

POLICING THE NEW DIGITAL BORDERS

By Julius Melnitzer

Powerful new “technologies that draw invisible fences around copyrighted work – and others that bust them open – are making copyright the hottest new area in IP

Professor Ian Kerr is one of those rare human beings who has managed to track the less than intuitive association among ethics, intellectual property (IP) and shopping carts. Given his occupation, one might have expected that Kerr, who holds the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa's Faculty of Law, would have been inspired by the kind of obscure theoretical study that underpins much academic inspiration. As it turns out, Kerr found his inspiration in a Loblaws' parking lot.

As he blissfully pushed his grocery-laden cart from the store, it came to a rather abrupt halt. As pragmatic as he is academically talented, Kerr's first assumption was that a rock had lodged between one of the wheels and the cart's frame. What he discovered instead was a lock on the wheel, one enabled by a beam of infrared light that circumscribed Loblaws' property line. It would be extreme to suggest the discovery offended him, but it did set him thinking.

"What if a GPS system disabled golf carts that ventured too close to the greens in contravention of club rules?" he asked himself. "What if wireless systems that track and monitor speeding could automatically apply the brakes of a car?"

He also has an answer: "We would have perfect control, but it would override the right to use property in times of necessity. That's what would have happened had the Loblaws lock existed on the shopping carts upon which so many people in New Orleans depended in the aftermath of Katrina."

To Kerr, perfect control is what prohibitions against circumvention of technical protection measures (TPM), the most controversial component of the digital rights management (DRM) debate, are all about.

"DRM technology automates norms so people won't have to make choices," he says. "In such a world, technology makes decisions that practical wisdom used to make. The result is that DRM can interfere with our legal autonomy, particularly the ability to exercise our rights of fair use and free speech."

The difficulty, however, is that DRM—sometimes called digital restrictions management—has become an integral feature of new digital marketing initiatives that promise to shape how content is monetized. And that means that lawyers are going to be at the forefront of a rich new motherlode of commercial activity.

It bears noting that DRM is not simply about anti-circumvention legislation, which is only the latest layer of protection devised for copyright holders. Copyright law, contract law in the form of rights grants and legal permissions, and TPMs themselves are all components of a complete DRM package. Because TPMs, their treatment in law, and their interaction with other components of DRM are at the heart of thousands of new business models, lawyers seeking to protect their clients will need to understand how these components meld. "Lawyers will have to be knowledgeable about the whole suite of protections if they're going to help their clients bring these new distribution models to market." says Mark Hayes of Blake, Cassels & Graydon LLP,

All this arises from the fact that the traditional sale and licensing techniques used to commercialize music, TV shows, and cinema is hardly the preferred business model for digital products these days. In fact, it's downright outmoded. Instead, creators and distributors are looking for ways to attach different kinds of limited rights to their digital products.

"DRM is already used in broadcast signals, internet encryption and e-commerce," says Barry Sookman of McCarthyTetraault LLP. "By providing protection from copying, DRM allows publishers to make their works available in diverse ways to different people. It makes possible the concept of selling the same thing to everybody or different products to individuals. It provides diversification for consumers who will pay less for the uses in which they are truly interested."

With the appropriate protection, content distributors can determine what kind of customer sharing is the most profitable and then monetize that sharing with pay per view, subscriptions, advertising or other revenue-generating approaches. TPMs can control who can access content, when users can access it, and for what purposes they can use it.

"Digital rights management and access protection entails the operation of software or hardware control that can monitor, regulate and price uses of digital files that contain protected content or software," explains Michael Einhorn, an economist who is a director at CONSOR Intellectual Asset Management, an international IP consultancy. "Electronic monitoring of a protected file is generally administered now through attached rendering software or containment that ensures access only to authorized users. Depending on the price that a user pays, protective owners may also limit use by number of plays, duration of access, temporary or partial uses, lending rights, and the number of devices on which the files may be accessed."

But unless they can be sure that the limits of their licenses will not be breached, tremendous risk exists for rights holders in an environment where the ubiquity and ease of use of copying technology and digital transmission means that a single act of unauthorized reproduction can proliferate globally in seconds.

"You have to think about DRM as a process where copyright holders try to stop piracy at the point of access where someone cracks TPM and makes content public," Sookman says. "It's an attempt to ensure that pirates don't completely emasculate copyright holders."

