vitality of "fair dealing," an important element of the copyright balance, would depend entirely on unilateral decisions by copyright owners.

An overly broad circumvention ban would also effectively undo the exceptions carefully crafted by the legislature and incorporated in the current Copyright Act. For example, section 69 of the Copyright Act specifically provides that a prescribed body can make a copy of, or adapt, a literary or dramatic work to provide persons who have a print disability with a Braille copy or copy otherwise modified for their special needs. However, if a literary work were released in a technologically protected form (such as an Adobe eBook), the exercise of the

---

[13] Copyright Act, sections 51-57 (libraries) and section 90 (archive recording).

[14] Copyright Act, sec. 43. *See also* sec. 42(1) (fair dealing for purpose of criticism or review); 42(2)&(3) (fair dealing for purpose of news reporting).

[15] Copyright Act, sections 44-49.

[16] Copyright Act, section 69 (permitting provision of Braille or otherwise modified copies). *See also* section 89 (provision of subtitled copies of television broadcast or cable programmes to persons who are deaf, hearing-impaired or physically or mentally handicapped).

[17] Copyright Act, sections 58-66.

[18] Copyright Act, section 70 (which permits the public recitation or reading of a reasonable extract of a literary or dramatic work); section 72 (permitting recording of a folk song for inclusion in certain archives);

[19] Copyright Act, section 84 (timeshifting), section 86 (copying of television broadcasts and cable programmes for private use), sections 41 and 82 (incidental copying).

[20] Copyright Act, section 68 (use of recorded spoken words in particular cases) and section 87 (free public display of broadcast or cable programmes), section 88 (reception and retransmission of broadcast and cable content) and section 71 (copying and distribution to the public of abstracts of scientific or technical articles).

[21] *See* Discussion Paper, paragraphs 170-171.

statutory right would likely require both an act of circumvention and the availability of circumvention tools, both of which could be prohibited by a broad circumvention ban.

The role of libraries could also be dramatically altered in a world of technologically protected works. Library patrons may someday find themselves faced with row upon row of pay-per-use works secured by technological protection measures. Broad anti-circumvention provisions would prohibit librarians and patrons from tampering with the restrictions imposed by copyright owners. Absent some right to circumvent, coupled with access to circumvention tools, the library will have been transformed from a repository of public knowledge into a mere rental outlet.

The risk posed by overly-broad circumvention provisions is that copyright law, with its mixture of rights and exceptions, would be supplanted by circumvention law. The copyright balance, instead of being crafted by elected representatives and the judiciary, would be dictated entirely by the private decisions of copyright owners. This result cannot be reconciled with the historical balance reflected by New Zealand copyright law.

Early experience with the broad anti-circumvention provisions enacted in the United States in the Digital Millennium Copyright Act (DMCA) bear out these concerns. The DMCA provisions include broad prohibitions on both acts of circumvention and circumvention devices.[22] In *Universal City Studios v. Reimerdes*, a number of major motion picture companies brought suit against *2600* magazine for publishing a software program, known as DeCSS, that defeats the CSS encryption scheme used to protect movies on DVDs. One defense raised by *2600* turned on the fact that DeCSS could be used to facilitate "fair use," a doctrine long-established in U.S. copyright law. The court rejected this defense, reasoning that the statutory exceptions to copyright had no application to violations of the DMCA's broad anti-circumvention provisions.[23] In effect, the court held that the use of technological protection measures on DVDs supplanted the legislatively-crafted copyright balance set forth in the U.S. Copyright Act.

New digital technologies will certainly pose new challenges for copyright owners. They will also pose challenges for those who otherwise would enjoy the benefit of legislatively-crafted exceptions to the Copyright Act, as they encounter an increasing number of copyrighted works that are protected by technological measures. These challenges, however, do not justify the wholesale abandonment of New Zealand's historical copyright balance in favor of technological controls unilaterally adopted by copyright owners. The balancing approach embraced by the Copyright Act has proven flexible enough to adapt to technological change in the past, and there is no reason to believe that it cannot continue to adapt. As the Discussion Paper recognizes,[24] the introduction of a specific prohibition on circumventing a technological protection measure or tampering with copyright

---

[22] *See* 17 U.S.C. § 1201.

[23] *See Universal City Studios v. Reimerdes,* 111 F.Supp.2d 294, 324 (S.D.N.Y. 2000).

