Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

November 4, 2004

Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

Attention: Jennifer Stoddart, Privacy Commissioner of Canada

Dear Commissioner,

Re: Critical privacy issues regarding digital rights management (DRM) technology

We are writing to request that the Office of the Privacy Commissioner of Canada ("OPCC") take prompt action regarding the privacy threats posed by DRM technology. Timely action on this issue is particularly important because the Canadian government may soon enact legal protection for DRM in the digital copyright context, without considering or addressing DRM's severe privacy implications. The legal protection for DRM that the government is contemplating is likely to encourage and entrench the privacy-invasive practices that DRM enables.

In this letter, we describe the background context of our request, a basic description of the privacy threats posed by DRM and why it is incumbent on OPCC to take action.

Background

Like an electronic security guard who never takes a break, DRM is a form of permanent technological protection that protects copyright works. DRM systems are typically comprised of an array of technological components, including encryption tools, surveillance tools, databases of works, owners and individual users, and license management tools. Copyright industries are increasingly using DRM to control public access to and use of digital works. Beyond simple copy-control mechanisms, DRM is designed to automatically manage and enforce contractual terms in relation to copyright works and other types of information.[i]

Heritage Canada and Industry Canada are currently drafting legislation that will provide legal protection for DRM. There are strong indications that these ministries will recommend that Canada prohibit the circumvention of DRM for the purpose of copyright infringement. The Standing Committee on Canadian Heritage specifically made such a recommendation in May of this year.[ii]

Université d'Ottawa • University of Ottawa
Faculté de droit • Faculty of Law
57 Louis-Pasteur, Ottawa (Ontario) K1N 6N5 Canada
(613) 562-5800 (2553) • (613) 562-5417 (Téléc/Fax)
www.cippic.ca • cippic@uottawa.ca

Based on the result of similar initiatives in other countries, particularly the United States, it is no secret that legal protection for DRM can be fraught with danger. The dangers inherent in DRM and laws that protect it include vesting excessive control in copyright industries over how the public can access and use works, denying fair use of copyright works, imposing unfair contract terms on consumers, enabling anti-competitive practices, stifling creation and innovation and reducing national security by chilling encryption and other scientific research. In addition to these important dangers, which CIPPIC is addressing in other forums, DRM poses a severe threat to personal privacy.

DRM poses an unprecedented threat to privacy

While DRM's impact on privacy has not yet received the mainstream media attention that other impacts have received, it has probably become trite to assert that DRM implicates user privacy. The *EU Copyright Directive*, for example, recognizes that DRM can have an impact on privacy and provides that DRM should be designed in accordance with the *EU Data Protection Directive*.[iii] Even the *DMCA* in the United States permits circumvention of DRM for the protection of privacy.[iv]

In basic terms, DRM implicates privacy because its continuous information collection and surveillance functions can provide owners with highly detailed and previously unavailable information about the reading, listening and viewing habits of end users. Both the nature of this information and the level of its detail are unprecedented. Even Microsoft's definition of DRM hints at this potential: "DRM is a set of technologies copyright owners can use to protect their copyrights *and stay in closer contact with their customers*".[v]

In addition to the nature and detail of the information collected by DRM, one of the most insidious aspects of DRM's impact on privacy is the fact that DRM is collecting information while people are engaged in highly private activities in places where they would likely have no expectation that they are being watched – DRM collects information while users are reading, watching or listening to content, typically in the privacy of their homes or other private spaces. In this way, DRM interferes with and chills Canadians' most private and personal intellectual freedom to access, explore and use copyright works, often privately and anonymously.

There are many real-world examples of DRM's threat to privacy, including the following statement from a recent Berkeley study of DRM-enabled content delivery services:

> The ways that information is collected and processed during use of the services examined is almost impenetrably complex. It is difficult to determine exactly what data a service collects, and merely discovering that separate monitoring entities sit behind the services requires a careful reading of the services' privacy policies.[vi]

Although further study of DRM's impact on privacy is required, especially as new systems are developed, there is a growing body of literature addressing its critical impact on privacy.[vii] The Information and Privacy Commissioner of Ontario has written on the issue, confirming DRM's threats to privacy.[viii] Highly regarded privacy groups such as EPIC have also documented these

threats, and EDRI (European Digital Rights Initiatives) is pursuing analysis under EU law, and are making their case with the Article 29 Committee..[ix]

Responding to the privacy threats posed by DRM

The privacy threats posed by DRM clearly fit within the mandate of the OPCC and the provisions of *PIPEDA*. The kind of information processed by DRM is sensitive personal information.[x] Crown action in this area, through legislation which authorizes the collection of this information in the privacy of one's own home, and sanctions the lack of transparency to users, may well give rise to a Charter challenge.

It is difficult to reconcile the operation of DRM with *PIPEDA*'s requirements. Here are a few immediate questions, which leap to mind upon examination of the CSA principles:

1. Who is accountable, in the event the copyright control mechanism malfunctions? How does the individual get redress? Who controls the data once it is gathered by the mechanism, and how does the individual keep track of the dataflow?

