



April 18, 2008

*Via Email*

House of Commons Standing Committee on Industry, Science and Technology  
Sixth Floor, 131 Queen Street  
House of Commons  
Ottawa ON K1A 0A6

Dear Members of the Committee:

**Subject: Industry Committee Study of Canadian Science and Technology**

---

The Canadian Internet Policy and Public Interest Clinic ("CIPPIC") is a legal clinic based at the University of Ottawa, Faculty of Law. CIPPIC's mandate is to provide a public interest voice in the policy-making process at the intersection of law and technology. We write to you in response to your motion of February 7, 2008, to conduct a study into Canadian science and technology.

We wish to focus our comments on three topics:

1. access to scientific data,
2. crown copyright, and
3. the dangers digital rights management technologies – and the laws that protect those technologies – pose to science research.

### **1. Open Access to Scientific Data**

Scientific data is the lifeblood of innovation. The Canadian government generates a huge volume of scientific data, both directly through the research activities of scientists employed by the government, and through its role funding the three federal research granting institutions. This data serves Canada best, generates innovation most, and advances knowledge most significantly, when it is openly accessible without restrictive licensing terms. Openly accessible data supports further research in both the public sector and private sector and allows for an efficient process for science to make its way from the lab into innovations that benefit Canadian researchers and businesses. This is not a controversial position: around the world, governments are making scientific data, generated through public funds, accessible to the public. The United States and the European Union, in particular, have moved rapidly over the past couple of years to improve access to publicly funded research. The Canadian government should follow suit, or risk undermining innovation and hampering the global competitiveness of Canadian businesses.

There are three areas in which the Canadian government could embrace open access.

First, the government itself holds huge volumes of publicly-funded scientific data. Unfortunately, under cost-recovery programs that paradoxically attempt to restrict the flow of this data to researchers, businesses, and individuals, government agencies often distribute this data in restrictive formats that impose complicated and onerous licensing conditions. Occasionally, agencies will restrict further dissemination of the data for fear of “competition” with the agency. This approach actually undermines Canada’s policies supporting commercial research and innovation, and should be scrapped in favour of an open access policy.

Second, Canada’s federal research granting institutions – the Natural Sciences and Engineering Research Council (NSERC), the Social Sciences and Humanities Research Council (SSHRC), and the Canadian Institutes of Health Research (CIHR) – should mandate open access publication of data assembled through its funds. This could generate enormous repositories of scientific data and generate opportunities for public and private innovation. The funding agencies are already starting to move in this direction. The CIHR’s *Policy on Access to Research Outputs* already makes clinical trial data available, and is now requiring grant recipients to ensure that publications are openly accessible through an online repository within six months of publication.

Third, many of Canada’s academic institutions are also strongly in support of open access. Universities are beginning to publish open access journals and are encouraging their academic to publish their material in open access repositories. However, universities could use guidance in developing the institutional policies necessary to implement and maximize the benefits of open access. The federal government has a role to play in facilitating universities’ transition to the open access model.

## **2. Crown Copyright**

Crown copyright grants Her Majesty copyright in any work prepared or published by or under the direction or control of Her Majesty or any government department. Crown copyright enables the practice of licensing access to data under onerous licensing terms that go beyond the terms of copyright to impose restrictions on use and distribution. Our submissions with respect to Crown copyright are closely related those with respect to open access: works authored at taxpayer expense best serve the public interest where the public is free to access, use, modify, and redistribute them without interference from the government.

The policy justifications usually offered for copyright law do not apply in the context of Crown copyright. The Crown does not require a grant of copyright in publicly-funded works as an incentive to the creation of those works. In the specific context of Crown copyright, it is often argued that Crown copyright is required to ensure accuracy and integrity of government materials. However, that argument is difficult to maintain in the face of the government’s ability to publish “authoritative” versions of publicly-funded works on the internet: a quick search of the applicable government department website can verify the accuracy or integrity of any re-published works. Moreover, while the

Crown's need to ensure the accuracy and integrity of legal materials might have some weight, those materials are already permissively licensed. The argument has less weight in the context of commercial and academic research, where there is already a significant interest in accuracy and integrity. In this context in particular, Crown copyright seems an impediment to Canada's interests. We note that the United States lacks a Crown copyright doctrine. American competitors accordingly enjoy a competitive advantage compared to Canadian researchers in accessing, re-using and distributing publicly-funded scientific data. CIPPIC submits that Canada's public interest is best served by permitting free access to Crown works. Free access to Crown works would facilitate innovation, further research, and the further distribution of Canadian research.