[24] Discussion Paper, paragraphs 43, 53, 168, option v, and 170.

management information would create a new layer of protection for copyright owners. If such new protection is viewed as necessary, it should be subject to at least the same limitations that apply to a copyright owner's other exclusive rights.

B. Freedom of Expression and Scientific Research

Section 14 of the New Zealand Bill of Rights Act 1990 recognizes that "Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form." In considering any proposed circumvention ban, the desire to grant additional protections to copyright owners must be tempered by serious consideration of this fundamental freedom. In particular, the freedoms of scientists and programmers to conduct research and publish their results and opinions may be threatened by overly-broad circumvention prohibitions.

Experience with the DMCA's anti-circumvention provisions in the United States illustrate the threat posed by broad circumvention prohibitions to free expression generally, and to scientific research in particular. Unlike the current New Zealand electronic protection provisions, the DMCA provisions impose a broad prohibition on both acts of circumvention and "any technology, product, service, device, component, or part thereof" that is used to circumvent technological measures that protect copyrighted works.[25] By sweeping an entire category of "technologies" into its "device" ban, the DMCA has effectively created a class of "forbidden knowledge," chilling a variety of publishers and scientists.

The *Universal City Studios v. Reimerdes* case illustrates the chilling effect that overly-broad circumvention prohibitions can have on the freedom of the press. As discussed above, in that case *2600* magazine published the DeCSS computer code as primary source material in the course of its ongoing coverage of the controversy surrounding the DMCA.[26] Notwithstanding the guarantee of freedom of the press secured by the U.S. Constitution's First Amendment, a court permanently enjoined the magazine from publishing the information, and further enjoined it from publishing links to other locations from which the information could be obtained.[27] In effect, the copyright owners in that case obtained a "stop the presses" order against the publication of truthful materials by a news publication covering a matter of public concern. The implications of such an outcome in New Zealand would certainly implicate the freedom of expression provided for by section 14 of the New Zealand Bill of Rights Act.

---

[25] 17 U.S.C. § 1201.

[26] Numerous U.S. courts that have examined whether computer code should come within the U.S. constitutional guarantee of free expression have concluded that such code can be expressive, and that when used expressively, is entitled to protection as speech. *See Junger v. Daley,* 209 F.3d 481, 485 (6th Cir.2000); *Bernstein v. U.S. Dept. of Justice,* 176 F.3d 1132, 1141, *reh'g granted and opinion withdrawn,* 192 F.3d 1308 (9th Cir.1999); *Universal City Studios v. Reimerdes,* 111 F.Supp.2d 294, 326 (S.D.N.Y. 2000); *Bernstein v. U.S. Dept. of State,* 922 F.Supp. 1426, 1436 (N.D.Cal.1996) (First Amendment extends to source code).

[27] *Universal City Studios v. Reimerdes,* 111 F.Supp.2d 294 (S.D.N.Y. 2000).

Copyright owners in the U.S. have also used the DMCA to block the publication of scientific research. In a case that has received considerable media attention, Princeton Professor Edward Felten and a team of researchers have been forced to file suit against a number of music industry entities after being threatened with circumvention liability for trying to present a scholarly paper at an academic conference.[28] Representatives of the Secure Digital Music Initiative (SDMI) claimed that the paper, which explained how Felten's team had defeated watermarking technology meant to protect digital music, was a circumvention technology prohibited by the DMCA.[29] Only after the Felten team filed a lawsuit did SDMI representatives back down from their earlier threats.[30]

Perhaps the most troubling application of the DMCA is the recent criminal prosecution of Russian programmer Dmitry Sklyarov. Sklyarov's employer, a Russian software company known as Elcomsoft, produced and distributed software that can be used to convert digital books from Adobe's eBook format into Adobe's PDF format. In the course of the format conversion, the use restrictions imposed by the eBook format are stripped away. It is undisputed that the Elcomsoft software can be used to facilitate noninfringing uses of eBooks (e.g., fair use excerpting, or to facilitate automated translation into Braille for blind readers or text-to-speech functions). Sklyarov himself was never accused of infringing a copyright, or assisting in the infringing activities of any third party. Nevertheless, for his part in developing the software, U.S. officials arrested him and held him in custody for 3 weeks.[31] He and Elcomsoft were recently indicted by a grand jury in San Jose, California. Based on the charges in the indictment, Sklyarov faces a maximum of 25 years in prison and a fine that could exceed $2 million.[32]

These three cases have cast a pall on a variety of publishers, innovators, scientists, and organizers of scientific conferences. For example, online service providers have begun to censor message board postings that discuss technological protection measures for fear of incurring DMCA liability.[33] Programmers have

---

[28] *See* Declan McCullagh, "Code Breakers Go to Court," *Wired News* (June 6, 2001) <http://www.wired.com/news/mp3/0,1285,44344,00.html>.

