How Restrictive Terms and Technologies Backfired on Sony BMG

Jeremy F. de Beer, University of Ottawa
INTRODUCTION

In late 2003, subsidiaries of international media and entertainment companies Sony Corporation and Bertelsmann AG joined forces to become the second largest player in the global recorded music business. This merger consolidated the catalogues and clout of two of the world’s “big five” music recording companies. The new industry heavyweight, Sony BMG Music Entertainment, is made up of major labels such as Arista, Epic, Columbia, RCA and others. It boasts an impressive portfolio of artists, ranging from Canadian sensation Avril Lavigne to new country rockers Van Zant, and including legends like Elvis and Streisand and megastars like Santana and Beyoncé.

According to the press release announcing the joint venture, the companies wanted “to create an environment where the global music audience can benefit and artistic expression can thrive”. Andrew Lack, then CEO of the new enterprise, said the merger would provide an opportunity “to bring greater value to music consumers around the world, and enable us to more effectively meet the needs of our artists”. Fast-forwarding to 2006, it has become apparent that Sony BMG’s music distribution strategies have neither benefited consumers nor met artists’ needs. To the contrary, Sony BMG’s restrictive contractual terms and digital rights management (DRM) technologies have alienated both consumers and artists.

At least 22 million Sony BMG music CDs included software that was designed to control consumers’ uses of music, but which in fact installed on their computers a program that interfered with normal system operations, caused serious security vulnerabilities, was practically impossible to uninstall and surreptitiously transmitted information about users’ computers and listening activities. Furthermore, consumers who had purchased one of these CDs could not use it on a computer without clicking to agree with misleading, not to mention ridiculous, terms and conditions.
When people were alerted to these facts, Sony BMG was attacked with legal actions in Canada, the United States and Europe. It is possible that there are further lawsuits or investigations still to come. Consumers also retaliated with their pocketbooks, leading to a dramatic drop in album sales for some Sony BMG artists. Artists have expressed disappointment with their labels and tried to distance themselves from Sony BMG’s tactics.

This article chronicles how and why Sony BMG’s tactics backfired so dramatically. It suggests that the root of the problem, pardon the pun, is fundamental mistrust of and disrespect for artists’ fans. Sony BMG’s classless actions demonstrate an unwillingness to satisfy consumers who want to obtain music in novel and convenient ways and on fair and flexible terms. The property, privacy and civil rights of honest music fans have been treated as collateral damage in the industry’s war on piracy.

Notably, my criticism in this article is not directed at DRM per se. Sony BMG’s deployment of such measures, however, is illustrative of the dangers of DRM systems. These events highlight what numerous scholars have repeatedly pointed out: Canada needs a balanced and comprehensive response to DRM, which not only protects technologies from consumers but also protects consumers from technologies.

The article is split into two parts. Part I chronicles the brief history of the Sony BMG saga. After describing how the story broke, it explains in non-technical terms exactly what Sony BMG’s DRM technologies do and why. It also analyzes the contractual terms and conditions that Sony BMG purported to dictate to consumers. Finally, Part II looks at some of the initial reactions to the events that occurred. Part II considers the legal and policy implications that flow from Sony BMG’s use of these terms and technologies. It describes a number of class action, individual and government legal measures that have been or may be initiated against Sony BMG as a result of its conduct. Most of the analysis concentrates on the viability of various causes of action under Canadian law. The article concludes by putting this specific scandal into perspective and looking at the broader repercussions for DRM, copyright and consumers in general.
PART I: A BIT OF BACKGROUND

It is a testament to the power of the Internet that this whole controversy was sparked by a weblog posting from computer security researcher Mark Russinovich. In October 2005, Russinovich was running a routine software test on one of his systems. He was shocked to discover that a “rootkit” had been installed on his computer. A rootkit, simply put, is a cloaking technology that hides files from diagnostic and security software. Unlike most people, Russinovich was able to understand the oddity of having a rootkit on his system, especially given his careful Internet surfing and software installation habits. Moreover, Russinovich realized that this rootkit in particular was quite poorly written, and that it was extremely difficult for him (and practically impossible for anyone else) to uninstall. After digging into the matter, he linked the presence of this rootkit to software contained on a CD he had recently played on his computer — an album by Van Zant called “Get Right with the Man” and produced by Sony Music Nashville, one of Sony BMG’s record labels. Understandably upset by what he had found, Russinovich blogged about the details of his discoveries.

News of the rootkit spread over the Internet like wildfire. Bloggers expressed surprise, anger and of course, technical and legal opinions about the implications of Sony BMG’s actions. Within days, the story had caught the attention of mainstream media. In part due to the publicity the matter was getting, additional disturbing information about Sony BMG’s DRM technologies began to surface.

