Setting the Record Straight: 32 Questions and Answers on C-32's Digital Lock Provisions

Professor Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa, Faculty of Law

June 2010

The C-32 Approach

1. Isn't the C-32 digital lock approach simply the required implementation to comply with the WIPO Internet treaties?
2. Penalties are reduced for individuals who circumvent for personal purposes. Doesn't this solve the problem?
3. The digital lock provisions in C-32 appear to distinguish between copy controls and access controls. Isn't that enough to address concerns about the bill's impact on fair dealing?
4. Are the digital lock provisions in C-32 constitutional?
5. Is it true that C-32 requires teachers and students to destroy some digital lessons 30 days after the course concludes?
6. Is it true that C-32 requires librarians to ensure that inter-library digital loans self-destruct within five days of first use?
7. The U.S. has a regular review of new exceptions every three years. Does Canada plan the same?

C-32's Circumvention Exceptions

8. Bill C-32 contains circumvention exceptions for encryption research and security testing. Doesn't that address the research concerns?
9. Bill C-32 contains a circumvention exception for privacy. Doesn't that address the privacy concerns?
10. Bill C-32 contains a circumvention exception for the visually impaired. Doesn't that address those access concerns?
11. Bill C-32 contains a circumvention exception for interoperability. Doesn't that address those concerns?

The Missing Exceptions

12. Does C-32 include "authorized circumventers" as is used in New Zealand to facilitate legal circumventions?
13. Are companies required to unlock locked content for legal purposes under C-32?
14. Does C-32 include an exception for non-infringing access, such as accessing DVDs from other regions?
15. Does C-32 include a circumvention exception for personal uses?
16. Does C-32 include a circumvention exception for digital archiving?
17. Does C-32 include a circumvention exception to protect minors?
18. Does C-32 include a circumvention exception for filtering software programs?
19. Does C-32 include an exception for circumventing digital locks that become obsolete or broken?
20. Does C-32 include an exception for court cases, laws, and government documents?
21. Bill C-32's digital lock provisions apply to copyrighted works. Does that mean that public domain (ie. out-of-copyright) works are not affected?

The Consumer Provisions

22. Bill C-32 purports to allow consumer to legally shift music from CDs to their iPods or other devices. Do they lose that right if there are digital locks on their CD?
23. Does Bill C-32 allow consumers to make legal backup copies of most commercial DVDs?
24. Does Bill C-32 allow consumers to shift content from a DVD to a portable video player such as an iPad?
25. C-32 purports to allow consumer to legally record television shows, yet cable companies are increasingly inserting anti-copying technologies into some broadcasts? Does C-32 allow for those programs to be recorded?
26. C-32 includes an exception for unlocking cellphones. Isn't that a positive new development?
27. Does C-32 require businesses to notify consumers about the presence of digital locks?
28. Isn't there an "analog hole" that would allow someone to record a DVD without circumventing the digital lock?

Business Considerations

29. Isn't this just a matter of consumer choice? If consumers don't want products with digital locks, no one is forcing them to purchase them?
30. Won't the digital lock provisions help bring new businesses to Canada like Hulu.com?
31. Are the concerns associated with digital lock provisions in the United States legitimate? What issues have arisen in the U.S. under the DMCA?
32. If these digital lock provisions are too restrictive, what compromises are available?

The digital lock provisions have quickly emerged as the most contentious part of Bill C-32, the new copyright bill. This comes as little surprise, given the decision to bring back the digital lock approach from C-61 virtually unchanged. The mounting public concern with the digital lock provisions (many supporters of the bill have expressed serious misgivings about the digital lock component) has led to many questions as well as attempts to characterize public concerns as myths. In effort to set the record straight, I have compiled 32 questions and answers about the digital lock provisions found in C-32. The result is quite lengthy, so I will divide the issues into five separate posts over the next five days: (1) general questions about the C-32 approach; (2) the exceptions in C-32; (3) the missing exceptions; (4) the consumer provisions; and (5) the business provisions. For those that want it all in a single package, I've posted the full series as PDF download.

Before getting into the 32 questions, it is worth answering the most basic question - what are anti-circumvention or digital lock provisions? The short answer is that they are provisions that grant legal protection to technological protection measures (TPMs). In plainer English, traditional copyright law grants creators a basket of exclusive rights in their work. TPMs or digital locks (such as copy-controls on CDs, DVDs, or e-books) effectively provide a second layer of protection by making it difficult for most people to copy or sometimes access works in digital format. Anti-circumvention legislation creates a third layer of protection by making it an infringement to simply pick or break the digital lock (in fact, it even goes further by making it an infringement to make available tools or devices that can be used to pick the digital lock). Under the Bill C-32, it would be an infringement to circumvent a TPM even if the intended use of the underlying work would not constitute traditional copyright infringement.

The C-32 Approach

Isn't the C-32 digital lock approach simply the required implementation to comply with the WIPO Internet treaties?