[29] *See* Letter from Matthew Oppenheim to Prof. Edward Felten, April 9, 2001 <http://cryptome.org/sdmi-attack.htm>.

[30] *See* Declan McCullagh, "SDMI Code Breaker Speaks Freely," *Wired News*, August 16, 2001 <http://www.wired.com/news/politics/0,1283,46097,00.html>.

[31] *See* Professor Larry Lessig, "Jail Time in the Digital Age," *N.Y. Times* (July 30, 2001) http://www.nytimes.com/2001/07/30/opinion/30LESS.html>; Declan McCullagh, "Hacker Arrest Stirs Protest," *Wired News* (July 19, 2001) <http://www.wired.com/news/politics/0,1283,45342,00.html>; Jennifer 8 Lee, "U.S. Arrests Russian Cryptographer as Copyright Violator," *N.Y. Times*, July 18, 2001.

[32] *See* Brad King & Michelle Delio, "Sklyarov, Boss Plead Not Guilty," *Wired News* (Aug. 30, 2001) <http://www.wired.com/news/politics/0,1283,46396,00.html>.

[33] Lisa M. Bowman, "TiVo Forum Hushes Hacking Discussion," *CNET News* (June 11, 2001) <http://news.cnet.com/news/0-1005-200-6249739.html> (censorship of discussion of video extraction software); John Borland, "Sega Wants to Silence Advice on Hacker Sites," *CNET News* (Oct. 4, 2000) < http://news.cnet.com/news/0-1005-200-2931893.html>.

withdrawn computer security products from the marketplace and have been reticent to reveal security weaknesses in existing digital rights management (DRM) technologies.[34] Sony has used the DMCA to crack down on an innovative potential competitor who offered a software emulator that permits Apple Macintosh users to play Playstation videogames without the use of a Playstation game console.[35] Prominent non-U.S. computer security researchers have expressed concerns regarding travel to the United States in light of the DMCA, and one researcher has refused to release his research for fear of future U.S. prosecution.[36] Russia has gone so far as to issue an official travel advisory warning programmers of the risks of prosecution in the United States under the DMCA's anti-circumvention provisions.[37]

These anecdotes indicate not only an impairment of the freedom of expression and scientific progress, but also suggest that overly broad circumvention protections may backfire, undermining the very science of computer security on which technological protection measures depend. It is by attacking technological protection measures and reporting the results that the science of computer security moves forward. If circumvention prohibitions deter security experts from testing protection systems, these systems will necessarily be less secure in the long run.[38] This outcome disserves not only the interests of science, but also the interests of the copyright owners who rely on protection systems to safeguard their copyrighted works.

C. Proposals

In light of the important public policy concerns discussed above, we propose the following:

Proposal 1: Consider whether any changes to the Copyright Act are required by the WIPO Copyright Treaty.

The EFF urges the Ministry to consider whether the existing provisions of the Copyright Act are sufficient to satisfy the requirements of Article 11 of the WIPO Copyright Treaty. The exclusive rights granted to copyright owners by the Copyright Act may already provide the "adequate legal protection and effective legal remedies" required by the Treaty. For example, most illegitimate circumvention activity will ultimately result in an unauthorized reproduction, and hence be subject to traditional copyright sanctions. Further, copyright holders' interests are protected by the existing copy-protection provisions in section 226, which prohibits the making, importing, selling and distributing of devices and

---

[34] Robert Lemos, "Security Workers: Copyright Law Stifles," *CNET News* (Sept. 6, 2001).

[35] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Technology L.J. 519, 556 (1999), available at <http://www.sims.berkeley.edu/~pam/papers.html>.

[36] Lisa M. Bowman, "Researchers Weight Publication, Prosecution," *CNET News* (August 15, 2001) <http://news.cnet.com/news/0-1005-200-6886574.html>.

[37] Jennifer Lee, "Travel Advisory for Russian Programmers," *N.Y. Times* (Sept. 10, 2001).

[38] National Research Council, The Digital Dilemma: Intellectual Property in the Digital Age (2000), at 311-30 (Appendix G describing methods of cryptology research).

means (which as the Discussion Paper notes,[39] appears to cover software) specifically designed to circumvent copy-protection, and also the publication of an information intended to enable or assist persons to circumvent such copy-protection.