THE TECHNOLOGIES

Ed Felten and J. Alex Halderman, researchers from Princeton University, revealed that problems exist with at least two different DRM systems used by Sony BMG. The rootkit that Russinovich had discovered was designed by a United Kingdom firm called First4Internet. It is referred to as XCP, which stands for “extended copyright protection” (aptly named since the content protection it provides extends well beyond that of traditional copyright law). Sony BMG also uses a system called MediaMax™, designed by SunComm.

MediaMax™ was, and continues to be, used by Sony BMG far more widely than XCP. XCP was included on about 2 million copies of 52 different albums in the United States. 120,000 units of 34 different albums containing XCP were distributed in Canada. On the other hand, an estimated 20 million CDs contain MediaMax™ software. It isn’t clear whether that number includes or is separate from Canadian figures.

Various problems have been identified with each of these DRM technologies. Although there are some differences between the two, there are also fundamental similarities. The following description, based on reports by recognized computer experts, is meant to be a relatively non-technical overview of the XCP and MediaMax™ programs.

When a CD containing XCP or MediaMax™ is inserted into a computer’s disc drive, it plays automatically if “autorun” is enabled on the system (as it is on most standard PCs). If “autorun” is not enabled, the user must start the installation process manually as he/she is not able to play the CD without doing so.

Before installing any files on the computer, XCP CDs will prompt the user to agree or disagree to an End User Licence Agreement (EULA), the terms and conditions of which are described in more detail below. Notably, however, when a MediaMax™ CD is inserted into a computer, a dozen files are installed immediately, prior to accepting or declining the EULA. And even if the user declines the EULA, MediaMax™ remains permanently installed and activated on the computer. If the user putatively accepts the terms and conditions of the EULA by clicking “agree”, the installation process will begin (or continue in the case of MediaMax™ CDs).

XCP and MediaMax™ are designed to limit the way that consumers can use the music contained on Sony BMG CDs. For example, the technologies prevent consumers from making more than three backup CDs. They also prevent consumers from copying the music to portable devices that are not “approved” by Sony BMG. This enables Sony BMG
to restrict compatibility to non-Sony products, such as the wildly popular Apple iPod®.

XCP and MediaMax™ CDs cannot be played through any computer program of the user's choice. They require additional software to be installed onto the computer. This inevitably requires system resources and interferes with the computer's normal functions. Although it is questionable whether performance standards would deteriorate noticeably to average users, the fact remains that both programs consume processor power, memory and Internet bandwidth.

Far more serious, however, is the fact that both programs increase security vulnerabilities. XCP installs itself as a rootkit at the core of the computer's operating system. Its presence and operation are concealed from the average user. It does not appear in the Windows® task manager, and can only be detected by experts using sophisticated tools. Because of the hidden nature of rootkits, they render computers vulnerable to hackers and viruses. Malicious programs have, in fact, been created to exploit these security vulnerabilities. MediaMax™ also renders the computer more vulnerable to exploitation. Although it is not a rootkit, the technology requires its user to login as an administrator, which grants enough privileges to manipulate any part of the computer system. One of MediaMax™'s components also runs as a "kernel process", meaning it always has access to the whole system. Sony BMG had been aware of potential vulnerabilities well before the story went public, but it was widespread reporting of security concerns that led Sony BMG, First4Internet and SunnComm to provide consumers with a patch to address these initial design defects.

XCP and MediaMax™ were practically impossible for average consumers to uninstall. XCP, for example, did not appear in the add/remove programs window of the computer's control panel. By attempting a manual uninstall, a user could damage the operating system and cause Windows® to malfunction. In order to successfully uninstall XCP, consumers were required to contact Sony BMG, input personal information into a form requesting further instructions via e-mail, respond to that e-mail either by visiting a Web site to update (rather than uninstall) the software or by repeating the request for an uninstaller, waiting one business day for a subsequent reply containing a link to yet another location where the program can finally be uninstalled. Users had similar difficulties attempting to uninstall MediaMax™.

Moreover, the uninstall procedures initially offered to consumers actually exacerbated the vulnerability problems by creating further security holes. For example, First4Internet and SunnComm uninstallers actually installed different components that could be used by any Web site to seize control of the user's computer, silently download, install and run software and then do anything it likes.

Of further concern is the fact that XCP and MediaMax™ "phone home" to Sony BMG. The programs surreptitiously establish a connection between the user's computer and servers owned or controlled by Sony BMG. They report information about the user's computer, operating system, software and Internet connection, and about the CD that the user is listening to at the time. Sony BMG maintains that this information is simply for the purpose of enhancing the consumer's experience by, for example, delivering album artwork and lyrics. However, MediaMax™ data transmissions reference a feature called "Perfect Placement", which, according to SunnComm, "presents the record labels and music producers with unparalleled targeted marketing opportunities". The basic point is it is impossible to know what exactly is done with the information collected.