No. The WIPO Internet treaties require that countries provide legal protection for digital locks, but leave considerable flexiblity in how this requirement is implemented. The U.S. has promoted its particular approach (as found in the DMCA and now in C-32) since before the treaty was even concluded, yet consensus in establishing the treaty was only achieved by adopting far more flexible language.

On the issue of legal protection for digital locks, the treaties require countries to provide "adequate legal protection and effective legal remedies" for technological protection measures. The U.S. initially proposed:

(1) Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the

device or service will be used for, or in the course of, the exercise of rights provided under this Treaty that is not authorized by the rightholder or the law.

(2) Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).

This language did not achieve consensus support with many proposed changes. A compromise position was ultimately reached using the "to provide adequate legal protection and effective legal remedies" standard. Not only does this language not explicitly require a ban on the distribution or manufacture of circumvention devices (ie. software programs used to circumvent digital locks), it is quite obvious that the intent of the negotiating parties was to provide flexibility to avoid such an outcome.

U.S. law professor Pam Samuelson chronicles precisely what happened in her 1997 law review article, The U.S. Digital Agenda at the World Intellectual Property Organization:

At the diplomatic conference, there was little support for the Committee's proposed language on circumvention technologies. Some countries opposed inclusion of any anti-circumvention provision in the treaty. Others proposed a "sole purpose" or "sole intended purpose" standard for regulating circumvention technologies. Some wanted an explicit statement that carved out circumvention for fair use and public domain materials. The E.U. offered a proposal that would have required contracting parties to adopt adequate and effective legal measures to regulate devices and services intended for technology-defeating purposes.

Facing the prospect of little support for its proposal or the Committee's draft anti-circumvention provision, the U.S. delegation was in the uncomfortable position of trying to find a national delegation to introduce a compromise provision brokered by U.S. industry groups that would simply have required contracting parties to have adequate and effective legal protection against circumvention technologies and services. In the end, such a delegation was found, and the final treaty embodied this sort of provision as Article 11.

This was, of course, a far cry from the provision that the U.S. had initially promoted. Still, it was an accomplishment to get any provision in the final treaty on this issue. The inclusion of terms like "adequate" and "effective" protection in the treaty will mean that U.S. firms will be able to challenge national regulations that they deem deficient.

In the years since the treaty was concluded, the U.S. and a handful of supporters have argued strenuously that countries should ignore the compromise language and adopt the U.S. approach. Yet some countries have rejected that advice - Canada's own bill C-60 adopted a flexible approach, as does the most recent copyright reform bill from India. New Zealand's law features many differences from the U.S. model and dozens of countries have added exceptions and changes to the basic U.S. approach. In fact, the reality is that of the 88 states that have ratified the WIPO Internet treaties, fewer than half that have adopted the U.S. model.

When the U.S. was in the process of implementing the WIPO Internet treaties into what became the DMCA, officials acknowledged the flexibility that exists in the treaty. Marybeth Peters, the U.S. Register of Copyrights, said in testimony before the House Judiciary Committee on 16 Sept. 1997:

"Some have urged that the legislation not address the provision of products or services, but focus solely on acts of circumvention. They state that the treaties do not require such coverage, and argue that devices themselves are neutral, and can be used for either legitimate or illegitimate purposes. It is true that the treaties do not specifically refer to the provision of products or services, but merely require adequate protection and effective remedies against circumvention. As discussed above, however, the treaty language gives leeway to member countries to determine what protection is appropriate, with the question being whether it is adequate and effective."

And, later in the same testimony, the clearest statement: "the treaties do not specifically require protection for access controls in themselves."

Applied to C-32, the current bill goes far beyond what is strictly required to be compliant with the WIPO Internet treaties. A more flexible, balanced implementation would still be WIPO compliant, provide protection for businesses seeking to use DRM, and maintain the copyright balance.

Penalties are reduced for individuals who circumvent for personal purposes. Doesn't this solve the problem?

No. First, claims that reduced penalties removes the impediment to Canadians circumventing digital locks for personal purposes assumes that concern for statutory damages is the primary motivator for a particular action. I disagree. In the education world, teachers and students will not break the lock because academic guidelines will make it clear that they can't. Similarly, research will also be stifled in the same way since researchers sign ethics documents when they apply for grants that their research plan is compliant with all laws. They can't sign the document in this situation, regardless of the likelihood of damages.

Second, C-32 also makes the distribution and marketing of devices (ie. software) used to circumvent illegal. This suggests it will be more difficult to get those tools (and perhaps risky), so the notion that people will circumvent in light of lower penalties is undermined by the underground nature of being able to do so.

Third, from a bigger picture perspective, rights holders have been complaining for years that the public does not respect copyright. This bill is an attempt to revive respect for copyright by having the law better reflect current norms (and therefore make it more respectable). However, you do not build respect for copyright by creating provisions that outlaw something but have the government indirectly say it is acceptable to violate its

new rule. C-32 should craft rules that generate support and acceptance in the public and thereby build support and acceptance for copyright more broadly.