It's not that content providers are unrealistic. "Record companies, movie distributors and software companies all know that everything they do is trackable," says Sunny Handa of Blake, Cassels & Graydon LLP. "But TPM prevents copying from becoming something anyone can achieve. It's a way of reducing the palpable fear that new business models will open the floodgates and give too much away for free."

The upshot is that, just as Loblaw's builds theft protection into its shopping carts, copyright holders and content disseminators are building TPMs into digital materials as a way of managing access and copying so that users cannot abuse the limited rights they pay for. "The whole point of DRM is protecting new methods of distribution without the need for individualized consent," Kerr says.

Indeed, Danielle Parr, executive director of the Entertainment Software Association of Canada, a trade association of video game publishers and distributors, notes that Canada is one of only a few developed countries that has not criminalized the distribution of anti-circumvention devices. "TPMs, supported by strong anti-circumvention legislation, are critical to the future success and growth of our members' business," she says.

The association's members include digital content giants like Microsoft and Sony. It would be easy to assume, then, that the anti-circumvention controversy is a matter of David battling Goliath, much as the Napster litigation was perceived. But a closer look reveals that digital sharing is no longer—and may never have been—simply about a bunch of geek kids developing programs to pirate music or videos. Rather, it's at the heart of the rights that businesses competing in the multimedia world have as against each other. Can they move content from one media to another or from one location to another? Can they reformat content? To what extent can they refer to content? Should paying customers of cable companies be allowed to watch locally blacked-out sports events on "time-shifting" devices?

These are the kinds of questions prompted, for example, by Google's recent US\$1.6 billion acquisition of video-sharing sensation YouTube: Google signed off only after YouTube entered into license agreements (a form of DRM) with major suppliers.

Similarly, Apple's announcement in September that it had developed a device that would wirelessly stream content between computers and televisions has significant DRM implications. It's unlikely that Apple or others will be able to license content for the device unless they agree to the inclusion of TPM to protect the copyholders.

As it turns out, not even the most ardent opponents of anti-circumvention legislation challenge the rights of copyright holders to protect their products. "Nobody argues that we should prohibit the use of TPMs," Hayes says. "The issue is how much of the state's power should be placed behind the technology."

Kerr is of the same view: "The question is not whether we need to protect copyright but whether we need to protect DRM," he says. In other words, the question reduces to this: should Canadian law mandate sanctions against TPM circumvention, or "hacking," as it is commonly known. When Bill C-60, the Liberal's proposed copyright reform legislation, died on the order paper with the demise of Paul Martin's government, the debate took off.

The US, on the other hand, has had anti-circumvention legislation in the form of the Digital Millennium Copyright Act (DMCA) since 1998. Content distributors favour the DMCA as a model for Canadian legislation. The law features broad provisions that potentially outlaw acts of circumvention and the distribution of circumvention devices even in cases where the act of distribution would not amount to copyright infringement. For example, it may be illegal to tamper with DVD encryption even where the intention is to make a copy for personal use — something that would fall under the "fair use" exception to copyright infringement.

In American law, fair use doctrine allows the public to use copyrighted works without permission in ways that do not unduly interfere with the copyright owner's market for her work. Fair use includes personal and noncommercial uses, including uses for the purpose of criticism, media reporting, teaching, comment, scholarship and research. Critics of the DMCA and similar legislation argue that using anti-circumvention-backed TPMs to control access to works, unilaterally eliminates fair use and disturbs the delicate balance between rightsholders and users that has developed in copyright legislation over the years.

But Einhorn reasons that the technical ability to protect, access and monitor use of software and content files may actually benefit consumers. "While suppliers of content conceivably may attempt to use DRM to encumber desirable uses otherwise protected by 'fair use,' content providers who hinder user control necessarily reduce the value of their own product," he says. "Consequently, producers who institute restrictive rules or technologies, or otherwise fail to appreciate the importance of customer ease, actually reduce market demand and prices."

Sookman puts it more succinctly: "There's isn't a publisher in the world who wants to create something that isn't easily used," he says.

The Canadian version of fair use is contained in our somewhat more restricted "fair dealing" principle. The narrower scope of the Canadian doctrine, however, does not materially affect the arguments for or against anti-circumvention legislation.