THE TERMS

Consumers who purchase XCP or MediaMax™ CDs and play them in a computer putatively agree to two related but different contracts. The first contract is formed at the point of sale between the consumer and the retailer. It addresses the terms and conditions related to the physical medium, and perhaps also the disc's digital content. In respect of this sales contract, there is no privity between the consumer and Sony BMG. However, a second contract, this one involving the consumer and Sony BMG, deals with the terms and conditions related to the content contained on the CD, including music and software. The relationship between these two contracts is fuzzy, and as discussed in Part II complicates an analysis of potential liabilities.

PURCHASE AND SALE

Consumers can purchase Sony BMG CDs through various retailers, including bricks and mortar specialty, big box or discount stores, such as HMV, Best
Buy or Wal-Mart, as well as online merchants like Amazon. At the point of sale, it is difficult to learn exactly what restrictions apply in terms of copying and compatibility. Online retailers will often include a statement on the Web page describing the product as a “CONTENT/COPY-PROTECTED CD”.

Customers of traditional retailers have the opportunity to examine the CD prior to purchase. Staff would not typically draw a customer’s attention to or further explain the CD’s limitations at the time of sale. Instead, consumers must rely on their own knowledge and inspection of the product. XCP CDs state at the upper-left corner of the jewel case: “CONTENT PROTECTED”. Some but not all MediaMax™ CDs have stickers on the front also stating: “This CD is protected against unauthorized duplication. It is designed to play on standard playback devices and an appropriately configured computer (see system requirements on back)...”. On the back of XCP and MediaMax™ CDs there is a small box that lists, for example: “Playback: CD/DVD/PC/Mac. PC: Windows 98SE/ME/2000SP4/XP, Pentium II, 128 MB RAM, IE 5.5+. Mac: OK. Ripping: PC: Windows Media Player 9.0. Mac: OK. Portable Devices: Secure Windows Media. Limited Copies”. The Electronic Frontier Foundation (EFF) has posted pictures of the XCP and MediaMax™ notices to help consumers spot these CDs.10

The extent to which the average consumer is aware of, let alone understands, these notices is unclear. Many consumers might reasonably expect that a “content protected” CD would still allow them to make unlimited backup copies. Consumers might also reasonably expect that if the CD were not compatible with the world’s most popular portable device, the iPod®, that fact would be expressly mentioned rather than implicitly omitted. The legal significance of these points is explained in Part II of this article.

USE OF THE CONTENT

If the consumer uses an XCP or MediaMax™ CD in an ordinary CD player, no further contractual issues arise. Sony BMG and the consumer will have no direct contractual relationship. If, however, the consumer attempts to play the CD using a computer, they are prompted to agree or disagree with terms and conditions contained in the EULA.

Sony BMG is aware that it cannot install and run XCP and MediaMax™ on consumers’ computers without consent. The EULA, therefore, provides an opportunity to obtain such consent. It also gives Sony BMG the opportunity to dictate the scope of the consumer’s ability to use the music contained on the CD, and to establish the terms and conditions regarding each parties’ rights and liabilities. Consumers have no ability to alter the terms and conditions, but are instead offered this contract of adhesion on a “take it or leave it” basis.

One of the key paragraphs preceding the EULA reads as follows:

As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small propriety software program (the “SOFTWARE”) onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted. However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.

The EULA itself sets out a number of terms and conditions, all of which are favourable to Sony BMG. The EULA purports to limit the rights a consumer would otherwise have as a result of ownership of the physical product.

It begins fairly non-controversially by granting the consumer a limited licence to use the music and software contained on the CD. Next it describes the features of the DRM system: for example, that it limits users to making three backup CDs and prevents users from listening to music except through an approved media player.

Of course, what the EULA does not say here is also significant. The EULA does not explain the precise nature of the program being installed, the security vulnerabilities it creates, the practical impossibility of uninstalling it, the surreptitious surveillance it facilitates or any other of the technology’s features.
The EULA does state that all of the consumer’s rights to use the music shall terminate if he/she no longer owns the physical CD. This condition expressly references a transfer by sale, gift or otherwise, but similar a provision later in the EULA would also seem to apply where the consumer’s CD is stolen or possession is lost for some other reason. Furthermore, the consumer would lose all rights upon filing for bankruptcy or being subjected to other legal processes pertaining to his/her assets or property.

In addition to expected prohibitions on copying and distribution, the EULA states that the consumer cannot change or make derivative works from the music. That would ostensibly prohibit remixing or using the music as background for a slideshow or home movie. The EULA also prohibits the consumer from exporting the music out of his/her country of residence.

