

Toronto Computer Lawyers Group: A Year in Review

Barry B. Sookman
May 31, 2005

The right people. The right results.™

McCarthy
Tétrault

mccarthy.ca

Introduction

- Courts are seeing the potential for “Internet liability”.
- Challenges posed by the Internet are being recognized as problems to be grappled with.
- Courts are recognizing that existing laws were not enacted with Internet and new technologies in mind.
- Courts and legislatures are struggling to adapt laws to new circumstances and to reconcile and balance conflicting objectives.
- Recognition of need for law reform.

Internet Liability

“The issue of the proper balance in matters of copyright plays out against the much larger conundrum of trying to apply national laws to a fast-evolving technology that in essence respects no national boundaries... The availability of child pornography on the Internet is a matter of serious concern. E-Commerce is growing. Internet liability is thus a vast field where the legal harvest is only beginning to ripen.” *SOCAN v. Canadian Assn. of Internet Providers*
2004 SCC 13

Internet Liability

“The Internet represents a communications revolution. It makes instantaneous global communication available cheaply to anyone with a computer and an Internet connection. It enables individuals, institutions, and companies to communicate with a potentially vast global audience. It is a medium which does not respect geographical boundaries. Concomitant with the utopian possibility of creating virtual communities, enabling aspects of identity to be explored, and heralding a new and global age of free speech and democracy, *the Internet is also potentially a medium of virtually limitless international defamation* [emphasis added].” *Barrick Gold Corp. v. Lopehandia*, 2004 CanLII 12938 (ON C.A.)

Internet Liability

- “Modern technology such as the Internet has provided extraordinary benefits for society, which include faster and more efficient means of communication to wider audiences. This technology must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights.” *BMG Canada Inc. v John Doe* 2005 FCA 193.
- See also, See, *In re: Charter Communications, Inc Subpoena Enforcement Matter* Case No. 03-3802 (8th.Cir. Jan. 5, 2005) at P. 14. See, *BMG Music et al v Gonzalez* 2005 U.S. Dist. LEXIS 910 (N.D.Ill.Jan 12, 2005) at P. 2., *A&M Records, Inc, v Napster*, 239 F.3d 1004 (9th.Cir.2001) at P. 1016.

Internet Defamation

Internet Defamation - Liability

- “Is there something about defamation on the Internet - "cyber libel", as it is sometimes called - that distinguishes it, for purposes of damages, from defamation in another medium? My response to that question is "Yes“...
- “In the Internet context, these factors must be examined in the light of what one judge has characterized as the "ubiquity, universality and utility" of that medium.”
- “Communication via the Internet is instantaneous, seamless, interactive, blunt, borderless and far-reaching. It is also impersonal, and the anonymous nature of such communications may itself create a greater risk that the defamatory remarks are believed.”
- *Barrick Gold Corp. v. Lopehandia*, 2004 CanLII 12938 (ON C.A.)

Internet Defamation - Liability

Although Internet communications may have the ephemeral qualities of gossip with regard to accuracy, they are communicated through a medium more pervasive than print, and for this reason they have tremendous power to harm reputation. Once a message enters cyberspace, millions of people worldwide can gain access to it. Even if the message is posted in a discussion forum frequented by only a handful of people, any one of them can republish the message by printing it or, as is more likely, by forwarding it instantly to a different discussion forum. And if the message is sufficiently provocative, it may be republished again and again. The extraordinary capacity of the Internet to replicate almost endlessly any defamatory message lends credence to the notion that "the truth rarely catches up with a lie". The problem for libel law, then, is how to protect reputation without squelching the potential of the Internet as a medium of public discourse [emphasis added]. *Barrick Gold Corp. v. Lopehandia*, 2004 CanLII 12938 (ON C.A.)