Another difficulty commonly associated with anti-circumvention legislation is that it can exceed the boundaries of copyright protection altogether.

"We've seen TPM legal rules applied in the US in many ways that have nothing to do with copyright," says Professor Michael Geist, who holds the Canadian Research Chair in Internet and E-Commerce Law at the University of Ottawa's Faculty of Law. "The phenomenon has been described as 'para-copyright,' as in something that is 'above' copyright."

Although US courts have shifted against using the DMCA in this way, there's a chilling effect on innovation. "Although you should win if your circumvention is challenged, even when there is no copyright in the underlying product, you could find yourself spending a lot of time and money in court," Geist says.

That's precisely the situation in which Skylink Technologies, Inc., a small Canadian company, found itself after it developed a universal garage door opener. Chamberlain Group, Inc., was a US company that manufactured garage door opening systems. Skylink's device worked on Chamberlain's products by breaking the codes in the US company's systems. After years of litigation, the US Federal Circuit ruled that the DMCA did not apply where copyright was not in issue. Other American courts, however, have reached differing conclusions.

So the problem persists. "There isn't a very bright line between protecting copyright and protecting other non-copyrighted materials," Hayes says. "The jagged edge of copyright doesn't fit easily with the hard edges of TPM, so we have to make sure that those hard edges don't exceed the appropriate limits of copyright protection."

For example, para-copyright problems might arise in Canada in the case of databases, or with regard to books on which copyright has expired. "If someone packages these in digital form and protects them with TPM which itself has the protection of anti-circumvention legislation, there's an issue as to whether we have unintentionally given non-copyright holders the same user rights that exist in traditional copyright," says Brad Freedman of Borden Ladner Gervais LLP. "And if we have, there's a question of whether we ought to."

The Electronic Frontier Foundation (EFF), a US non-profit group dedicated to "protecting digital rights," has published a lengthy paper entitled "Unintended Consequences: Seven Years under the DMCA." Among other things, the Foundation maintains that the legislation has chilled free expression and scientific research, jeopardized fair use, impeded competition and innovation and interfered with computer intrusion laws.

Brian O'Higgins is chair of the Digital Security Coalition, which represents Canada's leading digital security companies. They tend to take the middle ground in the anti-circumvention debate—that is, enact anti-circumvention legislation but limit culpability to instances where the intention is to breach copyright. He shares some of the EFF's concerns. He points out that when digital security companies search for software vulnerabilities, the flaw may be in the TPM. Legislation worded too vaguely, then, could expose his members to charges of tampering with the TPM in pursuit of the flaw.

"If the government overkills on anti-circumvention legislation, it may cause unintended grief," he says.

One individual victimized by that "unintended grief" is Russian programmer Dmitry Skylarov. US authorities jailed him for several weeks and detained him in the US for five months after he spoke at a conference in Las Vegas.

It seems that Adobe Systems Inc., developer of the ubiquitous PDF format, had complained to authorities that Skylarov had worked on a software program distributed over the Internet by ElcomSoft, his Russian employer. The software allowed owners of Adobe e-books to convert the books into PDF files, which had the effect of removing restrictions embedded in the digital books by e-book publishers. But no one accused Skylarov of infringing copyright or of helping anyone to do so.

"His alleged crime was working on a software tool with many legitimate uses [but which others] might use to copy an e-book without the publisher's permission," write the authors of Unintended Consequences.

Skylarov eventually went home, but not before authorities charged ElcomSoft. In December 2002, however, a jury acquitted the company.

Otherwise, the DRM debate affects lawyers and their clients by raising serious issues in various areas of the law, notably competition law, constitutional law, consumer law and privacy law. Competition issues arise because DRM

can be seen as a form of market control intended to keep competitors at bay. The EFF maintains that many copyright owners have wielded the DMCA to hinder legitimate competitors.

"The DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, and computer maintenance services," says Jason Schultz, an EFF staff attorney. "Similarly, Apple invoked the DMCA to chill RealNetworks' efforts to sell music downloads to iPod owners. It's all contributed to a dramatic drop-off in investment in innovation in the markets for digital music and video player software because the DMCA has made the risks for companies involved in developing media electronics so high that they simply won't take them anymore."