The EULA purports to exclude any and all warranties pertaining to the music and software. Indeed, the consumer is required to defend and hold Sony BMG harmless for any damages that result from the customer’s use of the music and/or software. Sony BMG disclaims responsibility for damages caused to the consumer or the consumer’s computer system, and in any event limits its liability to $5. And if the consumer wishes to sue to obtain that $5, he/she must do so in New York courts, according to New York law and without a jury trial.

According to the EULA, Sony BMG and any of its third party licensors may use the XCP or MediaMax™ software, as well as any approved media player, to enforce their rights under the contract at any time, without any notice to the consumer.

Consumers who have read and understood the implications of this EULA might be understandably reluctant to agree to it. But as the text preceding the EULA reminds consumers, if they do not agree they will be unable to use the CD in a computer. By the time a consumer has had a chance to consider the terms and conditions of use, many retailers will refuse to refund or exchange the product because the package will already have been opened.

**REACTIONS**

To summarize, both the XCP and MediaMax™ technologies used by Sony BMG:

- take up computer systems’ resources (disk storage space, if not also processing power and memory capacity, and also Internet bandwidth);
- make computer systems vulnerable to hackers and viruses (XCP because it is a hidden rootkit, and MediaMax™ because it allows for access to the computer’s main administrator account);
- are practically impossible for most people to uninstall;
- surreptitiously monitor and report information about consumers’ computer systems and listening activities; and
- come with an EULA containing false or misleading misrepresentations, and which fails to disclose material facts. Moreover, in the case of MediaMax™, the software was installed prior to and regardless of the user accepting the EULA.

It is not surprising that once people became aware of what Sony BMG was doing and how it was doing it, they were outraged. People became even angrier after hearing Sony BMG’s initial response to this scandal, which was unapologetic and even belligerent. The President of Sony BMG’s Global Digital Business division said in an interview with National Public Radio: “Most people, I think, don’t even know what a rootkit is, so why should they care about it”?

These events troubled public interest advocacy groups like the EFF, which wrote an open letter to Sony BMG expressing its concerns. Sony BMG’s response to the EFF’s letter was slightly more conciliatory, although far from satisfactory. The company said that it had taken steps to address the problems with XCP even before the EFF had raised concerns, including issuing security patches, providing uninstallers and implementing a recall and exchange program. It denied, however, the existence of any problems with the MediaMax™ technology. Also, according to Sony BMG, “it does not believe that its use of XCP copy protection software or its EULAs violated any laws”.

Many artists were not pleased with Sony BMG’s behaviour. The negative reaction is understandable when one considers the direct impact that this public relations fiasco had on certain XCP and Media-
Max™ albums. For example, when news about the rootkit on Van Zant’s hit CD broke, its ranking on the Amazon.com bestseller list plummeted.4 Carlos and Deborah Santana were forced to explain they have no control over whether copy protection is used on Santana records, and apologized to fans by saying “we feel extremely sad and angry that we have caused our fans distress with what we intended would bring you joy”.5 Although none of the CDs recorded by the Dave Matthews Band contain XCP or MediaMax™, the group has nevertheless objectied to its labels DRM tactics.6 The fact that they posted instructions to circumvent copy protection technologies on their Web site illustrates just how out of touch Sony BMG is with its artists.

Part II of this article will be published in the March 2006 issue of this newsletter.

[Editor's note: Jeremy deBeer is a law professor at the University of Ottawa. Professor deBeer specializes in intellectual and classic property and related areas of law.]

8 An antivirus company named F-Secure had allegedly notified Sony BMG of the rootkit issue in early October 2005.

99
PART II: LEGAL & POLICY IMPLICATIONS

Part I of this article chronicled Sony BMG’s use of digital rights management (DRM) systems on tens of millions of music CDs. It explained how it was discovered that these DRM systems, although designed to prevent unlicensed copying, actually compromised the security of computer systems, were impossible to uninstall and surreptitiously reported on consumers’ computers and listening activities. Moreover, they required consumers to agree to restrictive contractual terms through a misleading and onerous End-User Licence Agreement (EULA).

Consumers, public interest groups and government officials were not satisfied with Sony BMG’s voluntary responses to the problems described above. As a result, numerous legal actions were taken. Part II of this article will explain and analyze the legal and policy implications of Sony BMG’s use of restrictive contractual terms and DRM technologies. Particular emphasis will be placed on Canadian developments.