For the reasons noted above, attempts to satisfy the requirements of the WIPO Copyright Treaties through new, broadened circumventions prohibitions should be viewed as a last resort, acceptable only if "adequate protection" cannot be secured for copyright owners through adjustment of the exclusive rights traditionally granted by the Copyright Act. To the extent the Ministry believes some additional protections may be required, the Ministry should also consider whether any residual concerns would be better addressed by separate legislation aimed at computer tampering, rather than amendments to the Copyright Act.

Proposal 2: Any circumvention prohibition should be limited to circumventions undertaken for the purpose of infringement.

In the event the Ministry concludes that WIPO Treaties implementing legislation is necessary, and that such legislation should take the form of an anti-circumvention provision in the Copyright Act, we propose that such a provision be made expressly subject to the exceptions contained in the Copyright Act. This goal can be accomplished by prohibiting the circumvention of technological protection measures for infringing purposes, where such measures have been adopted to restrict acts not permitted by the Copyright Act.[40]

An anti-circumvention provision of this sort would accommodate the principle of balance embodied in the Copyright Act. For example, an act of circumvention would not be prohibited where undertaken for the purpose of engaging in activities permitted under the Act, including those activities authorized by the statutory exceptions applicable to "fair dealing," libraries, educational institutions, museums, and organizations that assist the perceptually disabled.[41]

Proposal 3: Any circumvention prohibition should include a "legitimate purpose" exception.

Any circumvention prohibition should also include an express exception permitting circumvention where undertaken for legitimate purposes. In arguing for prohibitions on acts of circumvention and circumvention devices, the copyright industries have understandably focused on movies, music, books and other traditional objects of copyright law. The use of technological protections in the digital realm, however, implicates public policy concerns reaching far beyond those addressed by the Copyright Act. Trade secret owners, privacy-seeking individuals, and network administrators, to name a few, are already deploying technological protection measures. Email traffic, for example, is entitled to

[39] Discussion Paper, paragraphs 157-158.

[40] This approach was proposed during the U.S. consideration of the DMCA. See H.R. 3048, 105th Cong. (introduced by Rep. Boucher and Campbell, Nov. 13, 1997).

[41] Some of these concerns were discussed in the Discussion Paper at paragraph 170.

protection under the Copyright Act as literary works. Assuming that privacy-seeking individuals begin to encrypt their email, would a network administrator be entitled to circumvent such encryption to examine their contents? What if the examination were limited to seeking out harmful computer viruses attached to email messages? These questions cannot be answered solely by the application of copyright law principles, but necessarily involve a consideration of privacy, computer security, and other public policies.

As technological protection measures are deployed in an increasing number of unforeseen contexts, the Copyright Act will increasingly become an ill-fitting straight-jacket for courts and policy-makers. Accordingly, a "legitimate purpose" exception will be necessary if the judiciary is to retain the flexibility to consider public policy issues beyond those addressed in the Copyright Act.[42] It is bad enough that circumvention provisions might supplant the copyright balance; without a "legitimate purposes" exception, circumvention provisions threaten to supplant other carefully crafted legal regimes, as well.

Proposal 4: Any circumvention prohibition must include protections for "innocent circumventors."

In order to offset the chilling effect created by uncertain circumvention rules, any monetary or criminal penalties for circumvention should be reserved for cases where the unlawfulness of the activity in question is clearly established. Defendants operating in good faith on uncertain legal terrain ("innocent circumventors") should face, at most, only injunctive penalties.

Rules that are unclear may have a chilling effect on legitimate uses of works that are nonetheless permitted under copyright law. As a result, circumvention provisions should be drafted so as to give clear notice to citizens regarding which activities are forbidden. However, because the circumvention provisions are likely to have application in areas unforeseeable today, some uncertainty regarding the precise scope of any circumvention prohibition will likely persist. A limitation of liability for "innocent circumventors" would reduce the chilling effect of such uncertainty. It would also decrease the chilling effect of over-reaching threats by copyright owners (such as the threats leveled at Professor Felten and his research team in the U.S.). This, in turn, will increase the likelihood that novel cases will be resolved by the courts, and clarifying the law for the future.