Schultz points to the growth and development of features for digital cameras and cellphones in the last year few years. "But if you look at the iPod, nothing much has happened except it has become smaller and slicker. You can't do much with it that you couldn't do when it first came out."

Constitutional law also comes into play because federal anti-circumvention legislation that is not clearly restricted to copyright issues may infringe on the provinces' jurisdiction over property and civil rights. And DRM legislation can affect consumer law because it will create new relationships between consumers and distributors.

Finally, because many TPMs use identification technologies to monitor the activities of individual consumers who access works, DRM engages privacy legislation. "DRM amounts to nothing more than a legal hack and the acronym should stand for 'digital routine monitoring,'" Kerr says. "If TPM is a virtual fence, DRM is a virtual surveillance system. Surveillance features are crucial to the technological enforcement of the licensing component and enable automated collection and exchange of various kinds of information about particular users, their habits and their individual use of digital material."

Kerr believes that any law protecting surveillance technologies that is used to enforce copyright should also contain express provisions that protect against the piracy of personal information.

The "Sony rootkit" debacle demonstrates the problem. It arose when Sony BMG Music Entertainment surreptitiously installed copy protection software known as the "rootkit" on audio CDs. When computers played the CD, it automatically fed the software into the computer's operating system. But by doing so, it opened security holes for viruses as well as causing other problems.

When Sony's actions emerged, the company supplied a removal utility. As it turned out, the utility merely unmasked the hidden files but did not actually remove the rootkit. The utility also installed additional software that could not be uninstalled without providing an e-mail address to Sony.

Although Sony ultimately provided a satisfactory removal tool, it was forced to recall the offending CDs and is now facing a host of class actions and regulatory investigations.

In Canada, privacy commissioners have expressed public concern over the impact of DRM on privacy. The Ontario privacy commissioner identified two of the primary risks as the possibility of a breach in the databases that store the personal information and the fact that many corporations view the personal information as a corporate asset that can be sold or licensed.

"Rights holders are going to have to be very careful implementing DRM systems, especially where the technology involves the use of personal information," Hayes says.

To be sure, the extent to which any of these problems will arise ultimately depends on the form that new legislation will take. The Conservatives have not tabled a draft bill, but there are strong indications that they will provide more robust protection against DRM circumvention than the Liberals did. "Bill C-60 at least linked copyright infringement with anti-circumvention legislation, because an offence occurred only if the circumvention was for the purpose of copyright infringement and not for innocent purposes like protecting privacy," Geist says. "The sense is that the Conservatives will remove that link, simply make anti-circumvention an offence, and create a series of exceptions from culpability."

Geist's concern, however, is that the legislation will need to create "dozens of exceptions" to avoid the unintended consequences already seen in the US. "The exceptions will almost certainly not catch all of these consequences," he says.

However that may be, it's not too early for lawyers to jump into the fray. "Lawyers should be helping their clients figure out what copyright reform means for them and whether they should try to influence the process," Freedman says.

There can be no denying that getting involved in IP matters over the last decade has proven very profitable to lawyers' bottom lines. "The firm used to discount my work, but the emergence of IP gave me a practice that really mattered," says Gabe Takach, the senior partner in Tory's technology group. "There's no longer any difficulty promising young people a career in any aspect of law that involves intellectual property."

It's true that patents have been the prime focus of IP's emergence, while the profile of copyright law-related issues has lagged despite the prominence of such cases as the Supreme Court of Canada's recent decision in *Robertson v. Globe and Mail*, which dealt with freelancers' rights.

But the emerging business models for commercializing digital content portend an infinite number of new business relationships from the time of a product's creation to the time of its use and as long as the use is continuing. "It will be the job of lawyers to ensure that technology and contractual rights interface in a way that commercializes a digital product and gets it to market safely," says Geist.

Doing that job will generate significant fees. "Years ago, I used to ask students who wanted to work as copyright lawyers what they would do the rest of the time," recalls Ron Dimock of Dimock Stratton LLP. "Today you can have a really decent practice dealing in copyright-related matters. It's a sexy topic in which there is a great deal of interest from the business community."

As there should be from the legal community.

Julius Melnitzer is a freelance legal affairs writer.