Within two weeks of this story breaking, Sony BMG, its parent companies, First4Internet, SunnComm and other unnamed defendants were all hit with lawsuits on behalf of representative plaintiffs across the United States. Plaintiffs alleged a wide range of causes of action, depending on the jurisdiction in which the claim was filed. Complaints included breaches of various statutes, common law torts and implied contractual warranties. Various financial and injunctive remedies were requested.

In early December 2005, a number of the pending actions were consolidated. By late December a preliminary settlement was reached, and by mid-January 2006, it was judicially approved. The settlement resolved all of the pending class action claims, but not any inquiries or actions by state or federal governments. It also only addressed the problems of people who purchased XCP and/or MediaMax™ CDs but did not experience damage to their computer systems as a result. In other words, it basi-
cally enabled consumers to get what they thought they had initially bargained for, plus some additional music for their trouble. It also required Sony BMG to acknowledge that its DRM technologies and its EULAs were problematic, to provide updates and uninstallers, to waive some of the EULA’s offensive provisions, to recall all XCP CDs and agree to a two-year moratorium on the use of MediaMax™, to obtain third party verification of its privacy practices and to promise independent testing of DRM technologies in the future. The settlement allowed consumers to opt-out and commence an individual action, which at least one consumer has done.2

Canadian class action lawyers were slightly slower to mobilize than their American counterparts. However, lawsuits were launched in Québec,3 British Columbia4 and Ontario.5 The claims sought Cdn$20 – 50 million, plus punitive and other damages, an accounting of profits and costs and interest. It is probable that these actions will be settled along the lines of the U.S. claims.

Because of the broader importance of the issues, it is worth taking a look at Canadian laws applicable in this type of situation. Actions could succeed under the federal Competition Act,6 provincial consumer protection laws like Ontario’s Consumer Protection Act7 (CPA), federal or provincial privacy laws and common law torts such as trespass to chattels, negligence (including products liability and negligent misrepresentation), deceit and conspiracy.

COMPETITION LAW

The Competition Act provides a private right of action in respect of material false or misleading representations made to the public for the purpose of promoting a product or business interest.8 Sony BMG has apparently made numerous false and/or misleading statements in the EULA, including misrepresenting the precise nature of the XCP and MediaMax™ technologies, the security vulnerabilities they create, the inability to install them and the data transmissions they initiate surreptitiously. It is also arguable that representations at the point of sale were misleading, given the vagueness of the statements on the CDs’ packaging. Professor Weatherall, an Australian expert on the subject of DRM regula-
tion, has suggested that Sony BMG’s conduct would likely run afoul of laws pertaining to misleading or deceptive conduct in Australia, and it is likely that the legal consequences in Canada are similar. In defence to an action under the Canadian Competition Act, it could be argued that any misrepresentations were not made “knowingly or recklessly”, as required by the statute. On balance, however, a plaintiff’s case would seem to be strong.

Also, the Commissioner of Competition may on her own initiative launch an investigation into possible violations of the criminal provisions of the Competition Act, and at any time can refer the matter to the Attorney General of Canada for prosecution. The Commissioner can apply to the Competition Tribunal to restrain alleged violations of the Competition Act. Professor Geist has noted that the Competition Bureau is often reluctant to intervene in matters concerning intellectual property protection. However, the issues raised by Sony BMG’s actions have little to do with copyright. There would seem to be no impediment to an investigation into this matter.

CONSUMER PROTECTION LAW

Ontario’s CPA provides remedies for breach of implied warranties and for unfair practices involving misrepresentations. The legislation contemplates class action proceedings to adjudicate such claims.

In terms of implied warranties, s. 9 distinguishes between contracts for services, which must be of a “reasonably acceptable quality”, and contracts for the sale of goods, to which the Sale of Goods Act (SOGA) apply. According to computer law expert Barry Sookman, sales of records, books and videotapes have been recognized as sales of goods despite containing intangible property. Sales of pre-packaged software would likewise implicate provincial sale of goods law. Whether Sony BMG was selling goods or providing services, it may have violated warranties relating to quality, quiet possession, fitness for purpose and/or merchantability.

Although protections under the SOGA may normally be negatived or varied by agreement or course of dealings, the provisions of the CPA apply despite any agreement or waiver to the contrary. The CPA states that any term purporting to avoid implied conditions or warranties under the SOGA is void. The disclaimers in Sony BMG’s EULA, therefore, are unenforceable.

The CPA also prohibits unfair practices, which includes making false, misleading, deceptive and/or unconscionable representations. It is fairly straightforward to argue that several representations made by Sony BMG were false, misleading and/or deceptive. It may be more difficult to argue that Sony BMG’s representations were unconscionable. Canadian courts have been reluctant to deny the enforceability of “clickwrap” agreements or characterize them as unconscionable. However, previous cases considered fairly standard and reasonable provisions, unlike those in Sony BMG’s EULA.