The digital lock provisions in C-32 appear to distinguish between copy controls and access controls. Isn't that enough to address concerns about the bill's impact on fair dealing?

No. The distinction in one section of Bill C-32, which was also contained in C-61, does not address the fair dealing concerns in the bill. First, the distinction between access controls (access to the work itself) and copy controls (copying the work) is a distinction without a difference for many of today's TPMs. The digital locks used by Amazon or Apple on e-books or the TPMs on DVDs are both access and copy controls. In order to effectively circumvent to be able to copy, you have to circumvent access. The locks often permit access for some uses, but not others. In other words, Canadians will often need to circumvent access to get to the copying and therefore will still be infringing under the law.

Moreover, even if a consumer could distinguish between access and copy controls, the tools themselves that would be used to circumvent for copy purposes cannot be lawfully marketed or distributed. The notion that it is permissible to circumvent for copying but that the software needed to do so can't be distributed demonstrates how this distinction really makes no real difference.

Finally, many of the other new exceptions - format shifting, time shifting, and backup copies - are covered by all digital locks, including both access and copy controls.

Are the digital lock provisions in C-32 constitutional?

Possibly not. The constitutionality of digital lock legislation has been examined in two articles by Canadian law professors. Both conclude that the provisions are constitutionally suspect if they do not contain a clear link to conventional copyright law. Their reasoning is that the constitution grants jurisdiction over copyright to the federal government, but jurisdiction over property rights is a provincial matter. Digital lock legislation that is consistent with existing copyright law - ie. one that factors in existing exceptions - is more clearly a matter of copyright. The C-32 provisions are arguably far more about property rights since the provisions may be contained in the Copyright Act, but they are focused primarily on the rights associated with personal property.

My colleague Jeremy deBeer conducted a detailed analysis of this issue in his article, *Constitutional Jurisdiction over Paracopyright Laws*. Many of his arguments were echoed in a 2009 article published in the Journal of Information Law and Technology by Professor Emir Aly Crowne-Mohammed and Yonatan Rozenszajn, both from the University of Windsor, which concluded that the anti-circumvention provisions found in Bill C-61 were unconstitutional. The authors argue that the DRM provisions were "a poorly veiled attempt by the Government to strengthen the contractual rights available to copyright owners, in the guise of copyright reform and the implementation of Canada's

international obligations. Future iterations of Bill C-61 that do not take the fair dealing provisions of the Copyright Act (and the overall scheme of the Act) into account would also likely to fail constitutional scrutiny."

Is it true that C-32 requires teachers and students to destroy some digital lessons 30 days after the course concludes?

Yes. Bill C-32 requires teachers that utilize a new educational exemption to destroy the lessons that they have created for their courses with one month of the conclusion of the course. Teachers must recreate the lessons each year, which obviously establishes a strong incentive to run as far away as possible from these new "rights."

Is it true that C-32 requires librarians to ensure that inter-library digital loans self-destruct within five days of first use?

Yes. While moving toward digital interlibrary loans has obvious advantages (speed and cost being at the top of the list), Bill C-32 forces libraries to implement DRM-based solutions. The requirements for legal digital interlibrary loans include limits on further copying and distribution that go far beyond what is necessary (they are presumably a response to the unlikely scenario that only a single Canadian library will purchase the copy of a work and use digital distribution to cover the rest of the country). Even worse is the requirement to destroy the digital copy within five days of first use. There are no similar requirements for paper-based copies of works and it makes no sense to force libraries to install DRM protections on digital copies to create time-limited uses.

The U.S. has a regular review of new exceptions every three years. Does Canada plan the same?

No. The U.S. DMCA experience leaves little doubt that the introduction of anti-circumvention legislation will create some unintended consequences. No matter how long the list of circumvention rights and other precautionary measures, it is impossible to identify all future concerns associated with anti-circumvention legislation. The U.S. DMCA addresses this by establishing a flawed tri-annual review process. The system has not worked well, creating a formidable barrier to new exceptions and long delays to address emerging concerns.

As bad as the U.S. system is, the proposed Canadian system under Bill C-32 is worse since there is no mandated review of the exceptions at all. Instead, Canada gets a flexible process that will allow the government to consider new exceptions if and when it sees fit. In other words, the same government that brought you the Canadian DMCA will decide if there is a need to add any exceptions. If Canada establishes anti-circumvention legislation, it should also establish an impartial process that will enable concerned parties to raise potential new circumvention rights without excessive delay. The process must be fast, cheap, and easily accessible to all Canadians. Bill C-32 establishes the criteria for the introduction of new circumvention rights but fails to implement an administrative structure to conduct the reviews.

C-32's Circumvention Exceptions

Bill C-32 contains circumvention exceptions for encryption research and security testing. Doesn't that address the research concerns?