### **3. Digital Rights Management Technologies and Anti-Circumvention Laws**

Digital Rights Management technologies ("DRM") employ technical measures to govern the means by which content may be accessed or used. Examples include regional coding, employed in DVDs to ensure that discs purchased in Europe cannot be played on devices in North America, and FairPlay, Apple's DRM that ensure that music purchased from the Apple iTunes online store will only play on an Apple iPod. DRM is often justified as necessary to permit innovation in digital distribution models. However, in practice, DRM is seldom directed primarily towards content protection. More often, it has anti-competitive objects. In both the examples offered here, DRM has been employed not to prevent infringement of copyright, to restrict opportunities for downstream businesses in the interests of maximizing profits for the content distributor. Regional coding does not prohibit reproduction – it prohibits use of legal content in a given region so that distributors may engage in price discrimination. Similarly, Apple's FairPlay is primarily directed at preventing consumers from enjoying music they've purchased from iTunes on a digital device manufactured by a competitor.

The challenges posed by these technologies are exacerbated by anti-circumvention laws. Anti-circumvention laws are an additional layer of legal protection that sits atop the technological protection afforded by DRM. Anti-circumvention laws originate with the WIPO Copyright Treaty and the WIPO Performers and Phonograms Treaty of 1996. These treaties oblige signatory nations to legislate "adequate legal protection and effective legal remedies" against the circumvention of "effective technological measures" used by authorized distributors of copyright protected content. They also require the provision of adequate legal remedies against tampering with "rights management information." These treaty requirements have often been accompanied in implementing legislation of ratifying nations by an "anti-tool" provision, which prohibits the use or distribution of devices or tools that could be used to circumvent or tamper with DRM. Collectively, this trio of anti-circumvention laws has proven controversial.

While the challenges posed by DRM and anti-circumvention laws are well known, in this submission, CIPPIC would like to highlight the unique challenges these technologies and laws pose security researchers. Security researchers routinely circumvent technical protection measures. As stated by a coalition of Canadian security businesses in a June

22, 2006, letter to the Ministers of Industry and Canadian Heritage (available at [www.digitalsecurity.ca](http://www.digitalsecurity.ca)):

We are not in the business of circumventing technological safeguards for the purposes of exploiting the weaknesses we find; rather, we are in the businesses of finding and addressing those weaknesses.

Security weaknesses are best found - and addressed - when a variety of security researchers examine a platform or application. The odds of one party devising the best response to a security issue are slim; the likelihood of an optimal response improves significantly when a community of security researchers has the opportunity to examine and test a platform or application. Anti-circumvention laws throw a shroud of legal risk over that community, and dampen security research at the edges. Simply, anti-circumvention laws that provide for excessive control make for bad security policy.

The work of security researchers is central to Canada's economic policies in respect of e-commerce. The work of Canada's security researchers facilitates consumer trust and confidence in the internet. Anti-circumvention laws must not undermine this work.

The experience of security researchers in the United States has substantiated those concerns. Professor Ed Felten, of Princeton University, has spoken of the effect the American *Digital Millennium Copyright Law* has had on his own research activities. In a submission to the Copyright Office requesting an exemption from liability under the DMCA for researching spyware (reproduced at <http://www.freedom-to-tinker.com/doc/2005/dmcacomment.pdf>), Professor Felten and Professor Alex Haldeman wrote that they:

waste valuable research time consulting attorneys due to concerns about liability under the DMCA. They must consult not only with their own attorneys but with the general counsel of their academic institutions as well. Unavoidably, the legal uncertainty surrounding their research leads to delays and lost opportunities. In the case of the CDs at issue [*i.e.*, the Sony rootkit], Halderman and Felten were aware of problems with the XCP software almost a month before the news became public, but they delayed publication in order to consult with counsel about legal concerns. This delay left millions of consumers at risk for weeks longer than necessary.

As the Committee is no doubt aware, the Canadian government is deliberating about whether to legislate anti-circumvention laws in Canada. Should the government elect to do so, such laws should carve out a comprehensive exception to liability for security researchers. CIPPIC calls on the Committee to endorse this position, and signal to the Canadian government the importance of this community to Canada.

\* \* \*

We trust you will find these comments helpful to your deliberations. We thank you for having presented us with the opportunity to address your committee. We would welcome

the opportunity to address the Committee should it choose to hold hearings into this matter.

Yours truly,

A handwritten signature in black ink that reads "David Fewer". The signature is written in a cursive style with a large, looped "D" and "F".

David Fewer  
Staff Lawyer  
CIPPIC