If Sony BMG’s representations were found to be false, misleading, deceptive or unconscionable, consumers would be entitled to rescind the contract and obtain any remedy available in law. Also, if retailers of Sony BMG CDs and/or First4Internet or SunnComm were involved in such practises, they would be jointly and severally liable.

As mentioned in Part I, there is a complex relationship between the contract entered into by a consumer and a retailer at the point of sale and the contract formed with Sony BMG via the EULA. It might be the case that representations on the CD packaging are incorporated only into the former contract — i.e., between the consumer and the retailer. If a consumer wished to pursue Sony BMG in respect of inadequate disclosure at the point of sale, the action may need to be based upon negligent misrepresentation, under which privity is not required. Conversely, it might be difficult to obtain a remedy from a retailer on account of misrepresentations contained in the EULA, unless those terms and conditions are somehow implicitly incorporated into the contract of sale. Or, perhaps it could be argued that a retailer’s failure to inform the consumer that he/she would be required to enter into a subsequent contract in order to play the CD in a computer itself constitutes a false, misleading, deceptive or unconscionable representation.

One of the Ontario class actions had pled that the officers and directors of the defendant companies are guilty of offences under the CPA for contravening the provisions dealing with implied warranties and unfair practices. It is unclear, however, whether and
how a representative plaintiff in a civil proceeding would be able to follow through with such claims.

The Minister of Consumer and Business Services does have the power to enforce the CPA and other legislation for the protection of consumers. Ministry staff may also gather information, independently or by appointing investigators, about matters that may be in contravention of the Act. Investigatory and remedial powers are broad. Although there has been no indication that Ministerial action is pending over the Sony BMG incident, this remains a possibility.

PRIVACY LAW

It could be argued that Sony BMG has run afoul of Canada’s federal privacy law, the Personal Information and Protection of Electronic Documents Act (PIPEDA). Jurisdictional issues would probably not be barrier to the application of PIPEDA in the context of Sony BMG’s actions. But a plaintiff would need to establish that Sony BMG has collected personal information about an “identifiable individual” to trigger this legislation. As explained in Part I, XCP and MediaMax transmit information about a user’s computer system, software and Internet connection. In theory, this could be used to obtain further information, but may not constitute personal information per se. To succeed, the argument here would have to be that PIPEDA applies to information that renders a person identifiable, not just identified.

Consent issues would also have to be overcome. In addition to the fact that the misleading EULA may have been ineffective to acquire consent, Professor Kerr has pointed out that a DRM licence aiming to circumvent PIPEDA or other laws might conceivably be invalid on the grounds of statutory illegality or public policy.

The more basic issue, however, is that Canadian privacy legislation has “more bark than bite”. Even if Sony BMG has violated the principles of PIPEDA, there would seem to be nothing an Ontario court could do about it at this point. A complaint must first be brought before the Privacy Commissioner, and even then, the Commissioner is without the power to make orders or impose proportionate sanctions.

Nevertheless, under PIPEDA, the Privacy Commission does have the authority to initiate a complaint and investigate the Sony BMG matter. Given that she has expressed concerns about the potential for DRM systems to compromise privacy rights, it is conceivable that an investigation might still be forthcoming.

TRESPASS TO CHATTELS

Liability might also arise under the tort of trespass to chattels, because Sony BMG has intentionally interfered with end-users’ possessory rights in respect of computer hardware and software. Although this tort is well-established under English, Canadian and American common law, it has been applied only recently in the computer context. No Canadian case has yet endorsed a claim for cyber-trespass, but there is ample precedent in the United States to support such an action, if non-negligible harm has occurred. Note that the traditional English authorities (i.e., not in the digital context) do not require any harm at all; the tort is actionable per se. The Canadian position on the harm issue is unsettled.

Some commentators have resisted the expansion of the cyber-trespass doctrine, largely because of its potential to further entrench property concepts in cyberspace. Although that concern is well-founded, it is important to distinguish situations where software is actually installed on a user’s computer from cases where the doctrine is used to stop unwanted e-mail messages, to thwart competition by preventing Web site scraping and/or to limit expression and stifle dissent. Where software is actually installed thus interfering directly with the user’s possession and enjoyment of the computer, a claim for trespass to chattels is more straightforward. Nevertheless, a solid theoretical understanding of this tort is necessary to ensure the law is developed in a principled manner.