No. The impact of the anti-circumvention provisions on the research community extends far beyond just encryption research and security testing. Bill C-32's exception is the same as that used in Bill C-61. When C-61 was introduced, I met with several University of Ottawa researchers engaged in fields as diverse as biblical scholarship and engineering. Their common thread was that their research plans would be stymied by Bill C-61. Researchers that need to circumvent in order to access content for media criticism, search technologies, network content distribution, etc. will all find themselves unable to conduct their research. Those that argue that Bill C-32 is unenforceable have never had their work subjected to an ethics review that invariably includes an examination of the legality of the methodology. If the work fails the review, there will be no grant funding and the research simply stops. The exceptions for encryption research and security testing are needed, however, the Canadian approach to exceptions has been to simply mirror the U.S. DMCA list. A general research exception is essential if Canadian researchers are to be able to continue their work.

Moreover, the encryption research exception requires the researcher to inform the target about plans for circumvention for research purposes. The exception already includes a condition that "it would not be practical to carry out the research without circumventing the technological measure" and that the person has "lawfully obtained the work," so the researcher has a legal copy and must pass a necessity barrier. The inclusion of an additional notice requirement should be dropped since it has little to do with copyright protection, yet creates a possible barrier for researchers who need to do encryption research without telegraphing their plans to the target organization. The exception also raises issues for peer review since the exception does not cover third party peer reviewers, who may be unable to adequately review the research.

Bill C-32 contains a circumvention exception for privacy. Doesn't that address the privacy concerns?

No. The exception fails to provide Canadians with full privacy protection and Bill C-32 unquestionably makes it more difficult for Canadians to effectively protect their privacy. The reason for this is that though there is an exception that permits circumvention to protect (and prevent the collection or communication of) personal information, the ability to exercise this exception is rendered difficult by virtue of the inability to legally obtain devices (ie. software programs) for this very purpose. The bill states that a person can offer circumvention devices or services for the protection of personal information only "to the extent that the services, technology, device or component do not unduly impair the technological measure."

Bill C-32 does not include a definition of "unduly impair." However, according to an Industry Minister official who was responding to a journalist inquiry under Bill C-61 about the same language:

"The intent of the provision is to ensure that while individuals may obtain devices and services that circumvent technological measures with a view to protecting privacy, any ensuing circumvention of the technological measure cannot be done in a manner that would enable unauthorised uses of the underlying copyright material by that person or by a third party."

In other words, you can use a circumvention device to protect your privacy but it cannot allow you to simultaneously access the underlying content. Of course, once most circumvention devices circumvent a technological measure, the protected content will be in the clear. Distribution of this form of device is therefore illegal. Moreover, service providers will be likely be unwilling to use this provision for fear of facing liability. Not only should the "unduly impair" wording be removed, but the bill should place a positive obligation on those companies that use DRM that may raise privacy concerns to provide the keys to circumvent their technological measure where requested to do so for privacy purposes.

Bill C-32 contains a circumvention exception for the visually impaired. Doesn't that address those access concerns?

No. The provision suffers from the same shortcoming as the privacy exception. While there is an exception for the act of circumvention, access to devices that can be used to circumvent again comes with the restriction that a person can offer circumvention devices or services only "to the extent that the services, technology, device or component do not unduly impair the technological measure."

The notion of not unduly impairing the TPM is even more non-sensical in this context given that the whole point of circumventing is to provide access to the content for those with perceptual disabilities. The content will obviously be in the clear since that is what is needed to provide the necessary access. The limitation on devices and services here makes absolutely no sense unless the real aim to stop those with perceptual disabilities from obtaining access. Not only should the "unduly impair" wording be removed, but the bill should place a positive obligation on those companies that use DRM to circumvent their technological measure where requested to do so for access for those with perceptual disabilities.

Bill C-32 contains a circumvention exception for interoperability. Doesn't that address those concerns?

No. The emergence of open source software as a powerful alternative to proprietary software models has been an important business and societal development. Open source software is today widely used by consumers (e.g., Firefox browser) and businesses (e.g., Linux operating system, Apache web server). From a policy perspective, the Canadian

government's professed goal is to create a level playing field so that the marketplace rather than laws will determine marketplace winners. It has opposed attempts to create policy preferences for open source (over the objection of some advocates and countries) instead favouring a more neutral approach.

Notwithstanding the claims of neutrality and trusting in the market, Bill C-32 creates significant marketplace impediments for open source software. Achieving a level playing field requires interoperability so that differing computer systems can freely exchange data. The bill includes an interoperability provision at Section 41.12, which states that the anti-circumvention provisions do not apply to:

a person who owns a computer program or a copy of it, or has a license to use the program or copy, and who circumvents a technological measure that protects that program or copy for the sole purpose of obtaining information that would allow the person to make the program and any other computer program interoperable.

