DIGITAL RIGHTS MANAGEMENT AND CONSUMER PRIVACY

An Assessment of DRM Applications Under Canadian Privacy Law

September 2007

EXECUTIVE SUMMARY

This Report provides the results of our study of digital rights management (DRM) technologies in use in the Canadian marketplace and their implications for consumer privacy. We have defined "DRM" in this Report to mean "a system, comprising technological tools and a usage policy that is designed to securely manage access to and use of digital information." We investigated the DRM technologies used in connection with the following products or services in Canada:

- Apple, *iTunes Music Store*
- Apple, *iTunes Video Store*
- Azureus, *Zudeo*
- eReader, *The Da Vinci Code*
- Disney/InterActual, *Pirates of the Caribbean* (DVD)
- Intuit, *QuickTax*
- Microsoft, *Office Visio*
- Napster
- Ottawa Public Library, OverDrive digital audio book
- Universal Studios, *Ray* (DVD)
- Sony BMG, Our Lady Peace, *Healthy in Paranoid Times*
- Symantec, *Norton SystemWorks 2006*
- Telus Mobility, *Spark*
- Ubisoft, *Prince of Persia: The Two Thrones*
- Valve, *Half-Life 2*
- Warner Music Group, Nickelback, *All the Right Reasons*

Using the data collected during our investigations, we assessed whether each application in question complied with the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).

Findings

Our assessment of the compliance of these DRM applications with PIPEDA led to a number of general findings:

- Fundamental privacy-based criticisms of DRM are well-founded: we observed tracking of usage habits, surfing habits, and technical data.
- Privacy invasive behaviour emerged in surprising places. For example, we observed e-book software profiling individuals. We unexpectedly encountered DoubleClick – an online marketing firm – in a library digital audio book.
- Many organizations take the position that IP addresses do not constitute "personal information" under PIPEDA and therefore can be collected, used and disclosed at will. This interpretation is contrary to Privacy Commissioner findings. IP addresses are collected by a variety of DRM tools, including tracking technologies such as cookies and pixel tags (also known as web bugs, clear gifs, and web beacons).
- Companies using DRM to deliver content often do not adequately document in their privacy policies the DRM-related collection, use and disclosure of personal information. This is particularly so where the DRM originates with a third party supplier.
- Companies using DRM often fail to comply with basic requirements of PIPEDA.

Technical Investigation

Our investigation provided us with the factual basis for our privacy assessments:

- Our investigation led us to distinguish "autonomous DRM" from "net-dependent DRM":
    - *Autonomous DRM* refers to DRM that needs no outside interaction to fulfill its purpose. Software that requires a CD-Key before becoming useable, DVDs that will only work with DVD players in certain regions and software that deactivates after a given number of uses are all examples of autonomous DRM.

- *Net-dependent DRM* refers to a growing trend in DRM schemes that involves either internet authentication, internet surveillance of uses and/or the tying of content to an online platform. Online music subscription services that deploy digital licenses to allow the use of locked content, web-enabled software validation and the tying of content to an online platform are all examples of net-dependent DRM.

The results of our investigations demonstrated that many, but not all, autonomous DRMs connect to and communicate with external computers during the course of the operation of the DRM. Conversely, *all* of the net-dependent DRM systems that we investigated communicate with external computers.

- Six of the products that we investigated used autonomous DRM. Four of these showed no communications. Since autonomous DRM does not appear to need to communicate to fulfill rights management purposes, it is natural to ask questions regarding those that do engage in external communications. Our investigations revealed that these communications appeared in most cases to be linked to advertising and web metrics.
- All of the online products and services with net-dependent DRM that we investigated disclosed communications to third parties such as Akamai Technologies, and DoubleClick. Our research informs us that these businesses partner with e-businesses to, among other things, process information, deliver content, offer web analytics services or deliver advertising. We were unable to identify the type of information we observed being disclosed to third parties.
- Some of the net-dependent products that we investigated involved products purchased from bricks-and mortar stores. With regard to these products, we observed DRM deployed in some cases to limit the number of uses or limit functionality. Others simply impaired functionality until authenticated *via* the internet or sometimes by telephone.