Internet Defamation - Liability

- “It is true that in the modern era defamatory material may be communicated broadly and rapidly via other media as well. The international distribution of newspapers, syndicated wire services, facsimile transmissions, radio and satellite television broadcasting are but some examples. Nevertheless, Internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by the features described above, especially its interactive nature, its potential for being taken at face value, and its absolute and immediate worldwide ubiquity and accessibility. The mode and extent of publication is therefore a particularly significant consideration in assessing damages in Internet defamation cases.”
Barrick Gold Corp. v. Lopehandia, 2004 CanLII 12938 (ON C.A.)
- See also: *Bangoora v. The Washington Post* (Ont. C.A.) (Internet Jurisdiction)

Internet Defamation – Jurisdiction to Enforce Orders

“Mr. Lopehandia is ordinarily resident in British Columbia, but there is no way to determine from where his postings originate. They could as easily be initiated in an Internet café in downtown Toronto or anywhere else in the world, as in his offices in Vancouver. Given the manner in which the Internet works, it is not possible to know whether the posting of one of Mr. Lopehandia's messages on one of the bulletin boards in question, or the receipt of that message by someone accessing the bulletin board, traveled by way of a server in Ontario to or from the message board. It may have, however. The highly transmissible nature of the tortious misconduct at issue here is a factor to be addressed in considering whether a permanent injunction should be granted. The courts are faced with a dilemma. On the one hand, they can throw up their collective hands in despair, taking the view that enforcement against such ephemeral transmissions around the world is ineffective, and concluding therefore that only the jurisdiction where the originator of the communication may happen to be found can enjoin the offending conduct. On the other hand, they can at least protect against the impugned conduct re-occurring in their own jurisdiction.” *Barrick Gold Corp. v. Lopehandia*, 2004 CanLII 12938 (ON C.A.) (emphasis added)

Internet Defamation – Jurisdiction to Enforce Orders

“Barrick's shares trade on the Toronto Stock Exchange. It is an Ontario corporation with its head offices and employees, and a business reputation, here. Indeed, the protection and vindication of that reputation in Ontario is what gives rise to the court's mandate in cases of this nature. These factors point to a real and substantial connection between Barrick and Ontario rather than to a jurisdictional link with the defendant. However, they suggest that if the appellant were to take an injunction granted by this Court to British Columbia - where Mr. Lopehandia does have a physical presence - and seek to enforce it there, in this "post-*Morguard* era", the order might be enforced against him by the courts of that Province. The argument for enforcement would be based upon the principles of order and fairness and upon what Professor Hogg has referred to as "an implicit full faith and credit rule in the Constitution of Canada" as a result of the Supreme Court of Canada's decision in *Morguard*... It is not for this court to usurp the role of the courts in another province, of course. However, the British Columbia Court of Appeal has held in two relatively recent cases that jurisdiction based upon the "real and substantial connection" test may be satisfied where the province asserting jurisdiction has a real and substantial connection with the subject matter of the litigation or the cause of action asserted: “*Barrick Gold Corp. v. Lopehandia*, 2004 CanLII 12938 (ON C.A.)

Patent Liability

Extra-territoriality of US Patent Law - NTP v RIM

“The question before us is whether the location of a component of an accused system abroad, where that component facilitates operation of the accused system in the United States, prevents the application of section 271(a) to that system. Pursuant to section 271(a), the ‘use’ of ‘any patented invention within the United States . . . during the term of the patent therefor, infringes the patent.” (emphasis added) *NTP, Inc., v. Research In Motion, Ltd.* (CAFC.Dec.14, 2004)

NTP v RIM

- “Section 271(a) does not preclude infringement where a system such as RIM’s, alleged to infringe a system or method claim, is used within the United States even though a component of that system is physically located outside the United States.”
- “When two domestic users communicate via their BlackBerry devices, their use of the BlackBerry system occurs ‘within the United States,’ regardless of whether the messages exchanged between them may be transmitted outside of the United States at some point along their wireless journey.” *NTP, Inc., v. Research In Motion, Ltd.* (CAFC.Dec.14, 2004)