The problem with this provision is that it does not extend far enough to maintain a level playing field. The classic example involves the use of Linux as a consumer operating system. Unfortunately, this operating system cannot officially play DVDs since most commercial DVDs contain a digital lock and the entity that controls the lock does not license the necessary locks to play DVDs on Linux. Programmers have developed alternatives, but all involve circumventing the digital lock, an act that becomes illegal under Bill C-32.

The interoperability provisions do not help address this issue, since DVDs may not be considered computer programs and many of the circumventing programs have functionality beyond playback of commercial DVDs. The net effect is that Bill C-32 erects an enormous barrier to open source software adoption, thereby harming innovation and a competitive marketplace. The solution - as proposed by the Computer and Communications Industry Association in 2000 - is to create an exception the substantially broadens the interoperability exception.

The Missing Exceptions

Does C-32 include "authorized circumventers" as is used in New Zealand to facilitate legal circumventions?

No. New Zealand's copyright law introduces the concept of "qualified circumventers." The law grants special rights to trusted third parties who are permitted to circumvent on behalf of other users who are entitled to circumvent but technically unable to do so. The current list of qualified circumventers includes librarians, archivists, and educational institutions. This approach rightly recognizes that many people will be unable to effectively use the exceptions inserted into the law. By creating a class of trusted circumventers, the law creates at least one mechanism to ensure that users retain their existing copyright rights.

Are companies required to unlock locked content for legal purposes under C-32?

No. Many countries have recognized the danger that combination of DRM and anti-circumvention legislation may effectively eliminate user rights or copyright exceptions in the digital environment. Creating exceptions is one way to address the issue, but another is to adopt an approach of "with rights come responsibilities." In this case, if companies are going to obtain new legal rights for DRM, they must also shoulder the responsibility of unlocking their content when requested to do so by users for legal purposes. This is a common theme in copyright laws around the world, which often identify courts, tribunals or mediators as the source to ensure that rights holders do not use DRM to eliminate user rights.

Does C-32 include an exception for non-infringing access, such as accessing DVDs from other regions?

No. Bill C-32 prohibits the circumvention of TPMs that have absolutely nothing to do with infringing copying. The most obvious example of this comes from the region coding found on DVDs and many computer games. Many DVDs include Macrovision (designed to stop copying a DVD to VHS), Content Scramble System or CSS (the subject of important litigation involving DeCSS, a software program created to allow Linux users to play DVDs since they were otherwise unable to do so due to CSS), and region coding.

The premise behind region coding is fairly straight-forward. With DVD region coding, the world is divided into eight regions (Canada and the U.S. form Region One). Consumer electronics manufacturers have agreed to respect region coding within their products by ensuring that DVD players only play DVDs from a single region. The net effect is that Canadian-purchased DVDs will play on Canadian-bought DVD players, but DVDs purchased in Europe, Australia, or Asia (all different regions), are unlikely to work on those same DVD players (with the exception of those DVDs that are region coded zero, which can be played worldwide).

Note that the use of region coding has nothing to do with traditional notions of copyright law. The underlying work may involve a copyrighted work - DVDs and video games regularly use region coding - yet the protection is designed to manipulate markets by restricting the ability to use fully authorized copies of works. Many countries have recognized this by specifically excluding non-infringing access controls from their anti-circumvention legislation. For example, New Zealand's copyright law includes a much different definition of technological measure, stating that:

for the avoidance of doubt, does not include a process, treatment, mechanism, device, or system to the extent that, in the normal course of operation, it only controls any access to a work for non-infringing purposes (for example, it does not include a process, treatment, mechanism, device, or system to the extent that it controls geographic market segmentation by preventing the playback in New Zealand of a non-infringing copy of a work)

Section 53a of Norway's anti-circumvention law states that the provisions shall not "hinder private users in gaining access to legally acquired works on that which is generally understood as relevant playback equipment," while Finland's law expressly permits circumvention for non-infringing uses of lawfully acquired copies. The failure to include such a provision under Bill C-32 is a striking failure that must be remedied.

Does C-32 include a circumvention exception for personal uses?

No. While other countries provide a blanket exception for personal use and establish a corresponding circumvention exception, Bill C-32 does not. For example, Lithuania's anti-circumvention provisions include a specific exception that preserve this personal use right by requiring content owners to enable legitimate uses. This approach has the benefit of not only preserving personal uses, but also placing the obligation on those that use TPMs to ensure that the public retains its rights.

Does C-32 include a circumvention exception for digital archiving?

No. While many countries have expressed concern about the impact of TPMs on the preservation of digital materials, Bill C-32 only exacerbates the problem by not creating an exception for digital archiving. Other countries have recognized this danger and sought to address it. For example, the Czech Republic's copyright law provides at Article 37 that:

(1) Copyright is not infringed by a library, archive, museum, gallery, school, university and other non-profit school-related and educational establishment:
a) if it makes a reproduction of a work for its own archiving and conservation purposes, and if such a reproduction does not serve any direct or indirect economic or commercial purpose;

That country's anti-circumvention provisions then specify at Article 43(4) that:

Legal protection under Paragraph (1) [the anti-circumvention provision] above shall be without prejudice to the provisions of . . . Article 37 (1) (a) . . . to the extent necessary to benefit from the exception. An author who used technical measures under Paragraph (3) in respect of his work shall make his work available to lawful users to the extent necessary to fulfill the purpose of the stated exploitation of the work.