Courts could look at numerous factors in determining whether a circumventor had undertaken circumvention activities, later determined to be unlawful, under a good faith belief that they were lawful. Factors could include whether previous judicial or regulatory pronouncements clearly established that the activity in question constituted unlawful circumvention, and whether the circumventor had reasonably relied on the opinion of counsel.

---

[42] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Technology L.J. 519, 543-46 (1999) (discussing need for "legitimate purposes" exception), available at <http://www.sims.berkeley.edu/~pam/papers.html>.

Proposal 5: The knowledge requirement contained in current Section 226(2) of the Copyright Act should be retained unchanged.

Section 226 of New Zealand's Copyright Act includes a limited prohibition on devices designed to circumvent copy-protection. The Discussion Paper invites comment on proposals to alter the knowledge element contained in Section 226 of the Copyright Act. EFF urges the Ministry to retain unchanged the current subjective knowledge element.[43]

As discussed above, if technological protection measures are not to displace the copyright bargain altogether, circumvention of protection measures (including copy-protections) for noninfringing and other legitimate purposes must be permitted. The corollary of this principle is that the public must have access to information and devices that will enable these legitimate circumvention activities. Technology vendors, however, will not invest in creating these devices if they face liability under an uncertain objective knowledge standard.

As the Discussion Paper recognizes,[44] the proposed alteration of the knowledge element contained in Section 226 is intended to prevent the making or distribution of "multiple use" tools that enable legitimate as well as illegitimate uses. Interfering with the development of technology that is capable of perfectly legitimate uses, however, is not the proper role of the Copyright Act. When a vendor intentionally facilitates copyright infringement by supplying devices or information that circumvents copy-protection, Section 226 properly holds him accountable. However, where a vendor makes a device that has multiple uses, including circumvention of copy-protection for legitimate, non-infringing purposes, no liability should attach. Were the rule otherwise, innovation in technology industry would be chilled.

The need to protect legitimate scientific research also counsels for the retention of Section 226's current subjective knowledge element. Section 226 currently includes not only devices, but also publication of "information" relating to circumvention of copy-protection. As a result, the publication of scientific research (such as the research of Professor Felten's research team, discussed above) could potentially fall within its scope.

Under the current Section 226, scientists and journal publishers can rest easy so long as they did not intend to facilitate infringement by third parties. If the knowledge element were replaced with a "should have known" standard, scientific researchers would face the same uncertainties that they face in the U.S. under the DMCA, uncertainties that have already resulted in a chill on research and publication.

---

[43] A person violates Section 226 only if he sells a circumvention device "knowing or having reason to believe that the devices, means, or information will be used to make infringing copies." *See* Section 226(2).

[44] Discussion Paper, paragraph 159.

V. Intermediary liability

Question 11 in the Discussion Paper asks:

a. Should ISPs be liable for copyright infringement in relation to the operation of Internet services?

b. If so, should they be liable for copyright infringement in relation to:

- temporary or incidental copies that are made without the permission of copyright owners in the provision of Internet services to subscribers; and/or
- infringing copies made by subscribers that are distributed using an ISP's services in all circumstances; or
- only for infringing copies made by subscribers that are distributed using the ISP's services in some circumstances?

c. If ISPs should only be liable for copyright infringement in relation to the activities of their subscribers in some circumstances:

- what should those circumstances be; and
- should liability be excused where ISPs have undertaken certain measures, for example to guard against the use of their services for activities that amount to copyright infringement or to restrict (or "take down") access to websites that contain infringing material where this comes to their attention?

The Discussion Paper discusses several approaches aimed at addressing the question of copyright liability for network intermediaries, such as Internet service providers (ISPs). We endorse the Ministry's efforts to craft rules that will clarify the murky state of the law regarding the copyright responsibilities of network intermediaries.

However, in addition to balancing the interests of rights holders and the ISP community, we believe that any solution to the question of ISP liability must also take the interests of the public into account. In particular, any copyright liability solution designed to assist network intermediaries should satisfy the following criteria: (1) it should create a regime that respects the privacy and free expression rights of Internet users; and (2) it should preserve and foster the end-to-end architecture that has made the Internet such an successful platform for innovation and competition.