NTP v RIM

“Although RIM’s Relay, which is located in Canada, is the only component that satisfies the “interface” of the “interface switch” limitation in the asserted claims, because all of the other components of RIM’s accused system are located in the United States, and the control and beneficial use of RIM’s system occur in the United States, we conclude that the situs of the “use” of RIM’s system for purposes of section 271(a) is the United States. Also, we conclude that the location of RIM’s customers and their purchase of the BlackBerry devices establishing control and beneficial use of the BlackBerry system within the United States satisfactorily establish territoriality under section 271(a).” *NTP, Inc., v. Research In Motion, Ltd.* (CAFC.Dec.14, 2004)

RIM v NTP- Government of Canada *Amicus Brief*

“Canada does not presume to advise the Court regarding the correct interpretation and application of United States patent law in this case. Canada does, however, believe that the decision of the panel represents on its face a novel and potentially far-reaching precedent regarding the application of United States patent law to cases in which a component of the activities allegedly constituting patent infringement is conducted, at least in part, in Canada. Canada also believes that this decision, as it relates to the interpretation and scope of 35 U.S.C. § 271(a), is susceptible of interpretations that may have unfortunate, and unintended consequences, affecting Canada’s interests, as well as the interests of Canadian companies carrying on multi-jurisdictional operations.” Government of Canada *Amicus Brief*

RIM v NTP- Government of Canada *Amicus Brief*

“The panel’s conclusion that “the location of RIM’s customers and their purchase of the Blackberry devices establishing control and beneficial use of the Blackberry system within the United States satisfactorily establish territoriality under Section 271(a),” ...gives rise to substantial uncertainty regarding the circumstances in which activities conducted outside the United States may form the basis of a violation of Section 271(a). This uncertainty, in turn, carries with it the risk that Section 271(a) may be applied differently depending upon where the allegedly infringing conduct occurs, that is, it is unclear whether Section 271(a) may be applied differently depending upon whether the allegedly infringing conduct occurs entirely within the United States, or partly within the United States and partly outside the United States. The panel’s adoption of this “control and beneficial use” rule also raises the risk that Section 271(a) may be accorded inappropriate extraterritorial application, contrary to basic principles of comity affecting Canada and the United States.” Government of Canada *Amicus Brief*

RIM v NTP- Government of Canada *Amicus Brief*

“Given the number and proliferation of businesses that conduct integrated operations across the Canada-United States border, the panel’s decision affects a substantial number of businesses with Canadian operations, including those carried on using networks and telecommunications. Canada is especially concerned that the uncertainty resulting from the panel’s decision, with its potential for being applied in an inappropriately extraterritorial or discriminatory fashion, may have the further troubling effect of chilling innovation by Canadian companies operating in key industry sectors in Canada, particularly the high technology sector. Such a chilling effect could result, for example, from an understandable concern by Canadian high-technology and other companies that the panel decision might be interpreted and applied in such a way that a company’s continuing to operate in Canada could give rise to a liability under Section 271(a) which the company might not face were it to relocate operations to the United States.” Government of Canada *Amicus Brief*

RIM v NTP- Government of Canada *Amicus Brief*

- “Canada is also concerned that the potential implications of the panel’s interpretation described above would negatively impact the integrity of the operation of Canadian intellectual property laws.”
- “The Government of Canada believes that the novelty of the question presented and decided by the panel with respect to the applicability of Section 271(a) in this case, and the potential consequences of that decision as applied to activities conducted in Canada, warrant the searching scrutiny and considered consensus uniquely available through *en banc* review by this Court. *En Banc* review would allow the Court to be assured that its interpretation of Section 271(a) will not lead to inappropriate, differential application of the statute or to inappropriate, extraterritorial application of United States patent laws...”Government of Canada *Amicus Brief*

Eolas v Microsoft Corp.