It is difficult to understand how a government can intentionally introduce legislation that will cause clear harm to the preservation of a country's own digital heritage.

Does C-32 include a circumvention exception to protect minors?

No. An exception that surprisingly is not included in Bill C-32's anti-circumvention provisions is an exception to protect minors. How does this arise in the context of copyright? One obvious example are parents who wish to stop their children from watching certain scenes in a movie. There are services such as ClearPlay that purport to

edit out sex, violence, and profanity from regular DVD movies. Regardless of one's view of such practices, surely it ought to be the right of a parent who has purchased the DVD edit a scene for their family's personal viewing purposes. Yet under Bill C-32, a parent who wants to shield their children from such content risks violating the law in order to do so.

Creating an explicit exception for the protection of minors is fairly common in other countries. Taiwan's anti-circumvention provisions include a blanket exception to protect minors (Article 80ter), while Singapore's Copyright Act features an exception to the anti-circumvention provision where the circumvention is "to prevent access by minors to any material on the Internet." There may well be other instances where a parent or school wishes to protect minors but faces the prospect of violating the law by circumventing a digital lock.

Does C-32 include a circumvention exception for filtering software programs?

No. As part of the U.S. Copyright Office's DMCA rulemaking procedure (under which it identifies non-infringing uses that are hampered by the DMCA), the Office has twice issued an exemption for circumvention of filtering software programs in order to identify the list of sites included within the program. Filtering programs can be used to filter or block inappropriate material, yet the same programs have been subject to considerable criticism over concerns that they may be overbroad and block perfectly legitimate material. The only way for a party to ascertain whether their site is included on the block list is to access the lists contained in the software program, a process that typically requires circumvention.

In 2000, the Copyright Office found that an exception for filtering programs was needed. It reaffirmed the decision in 2003. In 2006, Seth Finklestein, the primary supporter of the "censorware" exception abandoned the fight for another renewal and the exception was dropped. The same concerns remain, however, which is why a clear exception for the circumvention of filtering programs is needed within Bill C-32.

Does C-32 include an exception for circumventing digital locks that become obsolete or broken?

No. The inclusion of a right to circumvent in the event that the TPM breaks or becomes obsolete should be relatively uncontroversial. The U.S. Registrar of Copyrights has included a specific exception that addresses this situation since 2000. The exception reflects the recognition that the continual evolution of technology places the investment that consumers make in entertainment and software products or that libraries make in materials at risk in the event that a TPM ceases to function or becomes obsolete. While products do not come with a guarantee to function forever, the law should not impair consumers and libraries that seek to circumvent technologies that are no longer supported and thus create a significant barrier to access to their property.

Despite the obvious, recognized need for such an exception, Bill C-32 does not address the issue. There is a limited exception for software interoperability, but that provision does not come close address the concerns associated with obsolete or broken TPMs. Given the frequent changes in technology, it is a question of when, not if, technologies become obsolete. Bill C-32 must anticipate these technological changes by providing a right of circumvention due to obsolete or malfunctioning TPMs.

Does C-32 include an exception for court cases, laws, and government documents?

No. In order for the public to know their legal rights and obligations, access to the law is widely viewed as essential. Yet there is real danger that these kinds of materials - court decisions, legal statutes, and other government documents - could end up locked down using digital rights management. Other countries have recognized the danger of mixing digital locks, anti-circumvention legislation, and legal materials. For example, Sweden's implementation of anti-circumvention legislation tries to ensure access to court cases and government documents that are subject to TPMs. Canadians surely should enjoy full access to the law without the prospect of fears that they might violate the very law they are trying to access by circumventing a digital lock. An exception in Bill C-32 for this form of content is certainly needed.

Bill C-32's digital lock provisions apply to copyrighted works. Does that mean that public domain (ie. out-of-copyright) works are not affected?

No. Concerns about the impact of anti-circumvention legislation on public access and use of public domain materials is frequently addressed by arguing that the legislation only protects works that are subject to copyright. Since public domain materials fall outside that definition, works such as old public domain films that are enclosed with DRM could be lawfully circumvented. Those assurances notwithstanding, without the inclusion of a public domain circumvention right, circumventing DRM on works that combine public domain content with materials still subject to copyright could give rise to liability. In other words, pure public domain may be circumvented (provided you have the tools to circumvent), but once someone builds on a public domain work, they will benefit from the anti-circumvention provisions.