A. Privacy and Free Expression

The Internet affords individuals and institutions an unprecedented opportunity for free expression and exchange of information at a relatively low cost. Numerous network intermediaries, however, act as gatekeepers to the fora for communication online. For example, most Internet users rely on an ISP for network access, and may rely on a variety of other service providers for web hosting, instant messenging, message boards, email and access to newsgroups. Accordingly, although the Internet provides remarkable opportunities for

expression and communication, an Internet user's ability to partake of those opportunities depends on her relationship to a variety of network intermediaries. Network intermediaries are also in a position to directly influence the level of privacy that an Internet user enjoys. ISPs generally know the identities of their subscribers and have the ability to monitor all incoming and outgoing network traffic.[45] In light of these realities, it is crucial that any regime addressing the copyright liability of ISPs provide incentives that reinforce, rather than undermine, the free expression and privacy rights of Internet users.[46]

B. The End-to-End Internet Architecture

The Internet has not only created unprecedented new opportunities for inexpensive expression and sharing of information, but has also proven to be a remarkable incubator for technological innovation. Any regime aimed at limiting the copyright liabilities of network intermediaries should, to the extent possible, preserve and foster the rapid innovation that has characterized the Internet thus far.

Stanford Law School's Professor Larry Lessig has written extensively regarding the way in which one architectural feature of the Internet is largely responsible for its innovative character.[47] Professor Lessig refers to this feature as the "end-to-end" principle—the notion that the network itself should remain "stupid" (i.e., unable to discriminate between different forms of network traffic), while "intelligence" should be distributed to its "ends" (i.e., on the computers of end-users). Although this architectural principle was originally adopted for technical reasons, it soon became clear that it also entailed certain social and economic consequences. For example, the end-to-end principle by its nature fosters free expression, as it limits the extent to which network owners can censor content passing through its wires.

In addition, the end-to-end principle, by enforcing competitive neutrality, has profound consequences for innovation. Anyone with a new idea can rely on the fact that the network will treat her applications the same way that it treats competing applications introduced by the largest corporations. In contrast to the communications infrastructures that preceded it, such as telephone and cable television, the end-to-end architecture of the Internet creates an "innovation

---

[45] Users can, by employing cryptography, proxy servers, and creating secure "tunnels" between computers, take steps to make surveillance of their communications more difficult. Nevertheless, just as we do not place the burden on telephone users to stop eavesdropping by the telephone company, we should also protect the privacy of the less sophisticated Internet user.

[46] Limitations of liability for copyright infringement should also extend equally to any indirect liability for circumvention that may arise as a result of subscriber activities.

[47] *See* Larry Lessig, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (forthcoming October 2001); Larry Lessig, "Innovation, Regulation, and the Internet," *The American Prospect,* v. 11, issue 10 (March 27-April 10, 2000), available at <http://www.prospect.org/print-friendly/print/V11/10/lessig-l.html>; Larry Lessig & Mark Lemley, In re Transfer of Control of Licenses from MediaOne Group, Inc. to AT&T Corp. (testimony before the FCC regarding open access), available at <http://cyberlaw.stanford.edu/lessig/content/testimony/cable/lem-lesd.pdf>.

commons," an open, level playing field that permits innovators to compete on equal footing. The result has been an enormous explosion of innovative uses for the Internet.

Any limitation of liability that may be crafted for network intermediaries should be careful to foster, rather than undermine, the end-to-end principle. In particular, any legal structures that would place ISPs and other network intermediaries in a privileged position vis-a-vis other Internet users would appear to violate the end-to-end principle. Similarly, any legal structure that creates incentives for ISPs to monitor and discriminate between different types of content would seem to threaten the innovation commons.

C. Proposals

Proposal 1: Amend the Copyright Act to make it clear that temporary and incidental digital copies do not implicate the reproduction right.

For the reasons discussed at length above, EFF recommends that the Ministry exclude temporary and incidental digital copies from the scope of the reproduction right. Such a clarification will reduce (although perhaps not eliminate) the need for special copyright exceptions for network intermediaries. A major concern for network intermediaries is that they might be held strictly liable for copyright infringement based on the temporary and incidental copies (whether in RAM or in temporary disk caches) that are automatically transmitted through their computer systems by their subscribers. A clear rejection of the RAM copies doctrine would address this concern.

Proposal 2: No affirmative obligation to monitor Internet users.

In light of the principles discussed above, any limitation of liability for ISPs should not be conditioned on an affirmative obligation to monitor the activity of its users. Not only would such a system be burdensome on ISPs, it would violate the reasonable expectations of Internet users. Just as we do not expect that our telephone calls will be monitored by the telephone company, nor that our mail will be read by the letter carrier, so to should Internet users be able to rest easy in the knowledge that their every message is not being monitored for copyright infringement. In addition, a regime that requires monitoring would require that ISPs build a monitoring infrastructure that would discriminate among different users and content types. Such an infrastructure would undermine the end-to-end nature of the Internet.