2. The stated purposes of DRM are to protect copyright, but the information thereby collected will be ripe for data mining for other purposes. Such function creep will be difficult, if not impossible to detect. Further, because DRM is designed to implement and enforce copyright industries' licenses, there is a real risk that privacy rights will be rewritten in the one-sided consent terms of these licenses.

3. The collection limitation principle has been egregiously violated, because there are other ways and means to enforce copy control. As a surreptitious and continuous surveillance system, DRM tends to maximize, not limit, the collection and use of sensitive personal information.

4. Under DRM, personal data is gathered on an assumption of the guilt of the holder. Attempts to circumscribe the further disclosure of the personal information of the individual may be countered by contravention of agreement or possible theft of property arguments. Have we let loose in society a set of robotic police that will spy on innocent individuals regardless of probable cause?

5. Safeguards: If the right and ability of users to reverse engineer products is not protected, independent software experts will be unable to assess the protection of information inherent in DRM. What privacy impact assessment has been done on the data gathering mechanisms which the tools employ? What audit has been done on the companies involved? What about transborder dataflow, a timely issue in today's privacy discussions?

6. Openness: It has been hard for experts in the field to understand what is going on. At a minimum, better disclosure of the operations of the technology is required. There are particular issues with certain groups, such as children, the elderly, recent immigrants, etc.

7. Challenge: We anticipate your office and those of your colleagues in the data protection community will be swamped with complaints when the truth about the surveillance capacity of

these technologies becomes better known. Far better to demand putting the brakes on now, and have a full public debate on the implications of the technology.

DRM's privacy harms will be entrenched if Canada enacts legal protection for DRM without a full privacy impact assessment. You have the power to table a special report to Parliament, we would respectfully urge you to consider such an action. This is about nothing less than the right to read, write, and appreciate art anonymously. We have encouraged Canadian Heritage and Industry Canada to perform a full analysis of the costs and benefits of adopting an anti-circumvention law prior to proceeding further toward draft legislation. We have specifically stated that a full analysis should include the privacy implications of DRM and any proposed law. Despite our requests, these ministries are pushing ahead toward legislation, seemingly without considering or addressing any of the privacy implications of DRM.

If privacy is to be protected in this critical context, the privacy implications of DRM must be addressed prior to any possible anti-circumvention law being passed. Indeed, the passage of an anti-circumvention law in Canada is not a foregone conclusion. To the extent that the absence of such a law would help minimize incentives for a pervasive uptake of DRM, privacy would be better protected in Canada. There are a number of proposals for addressing privacy issues in DRM at a technical level and there might also be steps that could be taken at a policy level.[xi] It is incumbent on the OPCC to act in this matter as Canada's policy on DRM takes shape.

Yours truly,

Original signed by

Philippa Lawson
Executive Director

Alex Cameron
Associate

---

[i] For more information about DRM, see CIPPIC's Digital Rights Management webpage at <http://www.cippic.ca/en/faqs-resources/digital-rights-management/>.

[ii] <http://www.parl.gc.ca/InfocomDoc/Documents/37/3/parlbus/commbus/house/reports/herirp01-e.htm>

[iii] See *EU Copyright Directive*, at recital 57.

[iv] *Digital Millennium Copyright Act*, 17 U.S.C. § 512(i) (1998).

[v] Microsoft Corporation, "Definition of DRM", online: Microsoft <http://www.microsoft.com/windows/windowsxp/experiences/glossary_a-g.asp#drm> [emphasis added].

[vi] Deirdre K. Mulligan, John Han & Aaron J. Burstein, "How DRM-based content delivery systems disrupt expectations of 'personal use'" (2003). See also EPIC's Comments regarding DRM and privacy at <http://www.epic.org/privacy/drm/tadrmcomments7.17.02.html>

[vii] See *e.g.* EPIC's DRM and Privacy page at <http://www.epic.org/privacy/drm/default.html>; Julie Cohen, "DRM and Privacy" (2003) 18 Berkeley Tech. L.J. 575; Julie Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace" (1996) 28 Conn. L. Rev. 981; Lee A. Bygrave, "Digital Rights Management and Privacy – Legal Aspects in the European Union" in Eberhard Becker *et al.*, eds., *Digital Rights Management - Technological, Economic, Legal and Political Aspects* (New York: Springer, 2003) 418; Ian Kerr & Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" (2004) 2 Info., Comm. & Ethics in Society 87.

[viii] Information and Privacy Commissioner/Ontario, "Privacy and Digital Rights Management (DRM): An Oxymoron?" (October 2002), <http://www.ipc.on.ca/docs/drm.pdf>.
[ix] EPIC, "DRM and Privacy", <http://www.epic.org/privacy/drm/>.
[x] This was confirmed by Justice LeBel in *SOCAN v. CAIP*, 2004 SCC 45 at paras. 153-155.
[xi] For a description of some of these proposals, see Alex Cameron, "Infusing Privacy Norms in DRM: Incentives and Perspectives from Law" in *Proceedings of the 19th IFIP World Computer Congress, Toulouse, France* [forthcoming in 2004].