This is a particularly pronounced concern for historians, archivists, and film scholars since their ability to use public domain film or video may be limited by anti-circumvention legislation. For example, the distributor of a DRM'd DVD containing public domain films along with an additional commentary track would likely argue that there is sufficient originality such that the DVD is subject to copyright and that anti-circumvention provisions apply. While even supporters of the DMCA acknowledge that anti-circumvention legislation should not be used to privatize the public domain, they are loath to establish a full exception or circumvention right for public domain materials, arguing that all works contain some elements of the public domain and that a blanket exception could be used to cover virtually any circumvention.

A middle ground on this issue would include at least two provisions. First, a right to circumvent where the underlying work contains a substantial portion of public domain materials. The definition of "substantial" will obviously be crucial, but policy makers and legislative drafters must err on the side of ensuring that the public domain is not inappropriately enclosed. Second, given that anti-circumvention legislation encourages the use of DRM, the government should establish a policy that actively discourages its use on public domain materials. This could be achieved by blocking the right to use such technologies where non-DRM'd versions of the same works are not reasonably available to the general public.

The Consumer Provisions

Bill C-32 purports to allow consumer to legally shift music from CDs to their iPods or other devices. Do they lose that right if there are digital locks on their CD?

Yes. The new right to legally shift music is subject to an anti-circumvention limitation. In other words, the right to shift music to your iPod is not a right that you control. It is a right that is effectively dictated by the record label who can easily remove the right by including copy-controls on the CD release (there are thousands of these kinds of CDs owned by Canadians). In fact, the anti-circumvention limitation even applies to private copies onto blank CDs. This means that consumers pay for the CD and pay the levy on a blank CD that nominally gives them the right to make a personal copy, yet violate the law if they circumvent a copy-control in order to do so.

Does Bill C-32 allow consumers to make legal backup copies of most commercial DVDs?

No. The new backup copy provision are subject to an anti-circumvention limitation. Since most commercial DVDs currently contain several TPMs, consumers would not be able to legally make a backup copy of their own personal DVDs.

Does Bill C-32 allow consumers to shift content from a DVD to a portable video player such as an iPad?

No. The format shifting provision is subject to an anti-circumvention limitation. Since most commercial DVDs currently contain several TPMs, consumers would not be able to legally make a backup copy of their own personal DVDs.

C-32 purports to allow consumer to legally record television shows, yet cable companies are increasingly inserting anti-copying technologies into some broadcasts? Does C-32 allow for those programs to be recorded?

No. If there is a digital lock (often referred to as a broadcast flag) included with the broadcast, you can't legally circumvent it in order to record the program. Note that the U.S. has established limits on the use of the broadcast flag, but no such limits exist in Canada. As Canada transitions to digital, it is possible that broadcasters will increasingly

institute anti-copying notices to stop the very recording rights that C-32 purports to provide.

C-32 includes an exception for unlocking cellphones. Isn't that a positive new development?

The inclusion of a circumvention exception for unlocking cellphones is certainly a good thing, yet the net effect is merely to retain the status quo. It is currently legal in Canada to unlock a cellphone, with the primary barriers being carrier contracts and technical inability to do so. The new exception does not create any new rights to unlock the cellphone, but rather merely retains the current right to do so.

Does C-32 require businesses to notify consumers about the presence of digital locks?

No. Bill C-32 does not contain any notice requirement regarding the limitations imposed by DRM on a consumer product. Most consumers know little if anything about DRMs and the limitations that may be placed on consumer entertainment products such as CDs, DVDs, video games, or digital download services. While there may some limited disclosures - DVDs indicate the region code, if your eyesight is good enough you might notice that some copy-controlled CDs warn on the back corner that they may not play on all computers, and digital download services all feature lengthy user agreements that few consumers will ever read - they are plainly insufficient and the government should not support the legal fiction that "informed" consumers are knowingly purchasing products that contain a host of limitations.

For many consumers, these DRM products are simply not fit for purpose - they often won't play on your DVD player, on your iPod, or permit usage that most would expect is permissible. Moreover, consumers frequently can't obtain a refund for their purchases as many retailers won't accept returns on opened CDs and DVDs and digital download services do not offer refunds to disgruntled downloaders.

The federal government might argue that this is provincial problem, since consumer protection issues typically fall under provincial jurisdiction. The reality, however, is that the federal government can and should play its part to address the issue given the manner it which it is supporting the use of DRM through Bill C-32. It should consider establishing DRM labeling requirements (an approach also advocated by the Society for Law and Computers in the UK) so that consumers will be able to quickly identify capabilities, compatibilities, and limitations. The Competition Bureau is currently responsible for two labelling statutes - the Consumer Packaging and Labelling Act and the Textile Labelling Act. If labelling is required for upholstered furniture, surely it can be added for consumer entertainment products.

Isn't there an "analog hole" that would allow someone to record a DVD without circumventing the digital lock?

Yes. It is true that rather than picking a digital lock on DVD, a person could try to camcord an analog version of a film. In fact, this is precisely what the MPAA argued last year, claiming that there was no need for a film studies exemption in the DMCA since there is an analog way to create film clips. Rather than break the encryption on a DVD, teachers could camcord the same film clips. In fact, the organization showed a video demonstrating how to effectively camcord clips of DVDs without breaking the encryption on the DVD.