Proposal 3: Notice and take-down should be limited to materials residing on the ISP's own computer systems.

Any notice and take-down regime should be limited to materials hosted or cached on the ISP’s own computing equipment, and should not apply to materials stored on an Internet user’s own computer. The combination of “always on” broadband Internet connectivity and increasingly powerful personal computers will likely result in an increase in the number of Internet users who host their own Internet content. This development, in turn, is likely to result in a more diverse, decentralized ecosystem of affordable Internet technologies and content, and

should be encouraged. To the extent an ISP is providing only simple network connectivity, rather than storing content on behalf of its subscribers, copyright law should not create an incentive for it to monitor or intrude into the computer systems of its subscribers.

Proposal 4: Notice and take-down procedures should reasonably preserve user anonymity.

Anonymous speech has long played a crucial role in fostering free expression. From the pseudonyms used by the authors of the Federalist Papers in the colonial United States to the anonymous criticisms of Chinese communist rulers published in world newspapers in the 1980s, authors of politically sensitive publications have long relied on anonymity to protect their identities and sometimes even their lives. Similarly, anonymity protects "whistleblowers" reporting on government or business abuses or violations of law. A cloak of anonymity may also be crucial for victims of domestic violence or child abuse, and others who want to discuss sensitive, personal information without fear of reprisal or exposure. All of these situations occur daily on the Internet and all of them are worthy of some modicum of protection. This is not to say that Internet users are entitled to anonymity in all circumstances. But, by the same token, the public's right to speak anonymously ought not be overlooked on the Internet.

In the U.S., the ability of ISPs to unmask anonymous Internet users has proven to be a weakness in the protection of freedom of expression. Companies angered by critical comments on public message boards, for example, have found that they can easily file a civil suit, issue a subpoena to the ISP hosting the discussion, and obtain the identity of the speaker. These subpoenas have effectively stifled discussion in many public forums. The situation is even worse where allegations of copyright infringement are concerned. Under the DMCA's safe harbor provisions, a copyright owner is entitled to issue a subpoena to a service provider in order to obtain the identity of an anonymous Internet user. This subpoena can be issued even where the copyright owner has no intention of filing an infringement action—a take-down notice is enough to entitle a copyright owner to a subpoena. A service provider that receives such a subpoena, moreover, is not under any obligation to inform the subscriber that identifying information has been released.

We recommend that the Ministry omit subpoena provisions from any ISP safe harbor provisions that it may recommend. A notice and take-down procedure adequately provides to copyright owners the equivalent of an automatic injunction against alleged infringers. If a copyright owner requires additional information regarding an anonymous Internet infringer, the owner can file suit and avail itself of the ordinary judicial process, and require that the ISP disclose identifying information. There is no reason that copyright owners should be accorded a special right to breach the legitimate anonymity rights of Internet users upon the submission of a mere allegation of infringement. In addition, we recommend that an obligation be imposed on network intermediaries (including ISPs) to notify a subscriber when his or her identity has been requested by a third party.

Proposal 5: Any notice and take-down process should include a non-waivable affirmative counter-notice provision in favor of Internet users.

Any notice and take-down regime should include a non-waivable counter-notice provision in favor of Internet users. In the absence of such a provision, the free expression rights of individuals are likely to be at the mercy of unscrupulous copyright owners intent on stifling critical speech rather than protecting their works. For example, a corporate copyright owner intent on silencing a critical web site might deliver a take-down notice to the hosting ISP. In order to preserve its eligibility for the copyright liability safe harbor, the ISP will likely respond by taking down the site. As a result, a naked allegation would effectively entitle a copyright owner to the equivalent of permanent injunctive relief. The site owner, meanwhile, would effectively have been silenced without the benefit of any judicial process at all.[48] This concern is not merely hypothetical—there have been reported accounts in the U.S. of the DMCA's notice and take-down provisions being used to shut down web sites under circumstances that suggest that the copyright owner was responding to the site's critical message, rather than any infringement.[49]

In order to prevent abuses of the notice and take-down process, a counter-notification process should be put in place for users who want to contest a take-down notice. Under such a system, a subscriber would be notified of the ISP's receipt of a take-down notice, and would have the option, within a short time, of submitting a counter-notice under penalty of perjury disputing the allegation of copyright infringement. If the ISP receives the counter-notice within the relevant counter-notice period, it would forward a copy to the complaining party and would be relieved from any take-down obligation. At that point, the complaining party would be free to file suit against the subscriber directly. In order to further deter abusive take-down notices, a subscriber should be entitled to recover attorneys fees and costs in any case where a court concludes that the original take-down notice was sent in bad faith.