The EULA presents the most serious obstacle to a successful trespass to chattels claim. Consent is a defence to trespass (as well as the other tort actions discussed below), and the EULA correctly indicated that a small program would be installed on the user’s computer. The law often presumes that users will have read, understood and agreed to such terms and conditions. On the other hand, consent is only a valid defence if it is informed. Here, arguably, consumers were not made aware of the nature and extent to which their possessory rights would be compromised.
NEGLIGENCE

It is possible that Sony BMG, First4Internet and SunnComm are liable for negligence by defectively designing DRM programs, and/or failing to warn about foreseeable harms involved with these products. Two types of harm may be relevant: actual damage done to a user’s system or network, and the creation of unreasonable security risks.45

There is an established duty of care owed by product manufacturers to end-users. Whether the standard of care has been breached would be a controversial issue. Although it is true that security vulnerabilities are commonplace and inevitable in the software industry, it is arguable that this software is unreasonably risky. Reasonableness may depend upon various factors, including a cost-benefit analysis or consideration of the social utility of DRM technologies generally. It is unlikely that the harms experienced were too remote to be recovered. In terms of damages, consumers could conceivably recover for things such as the cost of diagnostic tests and repairs by computer technicians, and consequential time and productivity losses. Factual causation, however, may be a thorny issue.

Proving Sony BMG did attempt to mitigate consumers’ losses by eventually providing patches and uninstallers, but under the circumstances, consumers could not be blamed for sceptically taking matters into their own hands. Given the nature of the EULA, it may be difficult for Sony BMG to rely on defences such as consent.

As suggested above, issues of privity of contract may require a plaintiff to pursue an action in negligence for misrepresentations made at different times by Sony BMG and/or CD retailers. Such a claim could be made in addition to, or in the alternative to, a claim under products liability or other branches of negligence.

CONSPIRACY, DECEIT AND OTHER COMMON LAW TORTS

There are several other torts that may apply to the actions of Sony BMG, First4Internet and/or SunnComm, not to mention CD retailers. It is unlikely that these causes of action would result in any substantive remedial benefits to a potential plaintiff, as compared to other torts. For example, to prove conspiracy a plaintiff must establish a separate crime, tort or breach of contract, unless it can be shown that the co-conspirators acted intentionally.46

There may, however, be a strategic procedural advantage to an allegation of conspiracy to commit fraud or deceit, for example. Pleading negligence can be a complicated ordeal, especially in a class action context where there may be a large number of individual issues concerning, among other things, damages. Similarly, it may be better to leave it for the defence to initiate a discussion of the potential implications of an EULA.

CONTRACT LAW

Because of the existence of the CPA and the SOGA, it is unlikely that consumers would need to turn to common law rules of contract to address their concerns. That does not mean, however, that basic contract law is entirely inapplicable. Sony BMG artists might seek redress against their record label for negative publicity and, potentially, lost sales resulting from Sony BMG’s actions. So far, it does not seem that any Sony BMG artists have initiated an action against their record label, but this is not outside the realm of possibilities.

A Sony BMG recording artist will likely have entered into a personal services contract establishing the obligations of the artist and the record label.47 If so, the label may have special responsibilities and may even owe to the artist a fiduciary obligation. It is difficult to speculate in the abstract about possible contractual terms regarding the use of DRM systems in Sony BMG’s marketing and distribution of an artist’s recordings. But where Sony BMG has exploited an inequality in bargaining power, used undue influence or imposed unconscionable terms upon an artist, it is conceivable that the recording contract could be rescinded and damages sought. Equitable remedies could also be available.

MOVING FORWARD

Sony BMG is not the only music company using DRM systems. There are hundreds of millions of copies of hundreds of albums titles in circulation employing MediaMax™ or other DRM systems. Restrictive contractual terms and technologies are also used to control other types of digital content. The reason these events are significant, therefore, is not because they are unique. Rather, they illustrate the
potential abuses that can occur if consumers are not protected from the widespread deployment of DRM systems.

An analysis has shown that a number of laws might apply here, including competition, consumer protection and privacy statutes as well as common law tort and contract doctrines. Protection is piecemeal, and gaps do exist, but it seems that the main problem is not finding a viable cause of action. Successfully litigating a claim is another matter.

Class action procedures can and have been used to facilitate access to justice in respect of unacceptable DRM practices, but this process has limits. It would be a complicated undertaking to prove and quantify harms done to computers, security compromises or losses in productivity, and to attribute such damages to a specific DRM system. Although copyright holders are able to seek statutory damages if unable to prove actual harms caused by copyright infringements, there are no similar protections available to consumers.\(^{48}\) Recovery, therefore, might be limited to a fraction of the cost of the original product. That is an impediment to litigation, and undermines the law’s deterrent effects.