Leaving aside how surreal it is to see the same organization that travels the world demanding anti-camcording legislation now citing it as a solution, the analog hole is not a solution for making backup copies of DVD or format shifting. It might only be used for a very brief clip, but given the government's stated goal of modernizing Canadian copyright law, it is worth asking whether a law that proposed using camcording films to preserve basic copyright rights has struck the right balance. Note that the Film Studies Association of Canada was outspoken on C-61.

Business Considerations

Isn't this just a matter of consumer choice? If consumers don't want products with digital locks, no one is forcing them to purchase them?

Of course it is true that no one is forcing a parent to buy an educational or entertainment DVD for their children or for music lovers to purchase CDs. However, it is not strictly a matter of consumer choice. For example, I recently spoke at the Canadian Federation of Students annual meeting and was advised by several student leaders that faculties on their campuses were moving to require students to purchase electronic editions of course textbooks. Students in these programs were not faced with a consumer choice of declining to purchase. Rather, enrollment in the program mandated the purchase of digitally locked books. Given the emergence of the Amazon Kindle and Apple iPad, the move toward e-books on university campuses across the country will only increase. These students do not have the option of declining to purchase items with digital locks.

Won't the digital lock provisions help bring new businesses to Canada like Hulu.com?

There is no real evidence to suggest that the anti-circumvention rules found in C-32 will make Canada a more attractive place for digital investments. The delays associated with Hulu.com or Spotify have little to do with Canadian copyright law. Rather, they are licence related as the delays in obtaining Canadian licences from rights holders (in the case of Spotify) or the decision of U.S. broadcasters to sell the Internet licenses to Canadian broadcasters (in the case of Hulu.com) are the primary source of delays. In fact, there have been repeated rumours that Hulu will launch shortly in Canada. Spotify has indicated that it wants to enter the U.S. and Canadian market simultaneously.

Moreover, even the architect of the DMCA has admitted that it has been a failure. Bruce Lehman, told a McGill audience in 2007 that "our Clinton administration policies didn't work out very well" and "our attempts at copyright control have not been successful."

Are the concerns associated with digital lock provisions in the United States legitimate? What issues have arisen in the U.S. under the DMCA?

The concerns associated with anti-circumvention legislation such as that found in the U.S. DMCA are borne out by 12 years of experience under those rules in the U.S. Perhaps the most obvious problem has been the use of these legal provisions in cases that have nothing to do with copyright. The U.S. has been home to a litany of cases involving the DMCA and garage door openers (which involved Canadian-based Skylink), printer cartridge refills, hardware backups, and cell phones. None of these cases involved attempts to stop copyright infringement. Rather, they were fundamentally about exerting greater market control by thwarting potential competitors and reducing innovation.

For example, in the Skylink case, Chamberlain, a competitor in the garage door opener market, tried to stop Skylink from offering a universal garage door remote control. Chamberlain argued that Skylink needed to circumvent its TPM in order for its remote to function and that this constituted a violation of the DMCA. While some of the cases have ultimately been dismissed (including, after several appeals, the Skylink case), the mere threat of a lawsuit is frequently enough to dissuade many companies from entering the market or from developing an innovative new product.

For more on the U.S. experience, see the EFF report: Unintended Consequences: Twelve Years Under the DMCA.

If these digital lock provisions are too restrictive, what compromises are available?

The prior 31 questions identify many necessary reforms to C-32. As I have noted elsewhere, a starting position should be clarification that it is not an infringing act to circumvent for lawful purposes. This simple provision would allow the law to target large scale infringement but preserve user rights already contained in the law. Moreover, lawmakers should consider dropping the ban on the distribution or marketing of devices that can be used to circumvent. If it is acknowledged that there are legitimate reasons for circumventing a digital lock, Canadians should be able to legally acquire the tools they need to do so.

The prior discussion has also identified a range of additional compromise reforms. These include:

- the identification of "qualified circumventers" to allow Canadians without technical expertise to exercise their rights
- the removal of the lock requirements for digital lessons and digital inter-library loans
- the establishment of an impartial review process for new circumvention rights

- the extension of the encryption research exception to all research
- fixing the privacy and perceptual disability exceptions so that circumvention devices can be lawfully obtained
- extension of the interoperability exception
- a requirement on rights holders to unlock locked content in appropriate circumstances
- exclude non-infringing access controls from their anti-circumvention legislation
- establish a new exception for personal use
- establish a new exception for preservation of digital materials
- establish a new exception for the protection of minors
- establish a new exception for filtering software
- establish a new exception for obsolete or broken locks
- establish a new exception for court cases, laws, and government documents
- establish a new exception for public domain works
- remove the lock requirements on the time shifting, format shifting, and backup copy provisions
- require businesses that use TPMs to include a prominent warning on their packaging