In the U.S., the DMCA provides for a counter-notice procedure similar to the one detailed above. The U.S. provision, however, suffers from two serious flaws. First, it does not address whether an ISP is required to implement the counter-notice procedure, or whether it can instead avoid the obligation by obtaining a contractual waiver from its subscribers as part of its standard "terms of service" agreement. It appears that most ISPs in the U.S. include provisions in their contractual agreements that render the counter-notice provisions of the DMCA safe harbors optional, at best. Obviously, to the extent the implementation of a counter-notification procedure might increase costs to an ISP, the ISP may prefer to obtain contractual waivers in place of a counter-notice regime. Such an outcome, however, would render the counter-notice provisions an empty promise.

---

[48] The site operator could, of course, transfer the web site to another ISP. There is no guarantee, however, that the copyright owner would not deliver a take-down notice to this ISP as well.

[49] *See* Katharine Mieszkowski, "No Free Speech for Animal Rights Web Sites," *Salon* (Aug. 31, 2001) (British medical research company uses DMCA notices to silence critical animal rights web sites in the U.S.) <http://www.salon.com/tech/log/2001/08/31/dmca_animals/index.html>.

Accordingly, any contractual efforts by ISPs that purport to waive the counter-notification process should be expressly pre-empted.

The second weakness of the DMCA's counter-notice provisions is that it provides that a take-down is effective immediately upon notice, and remains effective for a 10-day period even in the face of a counter-notice. This arrangement transforms a simple allegation of infringement into an automatic gag order, an outcome that fails to protect the free speech interests of the web site publisher. A 10-day gag order, moreover, renders the counter-notice process substantially less useful to a subscriber, since moving the disputed content to another ISP may provide a more timely solution. Thus, instead of deterring abusive take-down notices and the resolution of disputed infringement claims by judicial inquiry, the U.S. counter-notice provisions encourage an inefficient game of whack-a-mole, as the subscriber shuttles from ISP to ISP in order to elude the draconian effect of abusive take-down notices.

Proposal 6: Anyone performing intermediary functions, including the transmission and routing of network transmissions, hosting or caching, should be entitled to whatever safe harbor is ultimately adopted.

Any limitation of liability should extend equally to anyone performing the functions of a network intermediary.

The rollout of "always on" broadband Internet connectivity, along with increasingly powerful PC hardware and software, has resulted in a recent renaissance for the "end-to-end" principles that have spurred Internet growth and innovation. Already, the sorts of activities once reserved for sophisticated systems administrators and online service providers (such as hosting a web site, having remote access to your home PC while traveling, and providing web services such as email to other Internet users) have become available to the average home Internet user.[50] Dramatically more "intelligence" is becoming available at the "ends" of the network. If this trend is permitted to flourish, a new wave of innovation is likely to emerge, as average Internet users become better able to participate in the networked world as a "peer," contributing services to the Internet community as well as consuming them. For example, individual Internet users have begun organizing grassroots wireless networks built on inexpensive 802.11b technology.[51] When these individuals provide network connectivity to their community, they are acting in exactly the same capacity as an ISP, and should be entitled to the same legal protections from copyright liability.

Restricting a limitation of liability to a category of incumbent ISPs, while withholding these same advantages from average Internet users who will increasingly be able to perform ISP functions, is likely to severely compromise

---

[50] Apple's recently introduced MacIntosh operating system, OS X, now includes Apache web server software, a powerful server once the province of sophisticated server operators. This software, which runs some of the largest e-commerce sites in the world, now ships standard on every MacIntosh, including the colorful, entry-level iMac.

[51] *See* Damien Cave, "Unchaining the Net," *Salon* (Dec. 1, 2000) <http://www.salon.com/tech/feature/2000/12/01/wireless_ethernet/index.html>.

end-to-end architecture principles. We urge the Ministry to ensure that all Internet actors, whether large ISPs or individual Internet users, will play on a level copyright playing field when providing identical services to third parties.

****

Thank you for your consideration.

Fred von Lohmann
Senior Intellectual Property Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
U.S.A.
fred@eff.org
+1 (415) 436-9333 x123