PIPEDA Assessments

Our privacy assessments of the DRM publishers and distributors engaged in third party communications disclosed a wide range of practices and varying degrees of compliance with *PIPEDA*:

Inappropriate purposes

- A number of organizations used DRM to collect, use and disclose personal information for inappropriate purposes (*e.g.*, Napster indiscriminately monitors its customers' communications to "check for …abusive language").

Excessive collection, use and disclosure of personal data

- Several organizations engaged in open-ended and indiscriminate collection, use and disclosure of personal information.

Inadequate notice

- Some organizations did not adequately specify the types of personal information they collected, the uses to which it was put and the entities to whom it was disclosed.
- Vague wording was a common problem across the privacy policies, as were privacy provisions that were spread across multiple documents for the same organization.
- We identified poorly disclosed or undisclosed tracking behaviour – both in our technical investigations and disclosed in privacy policies – and unexpected use of personal information.
- We identified undisclosed communications to third parties.
- We noted contradictions between observed behaviour and statements in the governing privacy policy.
- We encountered particular problems in the area of "technical information" – personal information of a technical nature, such as IP addresses – collected, used or disclosed through DRM, much of which was observed during the technical investigations. Sometimes neither the collection nor the purposes for it were disclosed.
- In several cases, although the organization acknowledged that it collects automatically collects "technical information" about users, most stated that this information (which almost always includes IP addresses) was not "personal information." Differing views on what does and does not constitute "personal information" is one of the most significant areas of potential divide between the DRM practices observed and the requirements of *PIPEDA*. This represents one of the most challenging privacy issues in relation to DRM because *PIPEDA* is only triggered when "personal information" is at issue.

No opt-out of unnecessary collection, use or disclosure

- Where organizations engage in DRM-enabled privacy invasive behaviours, they generally do not offer consumers the ability to opt-out of the unnecessary collection, use and/or disclosure of personal information.

Failure to appreciate reach of privacy law

- We noted consistent difficulty in addressing the privacy implications of DRM technology. Only one organization properly identified IP addresses as the personal information of users, and so subject to PIPEDA.

Failure to respond to Access to Information requests

- Almost half of the assessed organizations failed to even acknowledge our inquiry, much less respond substantively.
- None of the organizations we tested provided us with our personal information held by them.
- Only two organizations – Microsoft and the Ottawa Public Library – complied with requests to identify specific third parties to whom they had disclosed personal information.
- Only one firm gave a direct answer to the simple question, "Do you consider an IP address to be 'personal information'?"

We identified a number of third party communications during our technical investigations that were not easily explained by the organizations' privacy policies. These communications occurred at a variety of points, including in some cases while enjoying content. Some of these communications resolved to IP addresses belonging to known third parties such as Verisign, Akamai, Omniture and DoubleClick. We understand that some of these third parties collect personal information such as IP addresses in performing their services. We did not find that the organizations' privacy policies adequately explained these third party communications.

In addition, we did not find that any organization referred to Akamai or Omniture in the privacy policy and related documents that we reviewed. While it is possible that some of these communications amount to outsourced functionality, others appeared to involve third party services. Responses to specific inquiries about these

communications were generally unsatisfactory – only Microsoft and the Ottawa Public Library identified some of these organizations when presented with proof of the communications and a specific request to identify the third party. We know very little about these third-party communications; they raise important questions.

Conclusions

This report confirms that DRM is currently being used in the Canadian marketplace in ways that violate Canadian privacy laws. DRM is being used to collect, use and disclose consumers' personal information, often for secondary purposes, without adequate notice to the consumer, and without giving the consumer an opportunity to opt-out of unnecessary collection, use or disclosure of their personal information, as required under Canadian privacy law.