There are several options for overcoming these challenges. First, government regulators could exercise their existing legal powers to intervene in matters such as this. The State of Texas, for example, commenced an action under Texas’ Consumer Protection Against Computer Spyware Act.\(^{59}\) The Attorney General of the State of Florida and New York State Attorney General Eliot Spitzer are also investigating this matter.\(^{60}\) An Italian consumer rights organization has asked the government there to look into Sony BMG’s behaviour.\(^{51}\)

There has been no indication, however, that Canadian authorities at the federal or provincial level in Canada will get involved. Although there are no Canadian anti-spyware statutes akin to the Texas legislation, there are several grounds on which investigation could be justified if not required. As explained, Canadian competition, consumer protection and privacy laws include mechanisms for governmental intervention.

Regardless of whether or not Canadian regulators choose to exercise their powers under existing laws, Canadian legislators might consider responding to these events by enacting new legislation. Specific legislation could be enacted to deal with abuses of DRM systems, general anti-spyware statutes could be developed or consumer protection law as a whole could be bolstered. In deciding whether a general or specific response is preferable, government policy makers must weigh the flexibility of a technologically neutral approach against the precision of a tailored solution. Either way, stronger legal protection from technological measures seems warranted.\(^{52}\)

If new laws are necessary, one of the key questions is: which level of government is competent to enact such legislation. In a recent book chapter, I concluded that a strong argument could be made that the provinces have exclusive or shared jurisdiction over the matter of DRM systems.\(^{53}\) Other authors have also noted that DRM systems are really about commercial business models, privacy and computer security, and are only weakly connected to copyright law.\(^{54}\) The range of federal and provincial laws discussed in this paper confirms the importance of both federal and provincial involvement in the DRM debate.

Whichever level of government is addressing this matter, several principles ought to guide the development of legislation dealing with DRM systems. To begin, there must be a transparent and coherent policy on the compatibility of regulations addressing DRM systems with other laws, such as Canada’s private copying levy.\(^{55}\) These issues cannot be viewed in isolation. Moreover, legislation must protect fundamental Canadian values like respect for privacy, freedom of expression, market competition, informed contractual autonomy and responsibility for harms caused,\(^{56}\) while at the same time respecting the rights of music creators and recognizing the economic interests of record companies.\(^{57}\) Law and policy makers must pay attention to the Supreme Court’s remarks about the need to strike a balance.\(^{58}\)

So far, however, legislators’ response to DRM systems has been lopsided. Although Bill C-60\(^{95}\) would have set limits on the legal protection of DRM systems, that legislation addressed only one side of the broader issue. In other words, the federal government would have protected technological measures from consumers, but, as the foregoing analysis has shown, consumers also need protection from technological measures. The Sony BMG story confirms that it is time for both levels of government to adopt balanced laws addressing all aspects of DRM systems.

[Editor’s note: Jeremy deBeer is a law professor at the University of Ottawa. Professor deBeer specializes in intellectual and classic property and related areas of law.]
A law student in the United States has even created a Web site to track various proceedings: see <http://www.sonsuits.com>.

Mark Lyon v. Sony BMG Music Entertainment, Complaint, County Court of Hinds County, Mississippi, First Judicial District (January 5, 2006).


Competition Act, op. cit., s. 52.

Competition Act, op. cit., s. 23.

Competition Act, op. cit., s. 75.

M. Geist, “Anti-circumvention Legislation and Competition Policy” in M. Geist, ed., In the Public Interest: The Future of Canadian Copyright Law (Toronto: Irwin Law, 2003), at 211.

Consumer Protection Act, op. cit., s. 8.


Sale of Goods Act, op. cit., s. 53.

Consumer Protection Act, op. cit., s. 7(1).

Consumer Protection Act, op. cit., s. 9(3). Certain terms and conditions might also be void pursuant to the common law of contract: see Sale of Goods Act, op. cit., s. 57(1).

Consumer Protection Act, op. cit., Part III.


Consumer Protection Act, op. cit., s. 18.

Consumer Protection Act, op. cit., s. 18(12).

Consumer Protection Act, op. cit., s. 116.


See e.g., G.H. Fridman, The Law of Torts in Canada (Toronto: Carswell, 2002), ch. 28.


Copyright Act, R.S.C. 1985, c. C-42, s. 38.1.


See e.g., J. Bailey, “Deflating the Michelín Man: Protecting Users’ Rights in the Canadian Copyright Reform Process” in M. Geist, ed., In the Public Interest: The Future of Canadian Copyright Law (Toronto: Irwin Law, 2005), 125; I. Kerr, “If left to their own devices ...” in M. Geist, ed., In the Public Interest: The Future of Canadian Copyright Law (Toronto: Irwin Law, 2005), 167; M. Geist, “Anti-circumvention Legislation and Competition Policy” in M. Geist, ed., In the Public Interest: The Future of Canadian Copyright Law (Toronto: Irwin Law, 2005), 211.