- “Whoever without authority supplies or causes to be supplied in or from the United States all or a substantial portion of the components of a patented invention, where such components are uncombined in whole or in part, in such a manner as to actively induce the combination of such components outside the United States in a manner that would infringe the patent if such combination occurred within the United States shall be liable as an infringer.” s271(f)(i) U.S. Patent Act
- “Essentially, the claimed invention allows a user to use a web browser in a fully interactive environment. For example, the invention enables a user to view news clips or play games across the Internet.” *Eolas v Microsoft Corp.* (CAFC. Mar 2, 2005)

Eolas v Microsoft Corp.

- Eolas claimed royalty damages for both foreign and domestic sales of Windows with IE.
- Microsoft exports a limited number of golden master disks containing the software code for the Windows operating system to Original Equipment Manufacturers (OEMs) abroad who use that disk to replicate the code onto computer hard drives for sale outside of the United States.
- The jury awarded Eolas a royalty of \$520,562,280 and granted a permanent injunction.
- “This court must also decide whether software code made in the United States and exported abroad is a “component of a patented invention” under section 271(f).” *Eolas v Microsoft Corp.* (CAFC. Mar 2, 2005)

Eolas v Microsoft Corp.

- “Exact duplicates of the software code on the golden master disk are incorporated as an operating element of the ultimate device... the software code on the golden master disk is not only a component, it is probably the key part of this patented invention. Therefore, the language of section 271(f) in the context of Title 35 shows that this part of the claimed computer product is a “component of a patented invention.” *Eolas v Microsoft Corp.* (CAFC. Mar 2, 2005).
- Case remanded back to district court.
- Should Canadian companies be distributing software from the US to other countries?

Mercexchange LLC v eBay

- “At issue in this case is the fixed-price purchasing feature of eBay’s website, which allows customers to purchase items that are listed on eBay’s website for a fixed, listed price.”
- The jury found eBay and its affiliates liable for a total of \$35 million for infringing the business method patents in issue. *Mercexchange LLC v eBay, Inc.* (CAFC Mar 16, 2005)

Mercesexchange LLC v eBay

“In its post-trial order, the district court stated that the public interest favors denial of a permanent injunction in view of “a growing concern over the issuance of business-method patents, which forced the PTO to implement a second level review policy and cause legislation to be introduced in Congress to eliminate the presumption of validity for such patents.” A general concern regarding business-method patents, however, is not the type of important public need that justifies the unusual step of denying injunctive relief.”
Mercesexchange LLC v eBay, Inc. (CAFC Mar 16, 2005)

Mercexchange LLC v eBay

“Injunctions are not reserved for patentees who intend to practice their patents, as opposed to those who choose to license. The statutory right to exclude is equally available to both groups, and the right to an adequate remedy to enforce that right should be equally available to both as well. If the injunction gives the patentee additional leverage in licensing, that is a natural consequence of the right to exclude and not an inappropriate reward to a party that does not intend to compete in the marketplace with potential infringers.” *Mercexchange LLC v eBay, Inc.* (CAFC Mar 16, 2005)

Patent Reform

- The House Subcommittee on Courts, the Internet and Intellectual Property held its second hearing April 28 on a draft patent reform bill.
- Subcommittee members agreed in principle on the need to clarify the standards needed to obtain permanent patent injunctions.
- The draft bill provides that injunctions will not be granted in infringement actions unless "the patentee is likely to suffer irreparable harm."
- Courts would no longer be allowed to presume the existence of irreparable harm.
- Injunctions will be more difficult to obtain if a patent owner was not using the invention (a "working requirement").

Patent Reform

- Rep. Rick Boucher (D-Va.) expressed concern over maintaining the status quo in the area of patent injunctions. The automatic injunctions available under current law give the patentee enormous leverage during negotiations, he pointed out. "Why should the law give a patentee that kind of extraordinary leverage with the shakedown opportunities it provides?"
- The BlackBerry case in which RIM agreed to pay \$450 million to settle the NTP dispute is used as an example of why reform is needed.
- See, Adam B. Jaffe and Josh Lerner *Innovation and Its Discontents: How Our Broken Patent System is Endangering Innovation and Progress, and What to Do About It* (Princeton University Press, 2004)

Patent – Personal Jurisdiction

- Pedre products, including products alleged to infringe the patents in suit, are extensively advertised on a number of web sites to customers and potential customers in Washington, D.C. including on ‘pedre.com,’ Pedre’s own web site
- There are literally dozens of other web sites which also depict and tout Pedre products. Some of these web sites have hyperlinks to pedre.com.”. *Trintec Industries, Inc v Pedre Promotional products Inc* (CAFC Jan 19, 2005)

Patent – Personal Jurisdiction

- “the ability of District residents to access the defendants’ websites . . . does not by itself show any persistent course of conduct by the defendants in the District.”
- “Some cases have suggested that the availability and use of a highly interactive, transaction-oriented website (as opposed to an “essentially passive” website) by itself may support long-arm jurisdiction wherever the site is available to potential customers for the purpose of doing business.” *Trintec Industries, Inc v Pedre Promotional products Inc* (CAFC Jan 19, 2005)

Patent – Personal Jurisdiction

“Trintec refers to the availability of Pedre products on non-Pedre websites, but those sites would support jurisdiction only if Pedre had some responsibility for the third party’s advertising of Pedre products on non-Pedre sites. See, e.g., *Jung v. Ass’n of Am. Med. Colls.*, 300 F. Supp. 2d 119, 132 n.5 (D.D.C. 2004) (distinguishing cases where personal jurisdiction is based upon defendant’s activities on its own website from situation where third party’s website was used); *GTE*, 199 F.3d at 1352 (indicating the importance of “know[ing] for certain which defendants own and operate which websites” in determining jurisdiction). Although some of the non-Pedre websites contain hyperlinks to Pedre.com, it is unclear exactly how much, if any, control Pedre has over the contents of these third-party sites.” *Trintec Industries, Inc v Pedre Promotional products Inc* (CAFC Jan 19, 2005)

Copyright – Scope and Balance

Who Pays Piper?

“This appeal raises the difficult issue of who should compensate musical composers and artists for their Canadian copyright in music downloaded in Canada from a foreign country via the Internet. In an era when it is as easy to access a website hosted by a server in Bangalore as it is to access a website with a server in Mississauga, where is the protection for the financial rights of the people who created the music in the first place? Who, if anyone, is to pay the piper?”

SOCAN v. Canadian Assn. of Internet Providers 2004 SCC 13, per Binnie J.

Importance of IP Rights

The “capacity of the Internet to disseminate ‘works of the arts and intellect’ is one of the great innovations of the information age.” “Its use should be facilitated rather than discouraged, but this should not be done unfairly at the expense of those who created the works of arts and intellect in the first place.” *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13

Importance of IP Rights

“Intellectual property laws originated in order to protect the promulgation of ideas. Copyright law provides incentives for innovators -artists, musicians, inventors, writers, performers and marketers - to create. It is designed to ensure that ideas are expressed and developed instead of remaining dormant. Individuals need to be encouraged to develop their own talents and personal expression of artistic ideas, including music. If they are robbed of the fruits of their efforts, their incentive to express their ideas in tangible form is diminished.” *BMG Canada Inc.v John Doe* 2005 FCA 193

Scope of Copyright in Collective Works

- “Once an individual work is integrated into a collective work, the owner of the copyright in the individual work cannot restrict the reproduction of the collective work...Like the author who has the copyright in the original work, the owner of the copyright in the collective work has the sole right (a) to produce or reproduce the collective work or any substantial part thereof, and (b) to do so in any material form whatever: *Copyright Act*, s. 3(1)...”
- “The central issue, therefore, is whether the electronic version of the Globe, as found in the database, constitutes a reproduction of the Globe's collective work or a substantial part thereof.”
Robertson v. Thomson Corp., 2004 CanLII 32254 (ON C.A.)

Robertson v. Thomson

“Virtually all of the original arrangement and selection of the collective work is lost in the reproduction of an isolated, stand-alone article downloaded onto a computer, and shown on its monitor, from an electronic database as the result of a keyword search. The originality of the collective work through the editors' judgment, skill and labour, is dissipated. The stand-alone article is reproduced beyond the context of any collective work. The originality contained in the display of the search result in respect of a given freelance article is that of the author of the individual work. The essence of the search result is the individual freelancer's creative work.” *Robertson v. Thomson Corp.*, 2004 CanLII 32254 (ON C.A.) per, Weiler J.A.

Robertson v. Thomson

“...when the individual articles are disentangled from the rest of the collective work they are not covered by the Globe's copyright because their arrangement or link with the collective work is lost. The selection of the articles and the changes made to an author's individual article are relatively minor and of a factual mechanical nature. These types of changes cannot grant the Globe collective copyright in the articles themselves.” *Robertson v. Thomson Corp.*, 2004 CanLII 32254 (ON C.A.) per, Weiler J.A.

Robertson v. Thomson

- “The electronic version does not cease to be the Globe, or a substantial part of it, simply because modern technology permits a search and retrieval exercise that downloads the targeted article in a stand-alone fashion for viewing on the computer screen...., the databases enable articles to be retrieved from back issues of the Globe's collective works, as selected and edited by the Globe's editors, and with reference to the edition of the Globe from which they were retrieved, the section and page of the edition in which they were found, whether they were accompanied by illustrations or not, and the name of the author. This is not "simply a grouping of [the] individual works", in my view. Nor is the collective work of the Globe lost, fragmented, submerged or overwhelmed, in this exercise. It is not the author's work that is disseminated through the database; it is the article from the Globe's collective work that is disseminated.” *Robertson v. Thomson Corp.*, 2004 CanLII 32254 (ON C.A.) per Blair J.A. in dissent
- What will the Supreme Court decide?

Liability of Internet Intermediaries

- “Parliament has decided that there is a public interest in encouraging intermediaries who make telecommunications possible to expand and improve their operations without the threat of copyright infringement. To impose copyright liability on intermediaries would obviously chill that expansion and development, as the history of caching demonstrates.”
- “It is clear that Parliament did not want copyright disputes between creators and users to be visited on the heads of the Internet intermediaries, whose continued expansion and development is considered vital to national economic growth.” *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13

Liability of Internet Intermediaries

- “Paragraph 2.4(1)(b) is not a loophole but an important element of the balance struck by the statutory copyright scheme.”
- “It was enacted with the intent of ensuring that liability would not be imposed on intermediaries who supply software and hardware to facilitate use of the Internet.”
- “It was intended to encourage intermediaries to make telecommunications possible and to prevent liability that could chill such expansion.” *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13

Liability for Authorizing Infringement

- The knowledge that someone *might* be using neutral technology to violate copyright is not necessarily sufficient to constitute authorization, which requires a demonstration that the defendant did give approval to; sanction, permit; favour, encourage the infringing conduct.
- Notice of infringing content, and a failure to respond by "taking it down" may in some circumstances lead to a finding of "authorization". *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13
- What will the US Supreme Court do in the *Grockster* case?

Liability of Foreign Content Providers

- Supreme Court held the Copyright Act could be applied extra-territorially where there is a “real and substantial connection” between the infringement and Canada making it clear that those who communicate content over the Internet, or who authorize its communication, have obligations under Canadian copyright law.
- Will the rule yield predictable results?
- Foreign content providers whose music is telecommunicated to a Canadian end user will not automatically be subject to liability.
- A content provider will not necessarily be immunized from copyright liability by virtue only of the fact it employs a host server outside the country.
- Conversely, a host server does not attract liability just because it *is* located in Canada. *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13

Liability for Downloading

“When the Motions Judge stated that, under subsection 80(1) of the *Copyright Act*, R.S. 1985, c. C-42, “downloading a song for personal use does not amount to infringement,” he gave no consideration to the possible application of subsection 80(2) and the circumstances in which the defence of “private use” will not be available, such as, *inter alia*, where the reproduction of a musical work embodied in a sound recording onto an audio recording medium is done for the sale, rental, distribution, communication by telecommunication or performance to the public.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Liability for Downloading

“The Motions Judge also did not appear to consider whether all the requirements for the application of the exemption relating to personal use contained in subsection 80(1) of the *Copyright Act* were satisfied. For example, if the users were not using an ‘audio recording medium’, the defence of private copying would not be available.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Liability for Downloading

“The Motions Judge relied upon the case of *CCH Canada Ltd. v. Law Society of Canada*, 2004 SCC 13 to say that there is no “authorization” by the users of the plaintiffs’ sound recordings in the present case, when he had at the same time said the evidence as to infringement Page: 26 was inadequate. Obviously, at the early stages of this case, it is premature to reach any conclusion as to the applicability of the *CCH* case. Nor did the Motions Judge consider whether the users’ act of copying the Songs onto their shared directory could constitute authorization because it invited and permitted other persons with Internet access to have the musical works communicated to them and be copied by them.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Liability for Downloading

“The Motions Judge similarly made findings that there had been no “distribution” within the meaning of the *Copyright Act* so as to constitute infringement. He said that to have distribution, there must be a “positive act by the owner of the shared directory”, implying that making copies “available on their shared drives” is not a positive act. It is not clear that the legislation requires a “positive act” and no authority is cited in support of his conclusion.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Liability for Downloading

“The Motions Judge found no evidence of secondary infringement contrary to subsection 27(2) of the *Copyright Act* because there was “no evidence of knowledge on the part of the infringer.” This ignores the possibility of finding infringement even without the infringer’s actual knowledge, if indeed he or she “should have known” there would be infringement.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Liability for Downloading

“Thus, the danger of making such findings at the early stages of this case can be seen. I make no such findings here and wish to make it clear that if this case proceeds further, it should be done on the basis that no findings to date on the issue of infringement have been made.” *BMG Canada Inc. v John Doe*
2005 FCA 193

Finding Downloaders

“The Motions Judge, while finding that the motion was brought pursuant to Rule 238, went on to hold that the criteria for determining whether an equitable bill of discovery should be issued, would be equally applicable to a proceeding brought under Rule 238. I agree. In my view, the plaintiffs could invoke either Rule 238 or equitable bills of discovery and in either case, the legal principles relating to equitable bills of discovery would be applicable. The same issues are at stake in both procedures and there would seem to be no reason for not applying the same legal principles.”
BMG Canada Inc. v John Doe 2005 FCA 193

Finding Downloaders

“In my view, it would make little sense to require proof of a *prima facie* case at the stage of the present proceeding. The plaintiffs do not know the identity of the persons they wish to sue, let alone the details of precisely what was done by each of them such as to actually prove infringement. Such facts would only be established after examination for discovery and trial. The plaintiffs would be effectively stripped of a remedy if the Courts were to impose upon them, at this stage, the burden of showing a *prima facie* case. It is sufficient if they show a *bona fide* claim, i.e. that they really do intend to bring an action for infringement of copyright based upon the information they obtain, and that there is no other improper purpose for seeking the identity of these persons.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Finding Downloaders

- “There should be clear evidence to the effect that the information cannot be obtained from another source such as the operators of the named websites (KaZaA, *et al*).”
- “Also if an order for disclosure were granted, consideration would have to be given to the costs incurred by the respondents in assembling the information.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Liability for Private Copying

- **Section 79 Copyright Act:**
- **"audio recording medium"** means a recording medium, regardless of its material form, onto which a sound recording may be reproduced and that is of a kind ordinarily used by individual consumers for that purpose, excluding any prescribed kind of recording medium.
- The levy is imposed on a “blank audio recording medium” which is defined as (a) an audio recording medium onto which no sounds have ever been fixed, and (b) any other prescribed audio recording medium.

Liability for Private Copying

“The Board acknowledges that, when it enacted Part VIII, Parliament could not have envisioned recent technological developments (Private Copying III, p. 38). Indeed, the legislative history of Bill C-32, which amended the Act to include Part VIII, shows that at the time, