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

SEPTEMBER 2007

# DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES & CONSUMER PRIVACY

AN ASSESSMENT OF DRM APPLICATIONS UNDER CANADIAN PRIVACY LAW

www.cippic.ca

## ACKNOWLEDGEMENTS

CIPPIC gratefully acknowledges the financial support of the Office of the Privacy Commissioner of Canada for this study. The study was directed by David Fewer, Staff Counsel for CIPPIC, and coordinated by Philippe Gauvin, LL.M. candidate at the University of Ottawa, Faculty of Law. Vanessa Lavoie provided administrative support.

The following law students conducted investigations and/or conducted market research: Rachel Leck, Dan McConville, Seraphina Allen, Safwan Javed, Safina Lakhani, Kiernan Murphy, Denise Chapchal, Philippe Gauvin, Adam Barker. Special thanks to the following individuals who contributed to our DRM technological review: Mark McCans, Adam Barker, Byron Thom, Kiernan Murphy, Kris Constable and Angelique Mannella. Thanks to CIPPIC's Director, Philippa Lawson, for her contributions to the PIPEDA assessment framework and her thorough review of the draft.

An extra special thank you goes to our editors, Rachel Leck and Monique Moreau, for editing what ended up being a massive report.

The report was drafted by David Fewer, Philippe Gauvin, and Alex Cameron.

Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur St.
Ottawa, Ontario K1N 6N5
Canada
Tel: 613-562-5800 x.2553
Fax: 613-562-5417
Email: cippic@uottawa.ca



ISBN 978-0-9781083-2-8

This publication is also available on our website at www.cippic.ca and wiki at www.cippic.ca/drm.

# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

**T**his 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 discovered e-book software profiling individuals. We unexpectedly encountered DoubleClick – an online marketing firm – in a library service.
- 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 reserves the right to indiscriminately monitors its customers' communications to "check for …abusive language").

*Excessive collection, use and disclosure of personal data*

- Several organizations disclosed that they engage 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.

## PART 1 • INTRODUCTION

The new millennium has brought with it rapid technological change, particularly on the internet. Digital networks have profoundly transformed how we distribute creative works and the ways that individuals access and enjoy such works.

In the pre-digital world, individuals typically accessed creative works – such as books, magazines, newspapers, scholarly journals, paintings, and music – in tangible form by purchasing them at a retail outlet or by visiting a library.[1] In each of these examples, the characteristics of the analog world ensured that individuals were usually able to access and enjoy creative works with a high degree of privacy or anonymity, and autonomy. Once an individual had purchased or accessed an authorized copy of a creative work, it was generally up to them to determine when and under what conditions they enjoyed that work.[2] Copyright holders had no practical means to track individuals' access to and use of creative works; nor did they have any practical means to control such activities.

Digital networks have changed all of this. Many copyright holders are keen to make their works available digitally in order to exploit the efficiencies of digital distribution.[3] Individuals are also eager to explore new ways of accessing and enjoying creative works, for example by purchasing one song at a time rather than a whole album. However, many copyright holders have expressed reluctance to make their works available in digital format without a means to control the work, ostensibly to protect it against copyright infringement.[4] Many of these copyright

[1] Among other things, individuals also subscribed to cable television, rented movies and went to movie theatres.
[2] Individuals were of course subject to legal rules, including the rules of copyright law.
[3] See, for example, Neil Layton's Fading Ways label, which offers innovative distribution rules under its Share sampler series, <http://www.fadingwaysmusic.com/mission.html>.
[4] See, for example, Peter Lauria, "Bronfman Rips Jobs" New York Post (9 February 2007), <http://www.nypost.com/seven/02092007/business/bronfman_rips_jobs_business_peter_lauria.htm>: "We advocate the continued use of [digital rights management] in the protection of our and our artists' intellectual property."

holders have turned to technological tools in search of a means to control access and use of creative works in the digital environment. Known as "Digital Rights Management," or "DRM," these technological tools are changing the ways individuals interact with digital content.

DRM that is used to control distribution of an e-book, for example, might enforce a "read but don't lend" permission, restricting the ability of the individual to read the e-book on more than one computer. Other conditions that could be enforced by the DRM might include, for example: "read once," "erase in two weeks," "do not copy text," "do not print" or "do not copy." DRM might also permit creative works to be enjoyed only on a particular type of device, such as an iPod.

It is no secret that DRM technologies have spawned widespread controversy. There is a large and growing body of literature on the controversial aspects of DRM.[5] In general terms, proponents of DRM argue that DRM is necessary in order to protect the interests of copyright holders in the digital environment and to enable the development of new business models;[6] opponents of DRM have argued that DRM goes too far, placing excessive control in the hands of copyright holders in a way that upsets the balance in copyright law and poses other problems.[7] Some commentators have pointed to privacy concerns as one of the reasons why some

[5] See, generally, the resources cited in INDICARE, Natali Helberger (ed.), *State-of-the-Art Report: Digital Rights Management and Consumer Acceptability. A Multidisciplinary Discussion of Consumer Concerns and Expectations* (INDICARE, 2004), p. 126-134 <http://www.indicare.org/tiki-download_file.php?fileId=60> [INDICARE, *State-of-the-Art Report*].

[6] See, for example, Barry B Sookman, "'TPMs': A perfect storm for consumers: Replies to Professor Geist",

<http://www.mccarthy.ca/pubs/TPM_article_BSookmanV2.pdf>.

[7] See, for example, Michael Geist, "'TPMs': A perfect storm for consumers" *Toronto Star* (31 January 2005), <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article &cid=1107126609169&call_pageid=970599119419>, citing competition concerns, consumer protection, innovation issues, and freedom of expression values, among other things, as threatened by TPMs.

DRM can go too far; they have asserted that some forms of DRM use a surveillance mechanism to control access and use of creative works at the expense of individuals' privacy in connection with such activities.[8]

We do not assess the merits of the myriad issues and arguments in the controversy surrounding DRM.[9] Nor do we assess whether the use of DRM is, on balance, justified or not. Our focus in this Report is narrower: we provide a snapshot of the use of DRM in the Canadian marketplace, and assess such use against the privacy rights of Canadians. In particular, we examine how *PIPEDA* may apply to the use of DRM.

We divide this Report into four parts. In the remaining sections of Part 1, we offer a working definition of DRM, a basic overview of *PIPEDA*, "personal information" and IP addresses, an overview of the literature regarding DRM and privacy, and a description of the methodology that underlies this Report. In Part 2, we describe our investigation of the technical features of a number of DRM-enabled digital content products and services offered by a range of organizations in the Canadian marketplace. In Part 3, we offer our assessment of whether or not these organizations' use of DRM, as identified in our technical investigation, meets the requirements of *PIPEDA*. We conclude this Report in Part 4 with a summary of our findings and a call for future work in the area.

## *1.1 Working Definition of DRM*

Commentators addressing DRM in different disciplines and contexts sometimes mean different things when they use the term "DRM." DRM is thus an umbrella term that refers to an evolving category of technological systems. Although the term "DRM" does not have a standard, uniform definition, there are common threads that unite

[8] See, for example, Ian R Kerr, Alana Maurushat and Christian S Tacit, "Technological Protection Measures: Part I—Trends in Technical Protection Measures and Circumvention Technologies" (2003) at s. 5.2.2, <http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/5_e.cfm> [Kerr, Maurushat and Tacit, "Trends"].
[9] One of the important issues raised by DRM relates to competition law and policy. See, for example, Alex Cameron and Robert Tomkowicz, "Competition Policy and Canada's New Breed of 'Copyright' Law" (2007) *McGill Law Journal* [forthcoming].

the category to which it refers. At a general level, and for the purpose of this Report, "DRM" means:

> a system, comprising technological tools and a usage policy, that is designed to securely manage access to and use of digital information.[10]

By "technological tools," we refer to both hardware-based and software-based measures. In the copyright context, these tools are often called "technological protection measures" ("TPMs") or, simply, "technical measures." In this report, we distinguish between DRM systems and TPMs: DRM systems often utilize TPMs – the "technological tools" of our definition – as component parts.

The term "TPM" typically refers to technologies that control access to or use of information, or both.[11] A TPM that controls access to information might be as simple as a password protection. More complex access-control TPMs use encryption to regulate access to information by encrypting it and permitting decryption and access only by authorized individuals or devices.

Use-control TPMs control the uses that can be made of a work after an individual accesses it. The most common type of use-control TPM is a copy-control mechanism which regulates or prevents duplication of all or part of a work. Macrovision technology, for example, is a copy-control technology which prevents or distorts copying of Macrovision-protected DVDs.[12]

---

[10] We draw inspiration for this definition from Kerr, Maurushat and Tacit, "Trends," *supra* note 8, section 5.0, and from INDICARE, *State-of-the-Art Report*, *supra* note 5, p. 1. We use the term "information" intentionally to draw attention to the fact that DRM systems can be used in association with any type of information. It need not be information which is protected by copyright law.
[11] Kerr, Maurushat and Tacit, "Trends," *supra* note 8.
[12] *Ibid.*; Marcrovision, "Analog content protection for DVD," <http://www.macrovision.com/products/activereach_dvd/acp/index.shtml>.

By a "usage policy," we refer simply to the "rules of use" that the DRM enforces. Such policies might include rules like "do not copy," "play for two weeks," or "install only on this machine." These usage rights that are managed by DRM can be complex and go far beyond simple access and copy-control TPMs that may form part of a DRM system. For example, in connection with the usage policy, the DRM system may contain a payment system which processes payments for specific licensed rights in relation to content.[13]

### *1.2 PIPEDA, "Personal Information" and Internet Protocol Addresses*

*PIPEDA*[14] is a data protection law enacted at the federal level in Canada. The purpose of the legislation is set out in section 3 of the Act.[15] *PIPEDA* is intended to regulate the collection, use and disclosure of "personal information" such as that which may occur with DRM technologies.

Schedule 1 to *PIPEDA* sets out a series of obligations that organizations must adhere to. These are divided into ten principles as follows: (1) Accountability, (2) Identifying purposes, (3) Consent, (4) Limiting collection, (5) Limiting Use, Disclosure, and Retention, (6) Accuracy, (7) Safeguards, (8) Openness, (9) Individual access, and (10) Challenging compliance. In addition to these obligations, sub-section 5(3) of *PIPEDA* sets out an overarching limit regarding all commercial activities that involve

[13] See, generally, Niels Rump, "Digital Rights Management: Technological Aspects–Definition, Aspects, and Overview" in Eberhard Becker *et al.*, eds., *Digital Rights Management-Technological, Economic, Legal and Political Aspects* (Springer, 2003).
[14] Personal Information Protection and Electronic Documents Act, 2000 *Statutes of Canada* ch.5, <http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-8.6///en> [PIPEDA].
[15] PIPEDA, *supra* note 14, section 3. "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

the handling of personal information – these activities must be undertaken for "appropriate" purposes.[16]

There are three primary considerations that need to be satisfied before *PIPEDA* will apply to information practices in a given situation: the matter must be within the jurisdiction of *PIPEDA*, the matter must involve commercial activities, and the information at issue must be "personal information." This Report does not analyze the former two requirements. However, an understanding of "personal information" is crucial for the analysis which follows in this Report.

*PIPEDA* applies to the collection, use and disclosure of "personal information." This term is broadly defined in the legislation as follows: "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." The meaning of "personal information" arises in every matter under *PIPEDA*. In some cases, it is obvious that the information at issue meets the definition of "personal information" However, in the context of technologically-mediated or technologically-generated information – such as that collected via DRM systems – it is not always so obvious.

### 1.2.1 Internet Protocol Addresses as "Personal Information"

When computers communicate on the internet and other networks, they do so using "internet protocol" (IP) addresses. Under the current architecture of the internet, an IP address is a unique number comprised of four numbers (each between zero and 255) separated by dots: *e.g.* 120.0.54.19. Each computer is assigned a unique IP address while it is connected to the internet. This address may be different each time the computer connects to the internet because many internet service providers (ISP) assign IP addresses dynamically. This means that an individual using a computer to

[16] PIPEDA, *supra* note 14, s. 5. "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

browse the internet may be assigned a different IP address each time the computer is connected to the internet.

IP addresses are one type of information that a DRM system may collect from an individual accessing DRM-protected content. Thus, it is important to consider whether IP addresses can be considered "information about an identifiable individual."

Other jurisdictions have taken the view that IP addresses are personal information. For example, the European Union Data Protection Working Party has unequivocally concluded that IP addresses are personal data:

> The Working Party wishes to emphasize that IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66....
>
> In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means.[17]

On first impression, IP addresses also appear to meet the definition of "personal information" under *PIPEDA*. IP addresses, at a given time, identify the computer of an individual connected to the internet. Knowing the IP address of a computer at a given time can lead to a tremendous amount of information about the activities of an individual on the internet. An IP address is a key to discovering information about individuals' online activities and their identities.

[17] Article 29 Data Protection Working Group, "Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPV6" (30 May 2002), <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf>, p 3.

In *BMG v. Doe*,[18] the Federal Court of Appeal refused to order ISPs to disclose the identity of their customers in the context of alleged copyright infringement on p2p networks. Members of the Canadian Recording Industry Association (CRIA) had requested this disclosure. Armed principally with IP addresses and specific times that the allegedly infringing activities had taken place, CRIA sought to identify the individuals responsible. The lower court refused to order disclosure:

> Without any evidence at all as to how IP address 24.84.179.98 has been traced to *Geekboy@KaZaA*, and without being satisfied that such evidence is reliable, it would be irresponsible for the Court to order the disclosure of the name of the account holder of IP address 24.84.179.98 and expose this individual to a law suit by the plaintiffs….
>
> [G]iven the age of the data, its unreliability and the serious possibility of an innocent account holder being identified, this Court is of the view that the privacy concerns outweigh the public interest concerns in favour of disclosure.[19]

On appeal, the Federal Court of Appeal agreed with the lower court's criticism identified in this passage and refused to order disclosure of identity information.[20] It

[18] *BMG Canada Inc v John Doe*, 2005 FCA 193, <http://reports.fja.gc.ca/en/2005/2005fca193/2005fca193.html>, 252 *Dominion Law Reports* (4th) 342 [*BMG Canada v Doe*, FCA].
[19] *BMG Canada Inc v John Doe*, 2004 FC 88, <http://reports.fja.gc.ca/en/2004/2004fc488/2004fc488.html>, 3 Federal Court 241, para. 20.
[20] *BMG Canada v Doe*, FCA, *supra* note 18, para. 21. "Much of the crucial evidence submitted by the plaintiffs was hearsay and no grounds are provided for accepting that hearsay evidence. In particular, the evidence purporting to connect the pseudonyms with the IP addresses was hearsay thus creating the risk that innocent persons might have their privacy invaded and also be named as defendants where it is not warranted. Without this evidence there is no basis upon which the motion can be granted and for this reason alone the appeal should be dismissed."

is evident from this case and others like it[21] that an IP address will in almost every case, if not every case, be "personal information." In *BMG v. Doe*, the IP addresses were either information about the targeted individuals, or information about innocent account holders; in either case, the IP addresses were "about an identifiable individual."

In several case summaries, the Office of the Privacy Commissioner of Canada has held that an IP address can constitute "personal information" for the purposes of *PIPEDA* when it can be associated with an identifiable individual. Other commentators have confirmed this view.[22] In an early case, the former Commissioner dealt with a complaint regarding the collection of information from an individual's computer without his consent. The Commissioner noted the following:

> If an IP address is traced, it allows access to information such as Web sites visited by the computer's user or recent passwords used in obtaining access to secure accounts. The likelihood of tracing an IP address is small if the user has dial-up Internet access, but significantly greater if the user has a fixed Internet connection via a cable modem, as was the case with the complainant.[23]

In Case Summary #315,[24] the Commissioner was again faced with the question of whether an IP address is personal information. In this case, an individual requested

[21] See, for example, *Irwin Toy Ltd. v. Doe* [2000] O.J. No.3318 (S.C.J.).
[22] See, for example, David TS Fraser, "IP addresses are personal information" (29 January 2006) Canadian Privacy Law Blog, <http://www.privacylawyer.ca/blog/2006/01/ip-addresses-are-personal-information.html>. "I don't think there can be much doubt that an IP address is 'personal information' for the purposes of PIPEDA or the Personal Information Protection Acts of BC and Alberta, particularly as it appears in a server log. The information does not have to 'identify' an individual, but must be 'information about an identifiable individual."
[23] Privacy Commissioner of Canada, "PIPEDA Case Summary #25: A broadcaster accused of collecting personal information via Web site" (20 November 2001), <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp>.
[24] Privacy Commissioner of Canada, "PIPEDA Case Summary #315: Web-centred company's safeguards and handling of access request and privacy complaint questioned" (9 August 2005), <http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp> [Privacy Commissioner, "Summary #315"].

information from her email service provider in the course of attempting to determine whether another person had accessed her email account without her permission. She asked the email service provider to provide the IP addresses of the computers that had accessed her account over a given time period so that she could then take steps to identify the person responsible. This approach parallels the issues that arose in *BMG v. Doe*. As to the question of whether these IP addresses were "personal information," the Commissioner held as follows:

> […] the IP address does form part of the account information and should be released to the account holder (when she or he requests it). The account holder is then free to pursue identifying the individual through legal channels. As for whether the IP address is third party personal information, assuming that there is in fact a third party, **it is the personal information of both the account holder and the third party**.[25]

The IP addresses of the computers used to access the complainant's email account were thus held to be personal information of both the complainant (as the account holder) and the as yet unknown third party who had accessed her account.

In Case Summary #319,[26] the Commissioner had to resolve a complaint that an ISP was reading, *inter alia*, the complainant's originating and destination IP addresses when he was sending email messages. The complainant claimed that this was being done without his consent in violation of *PIPEDA*. In making her determinations, the Commissioner confirmed that IP addresses, even ones that are assigned dynamically, can be personal information. In this case, the originating IP address identified the complainant. The Commissioner also found that the ISP needed to know the destination IP address in order to deliver email messages. In the result, however,

[25] Privacy Commissioner, "Summary #315," *supra* note 24 [emphasis added].
[26] Privacy Commissioner of Canada, "PIPEDA Case Summary #319, ISP's anti-spam measures questioned" (8 November 2005), <http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.asp>.

she held that by virtue of sending email messages, the complainant had consented to the ISP reading the IP addresses at issue.

The Commissioner has also published materials which are consistent with the view that IP addresses are personal information. In the fact sheet titled "Protecting Your Privacy on the Internet,"[27] the Commissioner advises individuals to "surf anonymously by using third party software that hides [their] real IP address," in order to protect their privacy online.

Understanding that IP addresses are "personal information" is critical to an understanding of DRM's potential privacy implications. Organizations that do not appreciate that IP addresses and related technical information constitute "personal information" may fail to comply with *PIPEDA* in a number of areas when they do not treat the collection, use and disclosure of such information through DRM as being subject to *PIPEDA*.

### *1.3 DRM & Privacy*

This section provides a brief overview of some of the issues emerging from the existing literature regarding DRM and privacy. This Report does not take a position with respect to this literature. The conclusions reached in this Report are in many instances different than the conclusions reached by others who have studied other forms of DRM at different times. Indeed, the very purpose of this Report is to objectively and impartially consider the current state of the marketplace in Canada with a view to the potential privacy implications of DRM systems that may be in use. Nevertheless, the existing literature is useful in providing a framework for thinking about how some DRM systems may implicate privacy.

At a general level, DRM can implicate privacy because the overarching objective of many DRM systems is to regulate *who* is authorized to access and to use information

[27] Privacy Commissioner of Canada, "Protecting Your Privacy on the Internet" (6 November 2003), <http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp>.

in accordance with the usage policy. Although it is possible that "personal information" need not be involved in managing rights in relation to information,[28] many commentators have asserted that DRM collects personal information by the very nature of its functionality.[29] For example, each time an individual requests access to or use of a creative work, the DRM system might permit the requested action only after "phoning home"[30] to the content distributor to verify that the individual[31] matches the identity of an individual who has been authorized to engage in the requested activity.

DRM may also utilize surveillance functionality to monitor the activities of particular individuals accessing or using DRM-protected works, or to monitor how different individuals use a particular work.[32] Tracking how content is being used (and attempted to be used) can be thought of as a potentially integral part of how content is controlled and managed through DRM.[33] Others who have studied real-world implementations of DRM have substantiated the privacy concerns associated with DRM monitoring.[34]

---

[28] We will return to this issue at the conclusion of this Report.
[29] See, for example, LA 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* 418-446 (Springer, 2003).
[30] Graham Greenleaf, "IP, Phone Home: The Uneasy Relationship Between Copyright and Privacy, Illustrated in the Laws of Hong Kong and Australia," (2002) 32:1 *Hong Kong Law Journal* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=884329>, p. 35.
[31] Or their computer or other device.
[32] See, for example, Ian R Kerr, "If Left to Their Own Devices…How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy," in Michael Geist, ed., *In the Public Interest* (Irwin Press, 2005) 167-210.
[33] Julie Cohen, "DRM and Privacy" (2003) 18:2 *Berkeley Technology Law Journal* 575-617, <http://btlj.boalt.org/data/articles/18-2_spring-2003_symp_cohen.pdf>, pp 584-585 [Cohen, "DRM and Privacy"], citing several examples of DRM systems that monitor individuals.
[34] Deirdre K Mulligan, John Han and Aaron J Burstein, "How DRM-Based Content Delivery Systems Disrupt Expectations of 'Personal Use,'" <http://www.law.berkeley.edu/clinics/samuelson/projects_papers/WPES-RFID-p029-mulligan.pdf>. "[…] using the services studied initiates highly complex webs of information monitoring and exchange. For example, the number of advertising partners Pressplay engages with is unclear. However, it is clear that usage of the service involves interaction with a minimum of four separate entities with a minimum of four separate policies governing use of information collected about users. The other services examined all exhibit similar degrees of complexity."

The collection of information about accesses to and uses of creative works raises obvious privacy concerns. This type of information can reveal a great deal about an individual and can be used (and abused) in a number of different ways. Justice Lebel characterized information about an individuals' internet surfing and downloading habits as revealing of "core biographical" information about a person.[35]

The context in which DRM is deployed potentially challenges reasonable expectations of privacy. DRM is often employed in unexpected places, in contexts in which individuals are accustomed to anonymity and privacy in their enjoyment of creative works, for example in their own homes. The ability to engage in anonymous activity, particularly access to and enjoyment of creative works, raises a host of questions about which there is little agreement.

In the context of access to information, including creative works, the debate surrounding anonymity is particularly heated.[36] On the one hand, there is no question that anonymity has value in facilitating intellectual exploration and the development of new ideas and new creative works. Individuals' choices about what intellectual materials they access are influenced by whether or not they can access them anonymously. Surveillance (*i.e.*, a lack of anonymity) in this context chills individuals' access to intellectual materials and may lead them away from accessing many forms of information.[37] The ability and the legal right to speak anonymously

---

[35] *Society of Composers, Authors and Music Publishers of Canada* v *Canadian Assn of Internet Providers*, 2004 SCC 45, <http://scc.lexum.umontreal.ca/en/2004/2004scc45/2004scc45.pdf> [*Society of Composers, Authors and Music Publishers of Canada* v *Canadian Assn of Internet Providers*], para. 155. LeBel J, dissenting: "[an individual's surfing and downloading activities] tend to reveal core biographical information about a person. Privacy interests of individuals will be directly implicated where owners of copyrighted works or their collective societies attempt to retrieve data from Internet Service Providers about an end user's downloading of copyrighted works."

[36] See Ian R Kerr and Alex Cameron, "NYMITY, P2P & ISPS: Lessons from *BMG Canada Inc v John Doe*" in Katherine J Strandburg and Daniela Stan Raicu, eds., *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Springer, 2005), <http://ssrn.com/abstract=726764> [Kerr and Cameron, "NYMITY" (cited to SSRN)].

[37] Cohen, "DRM and Privacy," *supra* note 33, pp. 580-581.

and to receive information anonymously are instrumental in exercising an effective right of freedom of expression. This topic has received much attention in the United States.[38]

On the other hand, from the perspective of intellectual property holders, individuals' anonymity in connection with access to creative works in the digital networked environment has arguably contributed to widespread infringement of intellectual property rights. Anonymity can be used to "cloak the identity of someone revealing a trade secret, or distributing pirated copies of copyrighted intellectual property...."[39] Anonymous p2p file-sharing of video games, movies and other copyrighted works is the most well-known example of this problem from the perspective of copyright holders.

Not surprisingly, some iterations of DRM may resolve the question of anonymous access to creative works in favour of the copyright holder. DRM can involve a design choice to pierce the anonymity of individuals wishing to gain access to creative works. The goal is to either prevent the possibility of unauthorized use of works from occurring, or to ensure that those engaging in unauthorized activities are held accountable for their actions. This piercing of anonymity obviously comes at the cost of the valuable aspects of anonymity discussed above.

The design choice to pierce anonymity using DRM is not a necessary choice or foregone conclusion. It is one choice among many. Content protection does not require information about the identity of individuals accessing that content. A

[38] See generally Kerr and Cameron, "NYMITY", *supra* note 36; Julie Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace", (1996) 28:4 *Connecticut Law Review* 981-1039, <http://ssrn.com/abstract=17990>.
[39] A Michael Froomkin, "Anonymity in the Balance" in C Nicoll, Corien Prins and MJM van Dellen, eds., *Digital Anonymity and the Law* (TMC Asser Press, 2003).

number of proposals have been made for privacy- and anonymity-respecting DRM systems.[40] The Privacy Commissioner of Canada has noted this point:

> Alternatives exist that would provide copy protection and at the same time protect privacy. For instance, token and password systems could be used to authorize a download of digital content. Alternative, non-privacy invasive solutions do not appear to have been explored adequately, and this is what we must demand of DRM systems that are deployed in Canada."[41]

Concerns about DRM's potential privacy implications have led privacy regulators and policy-makers to focus increased attention on the matter. For example, the European Union Data Protection Working Party recently considered the issue:

> The Working Party is concerned about the fact that the legitimate use of technologies to protect works could be detrimental to the protection of personal data of individuals. As for the application of data protection principles to the digital management of rights, it has observed an increasing gap between the protection of individuals in the off-line and

[40] For a description of some of these proposals, see Alex Cameron, "Infusing Privacy Norms in DRM: Incentives and perspectives from law" in Yves Deswarte *et al.*, eds., *Information Security Management, Education and Privacy, IFIP 18th World Computer Congress, TC11 19th International Information Security Workshops, 22-27 August 2004, Toulouse, France* (Kluwer Academic Publisher, 2004), available at <http://www.idtrail.org/files/Alex_Cameron-Infusing_Privacy_Norms_in_DRM.pdf>. Credentica, a Montreal security software developer focusing on identity and access management, recently released a product called U-Prove, a user-centric identity management tool. See "Credentica Releases Software Product for User-Centric Identity Management" (13 February 2007) <http://www.emediawire.com/releases/2007/2/emw504697.htm>. The Privacy Commissioner of Canada has also expressed this view: see Privacy Commissioner of Canada, "Digital Rights Management and Technical Protection Measures" (November 2006), <http://www.privcom.gc.ca/fs-fi/02_05_d_32_e.asp> [Privacy Commissioner of Canada, "DRM Fact Sheet"].

[41] Privacy Commissioner of Canada, "DRM Fact Sheet", *supra* note 40.

> on-line worlds, especially considering the generalised tracing and profiling of individuals.[42]

Canada's privacy community has also voiced strong concern over DRM's potential for collecting, using and disclosing personal information, particularly in the context of possible legislation that would protect DRM.[43] This concern has been echoed by a number of Canada's privacy commissioners.[44]

DRM and privacy values need not necessarily prove antagonistic. Future DRM applications may well include interesting pro-privacy features that merit consideration. It has long been known that content protection does not require information about the identity of individuals accessing that content.[45] A number of

---

[42] Article 29 Data Protection Working Party, "Working document on data protection issues related to intellectual property rights WP104" (18 January 2005), <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf>, p. 8.

[43] See, for example, Canada's Privacy Community, "Letter from Privacy Community of Canada to Ministers Bernier and Oda," (17 May 2006) <http://www.intellectualprivacy.ca/documents/open_letter.pdf>. Canada's Privacy Community, "Background Paper: Critical Privacy Issues In Canadian Copyright Reform" (17 May 2006) <http://www.intellectualprivacy.ca/documents/background_paper.pdf>. In the interest of full disclosure, CIPPIC participated in the drafting of the Open Letter and Background Paper. See also INDICARE, *State-of-the-Art Report*, *supra* note 5, pp. 22-24.

[44] See, for example, Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Ministers Oda and Bernier (17 May 2006), <http://www.privcom.gc.ca/media/let/let_ca_060517_e.asp>; Letter from David Loukidelis, Information and Privacy Commissioner of British Columbia, to Ministers Oda and Bernier (17 May 2006), <http://www.oipcbc.org/publications/Comm_Public_Comments/F06-28751.pdf>; Open Letter from Ann Cavoukian, Information and Privacy Commissioner of Ontario, to Ministers Oda and Bernier (12 May 2006), <http://www.ipc.on.ca/docs/drmletter.pdf>; Letter from Frank Work, Information and Privacy Commissioner of Alberta, to Ministers Oda and Bernier (26 May 2006), <http://www.oipc.ab.ca/ims/client/upload/Copyright_ltr_May_26_06.pdf> The Office of the Privacy Commissioner of Canada has also since issued a Fact Sheet regarding DRM that includes the following statement: "The use of TPMs, however, can seriously affect the privacy rights of individuals, and by invading their privacy and reporting on their behaviour, impact other civil liberties such as freedom of association and freedom of expression. While rights holders have a perfectly legitimate view of the matter, it is also reasonable to expect them to enforce their rights only in a way which respects individual privacy rights." See Privacy Commissioner of Canada, "DRM Fact Sheet", *supra* note 40.

[45] See, for example, INDICARE, *State-of-the-Art Report*, *supra* note 5, citing P Vora, D Reynolds, I Dickinson, J Erickson, D Banks, "Position Paper: Privacy and Digital Rights Management," (2002) Workshop on Digital Rights Management for the Web, World Wide Web

proposals have been made for privacy-enhancing and anonymity-respecting DRM systems – technological designs to protect anonymity while aiding in fraud prevention have been around for many years.[46] For example, privacy can be infused into the technology design process and into the process of DRM standards-setting, a process which is ongoing.[47] Some commentators have offered specific examples of how this might be achieved: "[a] DRM system should provide easy pseudonymization that can be used to key databases."[48] This type of activity may already be taking place. However, the pseudonymization or alleged anoymization of data must pass the definition of "personal information" in *PIPEDA*. This will usually mean that IP addresses and other personal information must not be collected if they can be linked to an "ID" in a database, or to other potential personal information. Some years ago, the Information and Privacy Commissioner of Ontario published a guide to injecting privacy into DRM.[49]

This Report aims to explore the use of DRM in the Canadian marketplace and to determine whether and how DRM might implicate privacy, possibly including some of the ways described in the existing literature.

## *1.4 Methodology*

### 1.4.1 Selecting Products for Investigation

We surveyed the Canadian marketplace with a view to identifying and researching sectors that design and deploy DRM. We reviewed online and offline markets for: musical sound recordings, including both content-controlled CDs and online download

---

Consortium, 22-23 January 2001 INRIA - Sophia-Antipolis, France; <http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html>.

[46] See generally Stefan Brands, *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy* (MIT Press, 2000).

[47] See, generally, Cohen, "DRM and Privacy," *supra* note 33.

[48] J Feigenbaum, JE Freedman, T Sander and A Shostack, (2002) "Privacy Engineering in Digital Rights Management Systems," Proceedings of the 2001 ACM Workshop on Security and Privacy in Digital Rights Management, Berlin, LNCS Vol. 2320, pp. 76-105, <http://www.homeport.org/~adam/privacyeng-wspdrm01.pdf>.

[49] A Cavoukian, Information and Privacy Commissioner of Ontario, "Privacy and Digital Rights Management (DRM): An Oxymoron?" (2002) <http://www.ipc.on.ca/docs/drm.pdf>.

and subscription services; motion pictures and television (DVDs and downloads); interactive video games; office productivity software; electronic publishing (including electronic newspaper articles and "e-books"); library services; and peer-to-peer networks.

We used externally-compiled lists of market participants in various categories of media from which to draw a sample for investigation. Where possible, we selected the market participants with the greatest market share. In no case was a particular market participant or DRM technology targeted.[50]

### 1.4.2 Technical Investigations

The procedures used to investigate the DRM of various products required a combination of hardware and software tools to create the necessary test bed setup. A detailed flowchart of investigation procedures was then created to ensure that all products were investigated in a controlled manner. Care was taken to create a series of procedures that would closely mimic the installation, use and uninstall steps that would normally be taken for each investigated product.

#### *1.4.2.1 Hardware Setup*

Software can be designed to alter its behaviour when it detects that it is running under investigation tools such as virtual machines (like VMware).[51] We have therefore tried to make our investigation as transparent as possible to our test machine to create a controlled environment. The test bed was made up of two computers: (1) a gateway and monitoring machine; and (2) the actual testing machine.

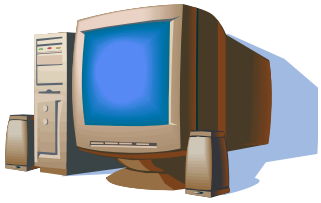
[50] The exception to this rule occurred in our pilot testing, where we selected a particular DRM implementation—the Sony XCP DRM—with known technological features and privacy concerns to help confirm the effectiveness of our technical assessment methodology.
[51] Greg Keiser, "Hackers Use Virtual Machine Detection to Foil Researchers" (20 November 2006) *Information Week*, <http://www.informationweek.com/software/showArticle.jhtml?articleID=194500277>.

Installed Software:

- RegSnap
- Rootkit Revealer

Installed Software

- Ethereal
- Squid proxy
- Cisco VPN



↔

↔

Testing Computer

MS Windows XP

Gateway Computer

Kubuntu Linux 6.06.1

Internet

The gateway machine was running Kubuntu Linux 6.06.1 and was masquerading network traffic for the testing machine. As described in the next paragraphs, extra software was installed on the gateway machine in order to make the network setup transparent to the testing computer and closer to the type of internet connection that a home user would have.

A Squid proxy was set up on the gateway machine, which transparently redirected all requests to the University of Ottawa web proxy. Port 80 on the monitoring machine was forwarded to the Squid port on the gateway machine, thus making the proxy transparent to the testing machine. A Cisco VPN client was also installed on the gateway machine in order to open up more ports. Although we expected most traffic to go through port 80, it was important to open as many ports as possible in order to capture all communications to and from the testing machine. In our lab, most common ports are closed off unless the VPN software is installed and running. For example, without the VPN software we would not have been able to capture SSL

traffic on port 443. The existence of the VPN client was unknown and transparent to the testing machine.

Ethereal v. 0.99.0 was used on the gateway machine in order to monitor the network traffic. There were two separate physical network interfaces in the gateway machine. One was connected directly to the testing machine through a crossover cable and the other was connected to the University of Ottawa network. The testing machine and the gateway machine were on their own subnet. When using Ethereal, only the network interface connected to the testing machine was monitored. This effectively reduced our packet logs to only those packets being transferred to and from the testing machine. Other traffic on the University of Ottawa network was not recorded.

The hard drive on the testing machine contained two partitions, one for Windows and one for Linux. The Windows partition was for the actual DRM investigation while the Linux partition was simply used to facilitate re-imaging of the Windows partition. PartImage v. 0.6.4 running on the Linux partition was used for both creating the Windows drive images as well as re-imaging the Windows partition between every investigation. This not only meant that we had a clean operating system for each investigation but also ensured that Windows updates were at the same level for each investigation. Windows XP on our test bed had full security updates up to February 7, 2007.

#### *1.4.2.2 Software Tools*

Our primary monitoring tool was Ethereal v. 0.99.0. Ethereal is a real-time protocol analyzer that allows a user to monitor various types of network traffic. We used Ethereal situated on the gateway computer to monitor the communications to and from the testing computer and the internet. In this manner we were able to record the packets between the DRM and the outside world. By using some of the built-in utilities within Ethereal and through the creation of some customary scripts, we were able to determine some interesting data about what information was being sent, and to whom.

Rootkit Revealer was run at several steps of our investigation procedure to ensure that no obvious rootkits were installed. Our investigations did not reveal any rootkits in the investigated products.

RegSnap is a simple utility that makes it very easy to compare snapshots of the Windows Registry and file structure. At various times throughout the investigation procedures, a Windows snapshot would be taken and stored for later comparison. On collection, the utility quickly copies the entire windows registry along with specific files including the Windows System directories.

#### *1.4.2.3 Investigation Procedures*

We undertook our investigations between the months of January and March of 2007. A specific set of procedures were developed. The investigation included all the basic functions of a piece of software including: installing, registering, uninstalling, and using the product. Snapshots of the registries and system directories were taken at important intervals and the network traffic was monitored continuously. For all the important steps, registry snapshots were taken before and after, in order to assess any changes. The complete investigation flowchart is shown below in Figure 1.

Where the user was given the option of accepting a contract such as an End User License Agreement or entering personal information such as an email address, both options were investigated. The system was monitored to see if we could observe a difference in behaviour due to these choices. Throughout the investigation, we paid particular attention to the network traffic using Ethereal.

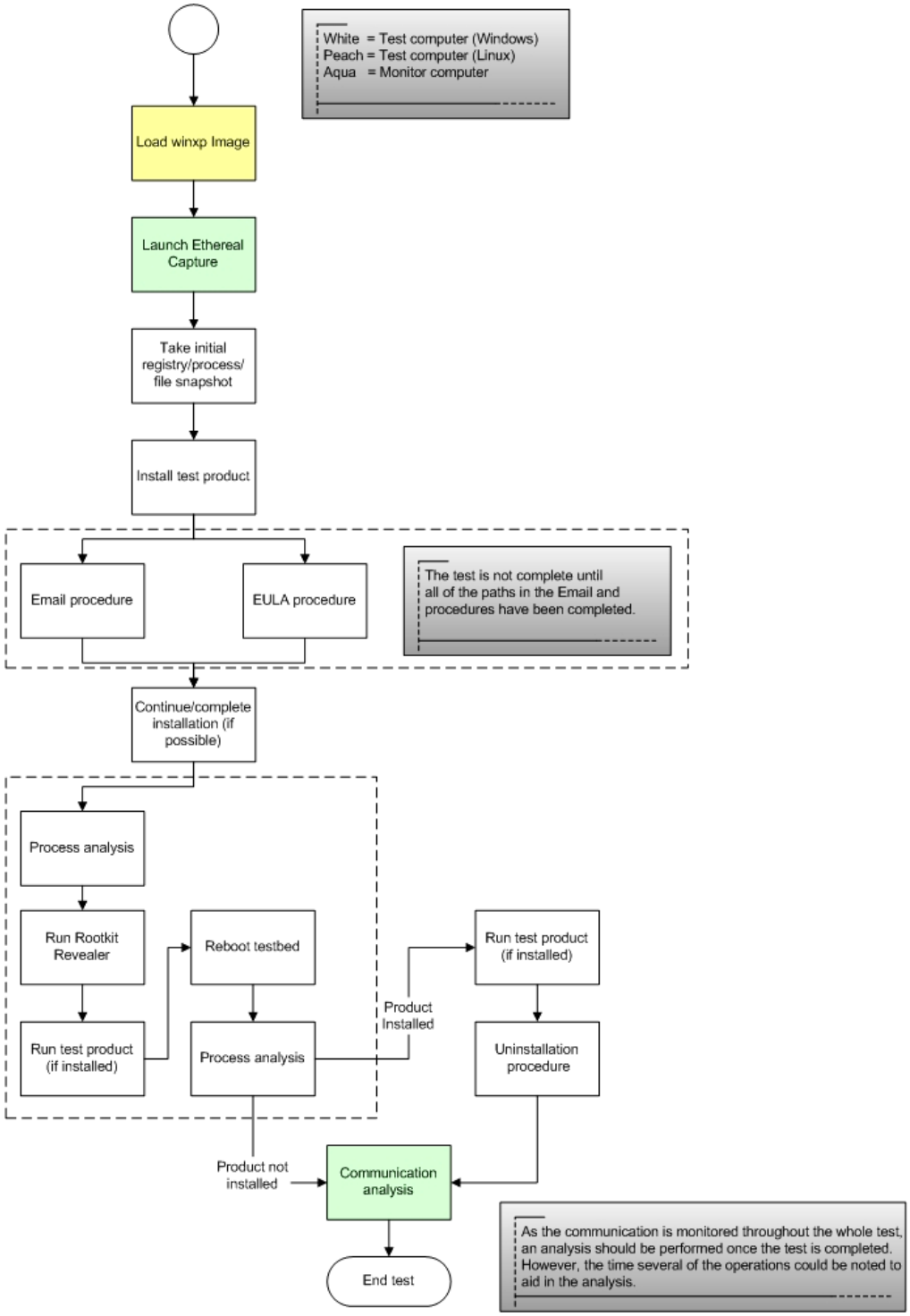



**Figure 1: Investigation Procedure Flowchart**

### 1.4.3 PIPEDA Assessments

The twelve organizations that were found to have engaged in automatic communications of information through the apparent use of DRM were assessed against the requirements of *PIPEDA*. Organizations using DRM that did not result in such communications were not assessed.

University of Ottawa law students and CIPPIC counsel acting as ordinary users of the DRM ("Assessors") conducted the *PIPEDA* assessments in March, 2007. The assessments analyzed organizations' compliance with the following *PIPEDA* Principles:

(a) s. 5(3) (Appropriate Purpose);
(b) Principle 4.2 (Identifying Purposes);
(c) Principle 4.3 (Consent);
(d) Principle 4.4 (Limiting Collection);
(e) Principle 4.5 (Limiting Use, Disclosure and Retention);
(f) Principle 4.8 (Openness);
(g) Principle 4.1 (Accountability); and
(h) Principle 4.9 (Individual Access).

Assessors performed each assessment by: (a) reviewing the data derived from the technical investigations described in the previous section; (b) reviewing license agreements, privacy policies and other information communicated during the installation and use of the DRM-protected content; (c) submitting an access request for their personal information by contacting the organization at the privacy contact the organization provided, usually through an email address; (d) submitting a follow-up inquiry to the organization to obtain more specific information about the operation of the DRM in relation to personal information; and (e) reviewing the results of steps (c) and (d). Steps (c) and (d) followed a set script.

CIPPIC counsel reviewed all of the *PIPEDA* assessments and then synthesized and summarized the results in the form that appears in Part 3 of this Report.

# PART 2 • TECHNICAL INVESTIGATION RESULTS

## *2.1 Introduction*

In presenting the results of our technical investigations in this Report, it is helpful to draw a distinction between what we have coined as "autonomous DRM" and "net-dependent DRM." Although useful for presenting the results here, this distinction did not factor into our technical investigations or our *PIPEDA* assessments substantively in any way.

> *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.

In our technical investigations, we found 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 communicated with external computers.

We also found that a number of the DRM products we investigated communicated with the same third parties: Akamai Technologies, Omniture and DoubleClick. Based on additional research, we were able to learn more about these companies. We

found that they partner with e-businesses to, among other things, process information, deliver content, offer web analytics services or deliver advertising.

Finally, our analysis of one of the net-dependent products that we investigated revealed that our username, login password and email address were communicated unencrypted over the internet.

### *2.2 Autonomous DRM*

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 assessment revealed that these communications appeared in most cases to be linked to advertising and web metrics.

Consider our investigation of Disney's *Pirates of the Caribbean* DVD (disc 2). When we inserted the DVD, a pop-up window appeared asking us to install the Interactual Player, software that plays DVDs on computers. Once we installed the software, a configuration window appeared with a tab marked "Privacy." We deselected all agreements to information transfers. Nonetheless, we captured communications to InterActual servers. Indeed, the software placed a cookie onto our test computer. The cookie itself can only be read by an InterActual website, but this does mean that InterActual may have collected our IP address, web browser and operating system information through the cookie request from our computer. As the InterActual interface window does not go through a web browser, it is likely that an unsophisticated user would not know that he or she is downloading advertising from the internet or delivering information to InterActual.

Our investigation of Sony BMG's "Our Lady Peace – *Healthy in Paranoid Times*" CD revealed similar results. As we played songs in Sony's included software player, our

test computer connected to a SunnComm server.[52] Although we cannot conclusively state that this connection is advertising-related, others have studied a different DRM system that connected to SunnComm's servers:

> Apparently a bug in the server software prevents it from returning any useful information. However, the name "Perfect Placement" in the URL provides a valuable clue about the server's purpose. A SunnComm web page describes "Perfect Placement" as a MediaMax feature that allows record labels to "[g]enerate revenue or added value through the placement of 3rd party dynamic, interactive ads that can be changed at any time by the content owner." Presumably the broken site is supposed to return a list of ads to display based on the disc ID.[53]

SunnComm can also collect a user's IP address, information about their operating system and web browser, and the time of the communication. In addition to this information, an ID number is sent to SunnComm. The number we sent during our investigation differed from that sent by Haldermann in the study from which the passage above originates. As suggested by Haldermann, this is probably a disc ID number to allow SunnComm to know what we are listening to and deliver advertising accordingly.

## *2.3 Net-dependent DRM*

### 2.3.1 Products Purchased in Physical Form

*Net-dependent DRM* systems rely on internet communications to fulfill their rights management purposes. Most of the *net-dependent* DRM products that we purchased

[52] While this is not the Sony rootkit, issues regarding SunnComm/MediaMax DRM have been brought to light by Professors J Alex Haldermann and Ed Felten. See J Alex Haldermann, "Sony shipping spyware from SunnComm, too" (12 November 2005), <http://www.freedom-to-tinker.com/?p=925&akst_action=share-this> [Haldermann, "Sony shipping spyware"].
[53] Haldermann, "Sony shipping spyware," *supra* note 52.

from bricks-and-mortar stores ("store-bought products") required internet authentication. Whereas *autonomous DRM* authentication usually requires a user to enter a valid identification key as pre-determined by the software, *net-dependant DRM* goes one step further and, for example, cross-references this key with a database to ensure that the key is not already being used by another user.

Our investigation revealed that many store-bought net-dependent DRM-protected products allow users a limited number of uses or limited functionality; others simply will not work until authenticated *via* the internet or sometimes by telephone.

One notable exception in the store-bought products that we investigated, however, was the computer game *Half-Life 2* created by Valve Software. This video game can be played on a personal computer by a single user; to our knowledge, there is no game-related technical need for an internet connection. However, *Half-Life 2* requires an internet connection and the installation of "Steam," Valve's proprietary online content delivery and validation platform. During the full installation Half-Life 2 and ten minutes of play, we captured nearly 100 000 packets of information communicated to and from Valve Software.

Other than the validation of our CD-Key, many of the communications captured during investigation of Half-Life 2 were related to software updates from Steam as well as delivery of advertising linked with the Steam platform. Some of the communications remain unexplained, however. When we first ran the game, our test computer requested a Certificate Revocation List from a Microsoft server. It also did so during play. It could be that Steam continually verifies that a user's software is legitimate during play. Also, when we uninstalled Steam a few packets were sent to a Valve server. The reason for this communication is currently unknown.

### 2.3.2 Online Products and Services

Online content subscription services such as the Ottawa Public Library (OPL) and Napster deploy digital licenses to allow the use of locked content. The downloaded content (an audiobook in the case of OPL and a music file in the case of Napster) is

also tied to an online platform. For example, our investigations revealed that if a user pays for a one-month subscription with Napster and tries to play Napster-acquired songs through Windows Media Player while Napster is uninstalled, then the digital license attached to the song will require the reinstallation of Napster. This is not a format issue; songs can be played outside of Napster. If Napster is installed on a user's computer, the user can play Napster-acquired songs through other platforms such as Windows Media Player.

All of our investigations involving online services revealed communications to third party sites belonging to companies such as Akamai Technologies, Omniture and DoubleClick. Although we know something about the general nature of these businesses, we do not know what information was sent to them.

As noted in our privacy assessment results below, even though almost all of the net-dependent DRM that we investigated (other than the store-bought Intuit Quicktax) communicated to third parties, at no time were we actively informed of the existence of these third parties or that information would be communicated to or from them.

## PART 3 • PRIVACY ASSESSMENT RESULTS

### *3.1 Overview*

Our privacy assessments disclosed a wide range of practices and varying degrees of compliance with *PIPEDA*.[54] Some organizations that we assessed performed poorly on their most basic obligations under *PIPEDA*. For example, only two organizations – Microsoft and the Ottawa Public Library – complied with our request to identify

[54] Although we endeavoured to focus our PIPEDA assessments on the privacy concerns raised by the use of DRM, it was sometimes difficult in practice to prevent our assessment of an organization's DRM-related privacy practices from devolving into an assessment of the organization's general privacy practices. This point is obvious upon reflection. Organizations develop "privacy policies"; they don't develop "*DRM* privacy policies." Those most attuned to their privacy obligations adjust their policies to reflect and anticipate the behaviour of their DRM technologies.

specific third parties to whom it had disclosed our personal information.[55] Almost half of the parties to whom we sent an inquiry failed to acknowledge or respond to our inquiry.

We found a range of behaviours associated with DRM. We identified 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. And we appreciated consistent difficulty in addressing the privacy implications of DRM technology. For example, only one organization identified IP addresses as the personal information of users.

Table 1 provides a breakdown of our assessments, showing, of organizations we assessed, the number who we identified as in compliance with *PIPEDA*, the number not in compliance, and the number we were unable to assess.[56]

[55] Only one organization, Microsoft, explained their relationship in detail with third parties once we specifically identified these third parties to them. We note that PIPEDA (principle 4.9.3) only requires third party identification where the organization is able to do so.
[56] By "unable to assess," we mean that we lacked sufficient information to come to a conclusion either way that is supported by the evidence. In most cases, this occurred because the information or evidence we sought was held by a third party–such as a DRM publisher– that we did not directly assess.

| PRINCIPLE | COMPLY | UNABLE TO ASSESS | FAIL |
|---|---|---|---|
| **Sub-section. 5(3)**: Does the organization collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances? | 4 | 0 | 8 |
| **Principle 4.2**: Does the organization identify the purpose for which it collects personal information? | 3 | 0 | 9 |
| **Principle 4.2**: If so, does it do so on or before collection? | 2 | 0 | 10 |
| **Principle 4.3.2**: Has the organization made a "reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used? | 1 | 0 | 11 |
| **Principle 4.3.6**: Does the organization require "express" consent to its collection, use or disclosure of personal information? | 2 | 0 | 10 |
| **Principle 4.3.3**: Does the organization, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes? | 1 | 0 | 11 |
| **Principle 4.4**: Is the collection of personal information limited (in both type and amount) to that which is necessary for the purposes identified by the organization? | 1 | 2 | 9 |
| **Principle 4.4**<br><br>Does the organization collect personal information by fair and lawful means (i.e., without deception | 5 | 4 | 3 |

| PRINCIPLE | COMPLY | UNABLE TO ASSESS | FAIL |
|---|---|---|---|
| or misrepresentation)? | | | |
| **Principle 4.4.1**: Does the organization specify the type of information it collects? | 1 | 0 | 11 |
| **Principle 4.5**: Does the organization use or disclose personal information for purposes other than those for which it was collected? | 0 | 10 | 2 |
| **Principle 4.8**: Does the organization have a "readily available" privacy policy? | 6 | 4 | 2 |
| **Principle 4.8.1**: Is the organization's privacy policy "generally understandable"? | 5 | 0 | 7 |
| **Principle 4.8.1**: Does the organization permit individuals to acquire information about the organization's privacy policies and practices without "unreasonable effort"? | 2 | 1 | 9 |
| **Principle 4.1.4(b)**: Has the organization established procedures to receive and respond to complaints and inquiries? | 5 | 4 | 3 |
| **Principle 4.9**: Has the organization responded to the individual's request with information of the existence, use, and disclosure of his or her personal information and, given the individual access to that information? | 2 | 2 | 8 |
| **Principle 4.9.1**: Has the organization provided a specific account of third parties to which it has (or may have) disclosed personal information about an individual? | 2 | 2 | 8 |

Table 1 – PIPEDA Assessment Results Summary

These results should be read in context. Statistics of this nature reflect the "all or nothing" nature of our assessment. To merit a finding of "compliant," an organization must be perfect; to earn a "non-compliant" finding, an organization need only err in one aspect.[57] Similarly, the assessments reflect the interlocking nature of the principles in *PIPEDA*. A single violation of the Act may percolate throughout the balance of the assessment. For example, a privacy policy's mis-description of a purpose for collecting information will have implications for consent, limiting collection, limiting use, retention and disclosure, and elsewhere.

## *3.2 PIPEDA Assessment Findings*

### 3.2.1 Sub-section 5(3) (Appropriate Purposes)

Sub-section 5(3) of the Act sets out an overarching limitation on the collection, use and disclosure of personal information; organizations may collect, use and disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. This test is highly contextual and depends on the circumstances.

Arguably, misidentified or vaguely described purposes and collection for undisclosed purposes violate sub-section 5(3) since such purposes are inherently inappropriate. However, for the purposes of our assessment, we considered only the underlying purpose itself without regard to short-comings in the manner of its description.

In order to assess whether an organization satisfied sub-section 5(3), we applied the plain meaning of the wording of the sub-section as supplemented by decisions of the Commissioner and the Federal Court. In *Eastmond v. Canadian Pacific Railway*,[58] the Federal Court laid out a test for assessing sub-section 5(3):

[57] For example, one vaguely described purpose would earn a finding of non-compliance despite excellent detail and disclosure in respect of all other purposes.
[58] *Eastmond v Canadian Pacific Railway*, 2004 FC 852 <http://www.canlii.org/en/ca/fct/doc/2004/2004fc852/2004fc852.html>, para. 127.

(a) Is the measure necessary to meet a specific need?

(b) Is the measure likely to be effective in meeting that need?

(c) Is the loss of privacy proportional to the benefit gained?

(d) Is there a less privacy invasive way of achieving the same end?

Although the Court acknowledged that this test might not be appropriate in every case, it provides useful guidance in assessing compliance with sub-section 5(3).

We encountered purposes that in the circumstances were quite privacy-invasive, unexpected and for which there were other less invasive solutions available. Napster, for example, states that it monitors messages (including email messages) sent to and from an individual's account with Napster in order to "check for obscenity, defamation or other types of abusive language, as well as for content that may infringe our rights or the rights of others." Although Napster includes this clause under the section "Information You Provide to Us," it is clearly not information that the individual provides to Napster. Applying the *Eastmond* test to Napster's practices, we concluded that this purpose did not pass the test, particularly since there were less invasive ways to achieve the same end. For example, Napster could merely respond to complaints as they arise, rather than engaging in indiscriminate monitoring of users' communications.

The Commissioner has considered at least one case under ss. 5(3) which raises issues similar to those implicated by DRM. In PIPEDA Case Summary #276, "The privacy implications of pay per view and piracy prevention measures," the Commissioner held that "[t]he company's purposes, namely, to bill for pay per view services and to prevent piracy were ones that a reasonable person would find appropriate in the circumstances."[59] Significantly for the purposes of our assessment, the Commissioner noted that: "There was no evidence that the company was

[59] Privacy Commissioner of Canada, "PIPEDA Case Summary #276: The privacy implications of pay per view and piracy prevention measures," (2 September 2004) <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_01_e.asp>.

collecting information from the telephone connection on subscribers' viewing habits" (emphasis added).

We found that a number of organizations collected, used and disclosed personal information for purposes of preventing "piracy" or enforcing legal rights. However, we also found many that went beyond that purpose to collect information on the user's viewing and related habits. For example, InterActual expressly states that it collects information about individuals' product usage information and "viewing behaviour information," among many other types of information, including IP addresses. In the case of IP addresses, InterActual states the following: "InterActual may use information derived from your IP address to deliver to you appropriate products, services and software and to prevent fraud." However, InterActual takes the position that none of the information it collects is personally identifiable, seemingly limiting its definition to: "name, address, telephone, email." Applying the definition of "personal information" in the Act to many of the policies and practices of InterActual, the organization is likely non-compliant with most if not all of the obligations under the Act.

The case of InterActual also raises the broader question of the appropriateness of DRM initiatives in general. We encountered InterActual's software in attempting to play a DVD: Disney's *Pirates of the Carribean*. DVDs can normally be played without the need to install software and to agree to broad-based collection, use and disclosure of information. Many of the purposes for InterActual's collection of this information appear to be marketing-related. A more general question (not examined in our assessment) might relate to the issue of whether such purposes are generally appropriate in the context of the enjoyment of creative works.

A similar question arises in the context of Valve, which states in its Privacy Policy that it tracks habits, usage patterns, and demographics. Valve also states that it tracks game selections and usage data. It would appear that there are less-invasive

measures that could be taken to prevent unauthorized copying and ensure product updates.

eReader's purposes are also of note because the organization openly profiles its customers:

> c. Profile: We store information that we collect through your stated preferences, cookies, log files, clear gifs, and/or third party sources to create a "profile" of your preferences. We tie your personally identifiable information, and your activity history, to information in the profile, in order to provide tailored promotions and marketing offers and to improve the content of the site for you. ...

Given that a variety of potentially detailed and sensitive personal information can be used to profile users in this manner (e.g. "profile" plus "your personally identifiable information" plus "activity history"), a reasonable person would likely only find the stated purposes to be reasonable if they were stated with some degree of specificity. In the circumstances, the following purposes seem inappropriate: "to create a profile," "to provide tailored promotions and marketing offers," and "to improve the content of the site for you."

eReader also requires its customers to use their credit card number as a password in order to unlock an e-book. Far less privacy-invasive measures could achieve the same end. Accordingly, we concluded that a reasonable person would likely object and find this purpose to be inappropriate in the circumstances.

### 3.2.2 Principle 4.2 (Identifying Purposes)

Principle 4.2 states: "The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."

In assessing compliance, we asked the following questions: (1) Does the organization identify and communicate the purpose for which it collects personal information? (2) If so, does it do so on or before collection? In our view, to merit the conclusion that the organization complies with Principle 4.2 the organization must:

1. communicate to the individual the purpose for which information is collected (so that the individual can reasonably understand why information is being collected from them),[60]
2. do so prior to or at the time of its collection, and
3. do so *accurately*.

The question of identifying purposes is obviously very closely tied to a number of other principles in the Act, and to sub-section 5(3). We note that, on one interpretation, Principle 4.2 is "inward facing," requiring an organization to identify to itself the purposes for which it collects personal information, and so serves as a check on indiscriminate collection. However, in PIPEDA Case Summary #361, the Assistant Commissioner interpreted Principle 4.2 to require the organization to identify those purposes in a manner sufficient to "explain why" a customer's personal information is being collected, and to do so in a manner that permits *the customer* to understand those reasons. This interpretation of Principle 4.2 reads into PIPEDA a requirement to provide reasonable notice of such collection to the consumer. Such a requirement could also be inferred from Principle 4.3's requirement to obtain the "knowledge and consent of the individual" to "the collection, use, or disclosure of personal information." We have adopted this interpretation to assess "notice" under both Principle 4.2 and 4.3.

[60] Privacy Commissioner of Canada, "PIPEDA Case Summary #361: Retailer requires photo identification to exchange an item," (23 February 2007) <http://www.privcom.gc.ca/cf-dc/2006/361_20061114_e.asp>. "A customer would therefore not likely be able to reasonably understand why any of this information must be collected, how long it will be retained (if recorded), or how the information will be used or disclosed."

Our Principle 4.2 analysis identified three groups of practices that violate the requirements of Principle 4.2:

1. missing, vague or inaccurately identified purposes,
2. inadequate steps to "identify" purposes in a manner that draws consumers' attention, and
3. practices with "timing" issues that fail to identify purposes prior to the collection of personal information.

We came across numerous purposes that were vaguely expressed or not expressed at all. Such expressions do not comply with Principle 4.2. Examples of the vague wording we encountered includes the following: "internal purposes," "administrative purposes," "service-related purposes," "to deliver a fun, personalized entertainment experience," "to better understand how our products and services are used so we can continually improve them," "marketing and commercial purposes," "for commercial exploitation," "to better understand the quality and use of its products and services and to provide you with more information and services based on your preferences," and "to track users and usage information." Some organizations had particular difficulty with precise and transparent descriptions. Napster, for example, discloses a number of purposes that are so vague as to not meet the requirements of *PIPEDA*. Napster's amorphous disclosures include "for our internal purposes," "to help us to serve you better," "for administrative purposes," "improve your service experience," "for other purposes," "for a variety of service-related purposes," "to personalize our service for your enjoyment," "to monitor and improve the performance of our technology," and "for our internal security audit log, aggregate trend analysis, and system administration."

InterActual, a provider of a software-based DVD player, explains its use and purpose for collecting zip code, age, gender, "product usage information," and "product usage behaviour":

> The anonymous demographic information, product usage information, and software and title upgrade information will be used primarily for marketing and commercial purposes, including market and product research and analysis, by InterActual and third parties.... [Emphasis added.]

InterActual provides some examples of "marketing and commercial purposes," but (through the use of the term "including") it does not limit itself to these examples. Apple provides another example of vague purposes. Apple states that it collects "technical and related information," including IP addresses, "to facilitate the provision of software updates, product support and other services to you (if any) related to the Apple Software and to verify compliance with the terms of this License." What Apple means by "related information" is unclear – as is what it means by "other services." Similarly, Azureus, the bittorrent client provider, states that it employs "tracking technology" without providing details.

With respect to "missing" identifications, Intuit failed to identify the purposes for which it collects personal information on co-branded websites (apart from assuring that it "is in accordance with our privacy practices"). Individuals would not be able to understand why Intuit was collecting information from them in these situations. Other organizations failed to mention relevant practices entirely. We observed communications in our technical assessment that were not obviously covered by any of the statements of purpose in the privacy policy documentation. This leads us to believe that some organizations may have failed to state all of the purposes for which they collect personal information. For example, the Ottawa Public Library's use of the OverDrive media console for implementation of digital audio book loans results in the disclosure of information to DoubleClick, a provider of ad serving technology. Neither the Ottawa Public Library nor OverDrive identifies this disclosure in their privacy policies (although subsequent investigation by OverDrive and the Ottawa Public Library suggests that the communication originates with the library, and not

with OverDrive). Similarly, Azureus offers no account for communications between its bittorrent client, Zudeo, and DoubleClick.

We encountered a number of situations where privacy policies contained inaccuracies that went to the issue of identifying purposes. Symantec, for example, states that its privacy policy applies to the use of its website, but further terms address activity other than website browsing.

Correct interpretation of the meaning of "personal information" under PIPEDA proved to be one of the largest problems with the organizations we assessed. None of the organizations we assessed acknowledged the privacy implications of IP addresses. Only one organization acknowledged in response to our inquiry that an IP address is personal information for the purposes of PIPEDA. Yet, over and over, we encountered disclosures that the organization collected IP addresses but characterized them as (for example) "non-personal information" (Intuit). Telus likely collects IP addresses, but refrains from identifying their collection directly and instead lumps them into the category of "anonymous data." Apple characterizes IP addresses as "certain information" that is "automatically" gathered and stored. Apple mistakenly says that IP addresses "[do] not identify individual users." Intuit dismissed our inquiries regarding the identities of third party recipients of communications observed in our technical investigation as unrelated to "personal information (as defined in the applicable legislation)" (implicitly classifying IP addresses as impersonal information).

Characterizations of technical information, including IP addresses and their potential to identify people, were often inaccurate. For example, Apple's documents suffer from a fundamental ambiguity in how it treats technical matters such as "pixel tags" and IP addresses. With respect to "pixel tags"[61] – also known as "web bugs" or "clear

[61] Wikipedia describes a "pixel tags" as another name for a "web bug," an object that is "embedded in a web page or e-mail and is usually invisible to the user but allows checking that a user has viewed the page or e-mail" <http://en.wikipedia.org/wiki/Web_bug>.

GIFs," a tracking technology – Apple explains what it uses them for, but fails to identify the information it is tracking. Since pixel bugs can log IP addresses, this is pertinent information. Pixel tags act like "cookies" to track user surf habits except that unlike cookies, a user cannot "turn off" pixel tags as they do not respond to browser privacy settings. With respect to IP addresses, Apple mistakenly says that IP addresses "[do] not identify individual users."[62] Apple states generally that it uses "certain information" to "track users' movements around the site," but fails to disclose the purposes of this tracking.

In terms of the act of "identifying" purposes, we considered the efforts made by an organization to bring a privacy policy to the attention of individuals. Principle 4.2.3 states that "the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected." Principle 4.3.2 (assessed below) requires that a "reasonable effort" be made by an organization to ensure that individuals are advised of the purposes. As noted above, these Principles taken together require effective notice by organizations to individuals of the purposes for which their information is being collected.

In terms of identifying purposes for collection before collection takes place, we refer to the discussion under Principle 4.3 but take this opportunity to note that in at least two situations, we observed organizations failing to present all of the relevant privacy documents to individuals where a specific technology used by the organization had privacy implications and the organization had developed a separate privacy policy to address that technology. For example, Symantec's LiveUpdate technology is incorporated into the product we investigated, Norton SystemWorks. Symantec offers a privacy policy that covers Norton SystemWorks, and a separate policy addressing LiveUpdate. LiveUpdate runs automatically on starting up Norton SystemWorks, without Symantec ever notifying the individual of LiveUpdate's separate privacy policy. Our investigation of the Ottawa Public Library, which uses

[62] See our discussion of how IP addresses constitute "personal information" under PIPEDA in Part 1.2.1, above.

OverDrive digital audiobook technology, raised similar questions about whether purposes had been identified to individuals prior to the collection of information.

### 3.2.3 Principle 4.3 (Consent)

Principle 4.3 requires that: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate." Consent is the cornerstone of *PIPEDA*. We assessed organization's compliance with three aspects of consent in *PIPEDA*:

(1) Principle 4.3.2 – Has the organization made a "reasonable effort" to advise the individual of its purpose for which the information will be used?
(2) Principle 4.3.6 – Does the organization require "express" consent to its collection, use or disclosure of personal information?
(3) Principle 4.3.3 – Does the organization, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes?

1. *Has the organization made a "reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used? [Testing 4.3.2]*

Principle 4.3.2 provides that: "Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."

Principle 4.3.2 imposes both substantive and procedural obligations on organizations. Substantively, the Principle requires organizations to state its practices "in such a manner" that an individual can reasonably understand how the organization will use or disclose personal information. Vague or open-ended descriptions, misdescriptions, and omitted descriptions of the information collected, or of the purposes of the

collection, use, or disclosure will fail to comply with Principle 4.3.2. Our discussion of those faults under Principle 4.2, Identifying Purposes, has obvious application to this aspect of Principle 4.3.2, and we refer the reader to our discussion under that Principle.

Procedurally, disclosure of an adequate privacy policy satisfies organizations' obligation to make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. We note that this obligation overlaps with organizations' wider obligation under Principle 4.8 to "make readily available to individuals specific information about its policies and practices relating to the management of personal information." The Privacy Commissioner has ruled that making information "readily available" to consumers includes making privacy policies available to the public in a variety of ways.[63] Note that the Commissioner requires multiple paths to disclosure; this is particularly important for those who do not have internet access. However, given that this Report focuses on digital technologies, we looked for an easily accessible digital or online version of the privacy policy in proximity to the product or service being assessed. The challenge then was to identify when the common practice of providing consumers with access to privacy policies through a link on a webpage met the "readily available" standard. We discuss the "readily available" requirement in more detail below, in our treatment of Principle 4.8.

Organizations may employ a range of techniques for making a privacy policy available to consumers:

- Organizations could present a policy to the consumer for express consent – an opt-in strategy. None of the organizations we assessed actively presented a privacy policy to the consumer.

[63] Privacy Commissioner of Canada, "PIPEDA Case Summary #304: Movie theatre chain strengthens personal information handling practices" (7 June, 2005) <http://www.privcom.gc.ca/cf-dc/2005/304_20050607_e.asp>.

- Organizations could reference the privacy policy in a license agreement that the consumer must then provide express consent to. A number of organizations took this approach, including Telus (in respect to its Mobility Terms and Conditions, but *not* in respect its Music Subscription Service Terms and Conditions – the service actually being assessed).
- Organizations made the policy available on their homepage and other pages on the website. Every organization we assessed offered a privacy policy in this fashion, although some (Sony BMG) applied only to the website, and not to the DRM being assessed.
- Other organizations explicitly (Intuit) or implicitly (Ottawa Public Library) referenced the privacy policy of a third party service provider.

In conducting our assessments, we distinguished between those organizations that provided both the content and the DRM technology (*e.g.*, Apple, Intuit, Valve) and those offering a third party's DRM service (Ottawa Public Library, Telus). We observed that the latter group had difficulty accommodating the behaviour of suppliers' DRM within their existing privacy policy. Their policies did not appear to have been drafted with the DRM suppliers' technology in mind.

For organizations providing DRM, we accepted the presentation of an applicable privacy policy on an associated webpage as satisfying *PIPEDA*'s requirement to make a "reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used.

For organizations supplying third party DRM, we assessed whether the content provider drew to the consumer's attention the DRM publisher's different privacy policy. We did not accept as sufficient a disclaimer that third parties may have different applicable policies (Intuit). That is effectively a disclaimer of responsibility for the organization's treatment of the consumer's personal information. A much clearer disclaimer would be required to bring such an approach into compliance with the Act.

For consent to be effective, we needed to find the organization's privacy policies in a document identified as a "privacy policy." Some organizations buried privacy disclosures in other documents. For example, Telus disclosed its technical data practices not in its Privacy Commitment, or its Privacy Code, but in an FAQ. Similarly, Intuit buries core privacy practice disclosures in its software license agreements.

Finally, we note that the Privacy Commissioner has found that providing examples up front of the kinds of personal information collected, and outlining a rationale for its collection, are keys to compliance with this Principle.[64] We found that the organizations generally did a good job of detailing examples of the kinds of information collected, but not always.

2. *Does the organization require "express" consent to its collection, use or disclosure of personal information? [Testing 4.3.6]*

Principle 4.3.6 provides as follows:

> The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

[64] Privacy Commissioner of Canada, "PIPEDA Case Summary #296: Language of consent and monitoring activity challenged" (20 April, 2005) <http://www.privcom.gc.ca/cf-dc/2005/296_050314_02_e.asp>.

A consumer's consent to the collection, use or disclosure of his or her personal information may take a variety of forms, among them express (or opt-in), implied, deemed, and opt-out. Express consent is positive consent, the strongest form of consent. Principle 4.3.4 allows for the form of consent sought by an organization to vary with the circumstances, and the Act itself fails to mandate particular forms of consent under given situations. The Office of the Privacy Commissioner has published guidelines for determining the appropriate form of consent – express implied, deemed, or opt-out – to the circumstances.[65] With respect to express consent, the Guidelines state that:

> An organization is encouraged to use this form of consent wherever appropriate, taking into consideration the reasonable expectations of the individual. This form of consent is least likely to give rise to misunderstandings and complaints.
>
> Principle 4.3.6 states that an organization should generally seek express consent when the information is likely to be considered sensitive.[66]

We consider that express consent to the collection, use or disclosure of personal information is required in respect of particularly sensitive information or unexpected uses or disclosures. In settling on this standard we have been guided by the language of the Act, the Guidelines, the Commissioner's decisions, applicable court cases, and the reasonable expectations of consumers.

We consider financial information such as tax information and credit card data to be "sensitive" information. We found that a number of organizations collect, use or

[65] Office of the Privacy Commissioner of Canada, "Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act," <http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp> [Privacy Commissioner of Canada, "Determining the appropriate form of consent"].
[66] Privacy Commissioner of Canada, "Determining the appropriate form of consent," *supra* note 65.

disclose sensitive information in contexts that we believe should mandate express consent. Intuit's Privacy Policy includes a broad definition of "personal information" that implicates tax data, including financial information and identification data of extreme sensitivity. Intuit's Privacy Policy goes on to state that:

> Intuit is a multi-national company and as such, personal information may be shared within Intuit and stored in countries outside of Canada. Currently, personal information may be stored or processed in the United States and therefore may be subject to US legislation.

This statement, combined with the open definition of "personal information", appears to reserve to Intuit the right to send sensitive tax and identification data across the border to Intuit facilities in the United States, thus exposing that data to American laws. Were this to be an accurate state of affairs, we would have expected Intuit to seek active consent to the practices. Intuit subsequently clarified that its customers' tax data remain on a secure server in Canada, and that its Privacy Policy does not reflect its actual practices in this respect. We note that, in any event, the transmission of tax data arises in the context of Intuit's online tax filing service, and not through the use of QuickTax without filing taxes online.

Similarly, eReader uses credit card numbers as passwords for the purpose of unlocking purchased e-books. eReader offers no way to opt-out and use an anonymous and more secure pass code.

With respect to "unexpected" uses of information, we regard tracking as unexpected where occuring in a context in which consumers are accustomed to privacy. When purchasing and enjoying music, videos, and reading material, consumers do not reasonably expect that they will be tracked and their information collected. In *SOCAN v. CAIP*, Supreme Court Justice Lebel described this kind of data as "core biographical information" in which individuals have a reasonable expectation of

privacy.[67] Similarly, we have characterized as unexpected particular communications: secondary marketing disclosures and unexpected cross-border communications of sensitive information.

We found that a number of organizations track consumer usage of content. Apple states that its iTunes service tracks customer usage of its services for purposes such as "to give you convenient access to our products and services and focus on categories of greatest interest to you." iTunes relies on passive acceptance of its privacy policy, and gives the user no means of opting out of being tracked.

eReader is perhaps the most aggressive of the organizations we assessed. eReader's policy states that: "We tie your personally identifiable information, and your activity history, to information in the profile, in order to provide tailored promotions and marketing offers and to improve the content of the site for you." eReader does not obtain express consent for this activity.

Without obtaining express consent, Azureus, a peer-to-peer client, similarly explains that it may access:

> certain information from your system by using different types of tracking technology. This "automatically collected" information may include internet Protocol address ("IP Address"), a unique device or user ID, version of software installed, system type, the content and pages that you access on the Azureus Platform, and the dates and times that you visit the Azureus Platform. [emphasis added]

InterVideo, a digital DVD player, claims to collect a great deal of content usage information. In addition to IP addresses, InterVideo collects user IDs, InterActual Player data, "Disc-specific information, such as the disc currently in the drive," and

[67] *Society of Composers, Authors and Music Publishers of Canada v Canadian Association of Internet Providers*, *supra* note 35, para 155.

"Demographic data (age, gender, zip code) entered by you in the Configuration Dialog." InterVideo does not obtain express consent to this activity.

3. *Does the organization, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes? [Testing 4.3.3]*

Principle 4.3.3 provides as follows: "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes."

In many ways, this inquiry gets to the heart of the privacy-based criticisms of DRM: content distribution organizations that in the past lacked direct access to consumers now, through the use of digital technologies, observe the behaviour of consumers even though the consumers' dealings with associated content has not changed. We observed a number of organizations conditioning access to content on this kind of observation. For example, Valve requires one to use its Steam service to play *Half-Life 2*, even though merely playing the game does not require online access (although network play obviously would). Similarly, Disney's *Pirates of the Caribbean* DVD installs InterActual's player, the user agreements to which indicate that the technology tracks user behaviour. Again, nothing about the act of enjoying a movie requires one to consent to surveillance. eReader's document states that it profiles its customers and uses that data to engage in marketing activities. Other examples were more modest, but equally surprising. For example, our use of the Ottawa Public Library's digital audiobook download service resulted in communications with DoubleClick, a web advertisement company. Subsequent communications with the Library and audiobook service provider suggest that the communications originate with the Library's web services, and not with the audiobook service. Similarly, Sony BMG's DRM produced unexpected communications to a single third party server –

that of SunnComm, its DRM provider. Each of these companies *conditions* supply of its services on consumer consent to this over-reaching behaviour, and each fails to offer consumers an opt-out.

### 3.2.4 Principle 4.4 (Limiting Collection)

Principle 4.4 requires as follows: "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means." We assessed organizations' compliance with three aspects of the Act's requirement that collection be limited:

(1) Principle 4.4 – Is the collection of personal information limited (in both type and amount) to that which is necessary for the purposes identified by the organization?
(2) Principle 4.4 – Does the organization collect personal information by fair and lawful means?
(3) Principle 4.4.1 – Does the organization specify the type of information it collects?

1. *Is the collection of personal information limited (in both type and amount) to that which is necessary for the purposes identified by the organization? [Testing 4.4]*

Principle 4.4 prohibits the collection of information on the basis of vague, non-exhaustive descriptions of information collected or the purpose of the collection.

We have already identified a number of cases of indeterminate language in respect of Principle 4.2. Indeed, the two Principles are closely connected. We won't repeat that analysis here.

One issue we frequently encountered involves the use of general definitions of personal information and failing to particularize the information used in connection with a given purpose. Apple, for example, relies upon a general (and non-exhaustive) definition of "personal information relevant to the situation." Similarly,

Intuit collects "usage data," which it defines non-exhaustively as including personal information "such as … your IP address."

2. *Does the organization collect personal information by fair and lawful means (i.e., without deception or misrepresentation)? [Testing 4.4]*

The requirement to collect personal information by fair and lawful means amounts to a prohibition on collecting personal information by deception or misrepresentation.

A number of organizations mischaracterized IP addresses as non-personal information (see, *e.g.*, Telus, OPL). Sony BMG's License Agreement states that "the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise" [emphasis added]. Yet, Sony BMG's copy-protected CDs communicate with third parties over the internet, disclosing personal information in the form of the consumer's IP address.

InterActual takes the view that none of the information it collects, uses and discloses is personal information:

> InterActual Player collects no personally identifiable information (name, address, telephone, email) from you. InterActual Player does not require nor accept any personally identifiable information when using one of its many features.

InterActual's description of what amounts to "personal information" is not the same as the definition in the Act. By qualifying "personally identifiable" information in this way, InterActual appears to suggest that "anonymous information" is anything that is not "name, address, telephone, email." Applying the definition of "personal information" in the Act to many of the policies and practices of InterActual, it appears that the organization is almost completely non-compliant with the

obligations under the Act. In its Privacy Policy, InterActual admits that it collects IP addresses:

> InterActual servers automatically collect IP addresses. From time to time, InterActual may use information derived from your IP address to deliver to you appropriate products, services and software and to prevent fraud.

InterActual also claims that it uses cookies to transmit "anonymous information," such as:

> • User ID (your numeric representation in the InterActual database)
> • InterActual Player-specific information, such as language, versions, DVD navigator information, current skin and other information pertaining to configuration settings of InterActual Player
> • Disc-specific information, such as the disc currently in the drive
> • Demographic data (age, gender, zip code) entered by you in the Configuration Dialog

Again, this information is not anonymous under the Act, particularly since it can be tied to an IP address when the cookies are sending the information, and be thereby used to create a very detailed profile of the individuals' viewing habits.

During installation, the "Registration" phase of the program requests the user to provide "anonymous demographic data" when installing. This includes ZIP code, Age (range) and gender. It also includes a statement that InterActual "collects and uploads anonymous product usage and viewing behaviour information" and that this information will be used and disclosed to third parties for "marketing purposes." Assuming that the allegedly "anonymous" information can be tied to an IP address or to other information (which seems to be suggested by the uses that InterActual may

make of IP addresses as described above), it fits the definition of "personal information" in the Act.

InterActual's Privacy Policy describes "Product usage information" as the following:

> …information about the discs played on your system on which InterActual Player resides. The product usage information is gathered only through the use of InterActual Player and is stored locally on your hard drive. The information is transferred from your hard drive to InterActual's servers on an anonymous basis once an online connection is detected. The information does not contain any personally identifying information, only anonymous information relating to product usage behavior. You can turn off the passing of product usage information to InterActual servers at any time by using the InterActual Player Configuration Dialog. [Emphasis added.]

In reality, InterActual reserves to itself the right to use this information for "commercial" purposes, and to pass the information on to "unrelated third parties for commercial exploitation." InterActual is to be credited for disclosing that it engages in this kind of behaviour, but in mischaracterizing the capacity of this data to be linked back to the consumer, it may mislead consumers as to the privacy implications of their use of InterActual's product.

Finally, we observe again that a number of our technical reviews disclosed internet communications that were not explained in applicable privacy policies. We were not able to account for these communications, and so are not in a position to say one way or the other that those communications comply with Principle 4.4. Only four out of twelve organizations answered our requests for information about their privacy practices. Only two of these answered substantively.

*3. Does the organization specify the type of information it collects? [Testing 4.4.1]*

Principle 4.4.1 of PIPEDA requires as follows: "[…] Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8)." Principal 4.4.1 prohibits vague, open-ended descriptions of information collected.

The question of indiscriminate collection arose in a number of assessments. For example, Napster states that it collects "personally identifying usage data" without providing details of the content of that data.

Our technical review introduced a significant assessment challenge. We frequently observed unexplained and unanticipated internet communications originating from our computer and terminating with an unfamiliar (or at times familiar, but unexpected) third party. Half-Life 2, for example, turned up literally dozens of unanticipated third party communications. Are these communications simply outsourced web functionality? Or do they involve something more? We were unable to assess the information communicated.

Other categories of information that this Principle addresses include information collected surreptitiously or without disclosure. The nature of the investigation we undertook generally did not permit us to observe this kind of behaviour.

### 3.2.5 Principle 4.5 (Limiting Use, Disclosure and Retention)

Closely connected to the principle of limiting collection is that of limiting the use and disclosure of personal information to those purposes for which it was collected. Principle 4.5 requires as follows:

> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

We assessed organizations' compliance with a single aspect of the Act's requirement that use, disclosure and retention be limited, namely, whether the organization uses or discloses personal information for purposes other than those for which it was expressly collected. Again, it was difficult for us to assess organizations' compliance with this Principle, since we could only assess behaviour that we could see. Generally, this involved assessing whether organizations adequately disclosed observed third party communications. We did not assess organizations' compliance with its obligation to limit retention of personal information.

Our technical review occasionally identified specific communications that conflict with positive terms of an applicable privacy policy. For example, the Ottawa Public Library and OverDrive, its DRM service provider, both promised not to disclose consumers' personal information for marketing purposes. Yet, our review identified internet communications with DoubleClick, a provider of ad serving technology. Subsequent communications from both organizations suggest that the communications originated with the Library's web services, and not with OverDrive.

For many of the DRM systems we examined, we noted a large number of internet communications that were not easily accounted for by the organization's policies. Without more information about the content of those communications, we cannot say with certainty that those organizations comply with Principle 4.5. We provide more commentary with respect to those communications in our discussion of Principle 4.9, Individual Access, below.

### 3.2.6 Principle 4.8 (Openness)

Principle 4.8 requires that "An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information." This information must be generally understandable and

individuals must be able to acquire information about the organization's privacy practices without unreasonable effort.[68]

We assessed organizations' compliance with this Principle by considering whether policies were "readily available," "generally understandable," and available without "unreasonable effort."

We concluded that several privacy policies were not "readily available." For example, although we found a privacy policy applicable to Sony BMG's website, we did not find one that covered its software or copy-protected CDs. Telus has a well-written collection of privacy documents; however, discussion of its privacy practices regarding technical data and IP addresses is located in a FAQ, not in the core privacy documents.[69] Apple places key privacy terms in its Software License Agreement which may be unexpected for those individuals looking for the privacy policies. Intuit relies upon the consumer to visit its website and find the policy; in some cases this would be sufficient. However, Intuit embeds privacy terms in its Software License Agreement and its Software Modules License Agreement; these are documents presented to the consumer in pop-up windows during installation but which are otherwise not readily available to consumers.[70]

We have addressed the issue of policies being "generally understandable" in other areas of this Report.[71] Many policies contain vague wording. We also wish to make the point that when policies are contained in multiple documents (e.g. Apple, Symantec, Telus, Valve), they may not be "readily available" and they may not be generally understandable – it is difficult to understand privacy rules when one must

[68] Privacy Commissioner of Canada, "PIPEDA Case Summary #348: Disclosure of diagnosis was inappropriate, but insurance company considered to be open about its privacy policies and practices," (14 August 2006) <http://www.privcom.gc.ca/cf-dc/2006/348_20060814_e.asp>. Finding that openness may be met where a privacy policy is available on a website and includes the email and telephone number of the Privacy Officer).
[69] A similar issue arises with Azureus.
[70] Similar issues arise in relation to InterActual.
[71] See Section 3.2.3 (Consent).

stitch together several different documents, especially if they are not consistent with one another. Policies can also fail to be understandable when they suggest that they apply to only website interactions as opposed to the use of software and content (e.g. Symantec, Sony BMG).

Our assessment also considered the organizations' privacy documents with a view to identifying whether the organizations provided accounts of third party communications. Few organizations identified specific third parties. eReader's policies mention that it discloses information to DoubleClick. Similarly, Napster's policies provide a relatively fulsome account of its need to contact Microsoft:

> From time to time, the security on the Napster Client software may be upgraded by our supplier, which is currently Microsoft. Microsoft advises us that for security upgrades, your player will connect to an internet site operated by Microsoft and will be sent a security file, along with a unique identifier, which does not contain any personal information about you and is not used to personally identify you or track your activities. Microsoft uses this information to prevent security breaches that could affect you. For more information, please feel free to read Microsoft's privacy policy at http://www.microsoft.com/Windows/windowsmedia/software/v7/privacy.asp#_Security_Upgrade_(Individualization)

Both the Ottawa Public Library and its digital audio book provider, OverDrive, take pains to describe Microsoft's security upgrade process – the process by which Windows Media Player incorporates DRM. Unfortunately, the Library did not take similar pains to disclose DoubleClick's involvement with the Library in supplying web services. In fact, the nature of DoubleClick's involvement with the Library only became clear after news of our research became public. DoubleClick's services are, in fact, unrelated to the Library's audiobook service and unrelated to OverDrive's technology.

The more common approach, however, is to identify classes of third parties to whom disclosures *may* be made. For example, Azureus' privacy policy states that:

> We may disclose User information to affiliated companies or other businesses or persons to: provide web site hosting, maintenance, and security services; fulfill orders; conduct data analysis and create reports; offer certain functionality; and assist Azureus in improving the Azureus Platform and creating new services features.

Valve, interestingly, grants itself authority to report your use of "cheats" to "other online multiplayer hosts."

The problems we identified above in respect of vague, indeterminate or open-ended descriptions of information, purposes, and uses carried through to descriptions of purposes and third parties for disclosures. For example, Apple's privacy policy reads as follows:

> it may be advantageous for Apple to make certain personal information about you available to companies that Apple has a strategic relationship with or that perform work for Apple to provide products and services to you on our behalf. These companies may help us process information, extend credit, fulfill customer orders, deliver products to you, manage and enhance customer data, provide customer service, assess your interest in our products and services, or conduct customer research or satisfaction surveys.

This statement describes none of the potential information disclosed, the purpose of the disclosure, or the identity of the third party, with specificity.

With respect to the effort required to obtain policies, most of the companies we encountered provided an email address and other contact information through which individuals could acquire information about the organizations' privacy policies and practices. Some companies replied to our request for information and access. Intuit, for example, responded to our inquiry with a substantive account of its privacy practices. However, Intuit's reply failed to disclose what personal information is made available to related organizations within the Intuit family. Organizations that did not reply to our request for information and access cannot be said to meet the openness principle.

Symantec's Customer Profile Form was one area where we found a problem in the way that Symantec invited consumers to contact the organization regarding privacy. The Customer Profile Form asks for (and in some cases requires) individuals to disclose personal information that they might have never disclosed to Symantec before. For example, if the individual set up their installation without creating an account, then Symantec would only have been provided the Product Key. However, the Customer Profile Form then asks individuals to disclose the following information: Personal Information, First Name (required), Last Name (required), Address (required), City (required), State (required for US), Province (International Residents), Zip/Postal, Code (required), Country/Province (required), Phone Number, Email Address.

If a user is able to install and use the Symantec product by providing only a Product Key (to authorize the software), then it is not clear why customers seeking information about privacy practices or technical support for their product should have to provide more than their Product Key to do so. Requiring additional information from individuals before responding to their requests for information about privacy suggests that the Openness principle is not being complied with.

### 3.2.7 Principle 4.1 (Accountability)

Principle 4.1 states as follows: "An organization is responsible for personal information under its control and shall designate an individual or individuals who are

accountable for the organization's compliance with the following principles [i.e., each of the ten principles enumerated in the Act]." We assessed organizations' compliance with a single aspect of Principle 4.1: does the organization comply with Principle 4.1.4(b) by "establishing procedures to receive and respond to complaints and inquiries"?

Surprisingly, not every organization we looked at provided a privacy contact. For example, InterActual does not provide a privacy contact because it contends that "no personally identifying information is being gathered from you"; of course, were this true, it would beg the question of why they have a privacy policy at all. Sony BMG does not provide a privacy contact in connection with its DRM CD, but has a contact on its privacy policy on its website. A letter, addressed to "Privacy Officer" and sent to that address enclosing our privacy questions was returned to the author months later, stamped "Return to Sender" and "Contact Person Required". PIPEDA requires organizations to designate an individual or individuals who are accountable for the organization's compliance with the Act.

Most organizations provided a privacy contact but not all responded meaningfully or at all to our requests for information and access. The most common response we received was merely a "privacy run-around" – a request to consult the organization's privacy policy. We concluded that either a complete failure to respond or a "privacy run-around" response indicates a failure to establish *effective* procedures and thus a failure to be accountable.[72] Intuit, Microsoft, Napster and the Ottawa Public Library were the only organizations to respond in a way that addressed the substance of our inquiry. Microsoft and the Ottawa Public Library were the only organizations to respond to our inquiry about particular third parties, but only once we had identified these third parties.

[72] Privacy Commissioner of Canada, "PIPEDA Case Summary #346: E-mail message raises questions about purposes, credibility and accountability" (15 June 2006), <http://www.privcom.gc.ca/cf-dc/2006/346_20060615_e.asp>.

### 3.2.8 Principle 4.9 (Individual Access)

Principle 4.9 provides as follows:

> Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

We assessed organizations' compliance with two aspects of the Act's obligation to provide consumers with access to their information:

(1) Principle 4.9 – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information.

(2) Principle 4.9.1 (and 4.9.3) – Has the organization provided a specific account of third parties to which it has (or may have) disclosed personal information about an individual?

1. *Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. [Testing 4.9 in combination with ss. 8(3)]*

Principle 4.9 operates in conjunction with sub-section 8(3) of PIPEDA. Sub-section 8(3) provides as follows: "An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request."

Every organization we asked to provide us with access to our personal information failed to do so. The best of our responses identified the type of information collected, but failed to provide access. Others simply suggested we review their privacy policy. More failed to respond.

2. *Has the organization provided a specific account of third parties to which it has (or may have) disclosed personal information about an individual? [Testing 4.9.1 and 4.9.3 for the "may haves"]*

Principle 4.9.1 (in part) provides as follows: "[T]he organization shall provide … an account of the third parties to which [the individual's personal information] has been disclosed."

Principle 4.9.3 provides as follows:

> In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

Our inquiry to each organization was particular: we requested a list of the third parties to whom it has (or may have) actually disclosed our personal information. No organizations responded to the question with particulars. Microsoft and the Ottawa Public Library did provide us with a detailed response, but only once we had identified these third parties to them.

### 3.2.9 A Note on Observed Third Party Communications

Our technical review produced the greatest challenge to our ability to assess compliance with *PIPEDA*. Many of our technical reviews identified a large number of communications with third party IP addresses that are not easily explained by the applicable organization's privacy policy. Interestingly, these communications occurred at a variety of points, including (in the case of eReader, Half-Life 2, Apple and Napster) during use or enjoyment of content.

The third party communications fall into three categories: (1) communications to unresolved and unknown IP addresses, (2) communications to resolved IP addresses belonging to unknown organizations, and (3) communications to resolved IP addresses belonging to known organizations.

We do not have a great deal to say about the first and second categories of communications. We have put our questions about these communications to the organizations involved but in no case were we offered a useful response.

The third category of communications we found more interesting. Many of these communications were to organization such as Verisign, Akamai, Omniture, and others. Generally speaking, we know something about their businesses. Verisign, for example, provides digital signatures and performs a crucial role in authenticating parties for the purposes of e-commerce. Akamai and Omniture play important roles in facilitating effective communication of web-based services.

We know that some these parties collect personal information. For example, Akamai's privacy statement indicates that Akamai collects IP addresses, information about a user's operating system, web browser, the time of communication and the user's geolocation. We would expect to see an account of the disclosure of personal information – such as IP addresses – to such third parties in the privacy policies of organizations we assessed. However, we did not see a single reference to Akamai or Omniture in the documents we reviewed (although Microsoft did disclose its relationship with Akamai and WebTrends in correspondence with an Assessor).

It is possible that some of these activities related to outsourced functions. The Privacy Commissioner considers outsourcing a "transfer" for processing, not a "disclosure" requiring consent under the Act.[73] That raises the question of whether

[73] See, for example, address by Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada, to The Canadian Corporate Counsel Summit, "Protecting Personal Information in Canada and Abroad" (6 March, 2006),

the services of Akamai, Omniture, and similar organizations amount to outsourced processing. If so, the "transfer" of personal information to such services would not require consent. If instead such services amount to *more* than outsourced processing, disclosures of personal information to such organizations requires a degree of transparency to provide consent to the transfer. There is a case to be made that these services are simply outsourced data processing where they essentially replace or supplement functions formerly performed in-house. However, other services, such as the "web analytics" services offered by Akamai, are clearly more than third party processing.

The Commissioner has emphasized that transparency is one of the cornerstones of PIPEDA, even in the case of transfers of personal information in the outsourcing context that do not require the consent of the affected individual. In the CIBC cross-border data transfer decision, the Assistant Privacy Commissioner concluded as follows:

> What the Act does demand is that organizations be transparent about their personal information handling practices and protect customer personal information in the hands of foreign-based third party service providers to the extent possible by contractual means.[74]

We found little transparency in our assessment of these data communications. Only one organization provided us with a detailed response to our specific inquiry into these communications: Microsoft clarified that:

> Microsoft may use services from other companies, such as Akamai Technologies and WebTrends, that enable them to derive a general

---

<http://www.privcom.gc.ca/speech/2006/sp-d_060306_pk_e.asp>, citing Privacy Commissioner of Canada, "PIPEDA Case Summary #313: Bank's notification to customers triggers PATRIOT Act concerns" (19 October, 2005) <http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp> [PIPEDA Case Summary #313].

[74] PIPEDA Case Summary #313, *supra* note 73.

> geographic area based on your IP address in order to customize certain services to your geographic area. Microsoft may also hire other companies to provide limited services on our behalf, such as handling the processing and delivery of mailings, providing customer support, hosting websites, processing transactions, or performing statistical analysis of our services.

Other organizations were not so forthcoming. Faced with the same question, Intuit responded that:

> We are not normally in the practice of addressing questions requiring us to identify to or from where all communications transpiring an individual's computer may be coming or resolving. [*sic*]

Intuit's representative went on to state that he had consulted with Intuit's development team, which hypothesized that some of these communications resolved to the Assessor's ISP and others originated with other programs installed on the Assessor's computer.

We found these responses, globally, less than satisfactory. We know very little about these communications, and yet they raise important questions.

## PART 4 • CONCLUSIONS

Canadians are now exposed to DRM in a variety of forms and with respect to a wide range of digital information products. Perhaps as a result of their increasing presence in the market, DRM technologies have spawned widespread mainstream controversy in Canada and abroad, with privacy concerns as one of the main areas of debate. Our research found that these concerns are justified.

As a result of our technical investigations, we concluded as follows:

- Of the 16 organizations deploying DRM technologies we reviewed, only 12 were found to have engaged in internet communications.
- The range of communications initiated by the DRM varied from a single "phone home" in the case of a copy-protected CD to literally thousands of independent communications initiated by a BitTorrent client.
- Akamai, Omniture and DoubleClick are seemingly connected in some form to a number of the DRM-related products that we assessed.

Our examination of the privacy implications of DRM led us to a number of conclusions:

*Inappropriate purposes*

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

*Excessive collection, use and disclosure of personal data*

- Several organizations disclosed that they engage 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'?"

With respect to future work, many topics present themselves. The potential of privacy-enhancing DRM applications offers one such topic. Similarly, the coming years will likely produce legislation relevant to both DRM and privacy, including Canadian anti-spyware legislation and revisions to copyright law to introduce anti-circumvention laws. DRM and privacy are relevant to both areas of law, and it is our hope that this Report might make a contribution to consideration of such proposals.

This report confirms that DRM represents a challenge to privacy interests, but a challenge with two edges. DRM may, at times, pressure consumers' privacy interests. However, as our Report makes clear, DRM also challenges organizations' compliance with privacy laws.

As DRM technologies evolve, and as our collective appreciation for DRM's challenges to privacy matures, we hope that policy-makers, market participants and technologists will respond to these challenges with policies and tools that are more respectful of privacy. We already see this dynamic operating in the marketplace. However, our study's results suggest that there remains room for progress.

## The Canadian Internet Policy and Public Interest Clinic (CIPPIC)

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established in fall of 2003 at the University of Ottawa, Faculty of Law, Common Law Section. CIPPIC seeks to ensure balance in policy and law-making processes on issues that arise as a result of new technologies. Clinic counsel work with upper year law students on projects and cases involving the intersection of law, technology and the public interest.

www.cippic.ca

**University of Ottawa, Faculty of Law**
57 Louis Pasteur, Ottawa, ON K1N 6N5
**tel:** 613-562-5800 x2553 **fax:** 613-562-5417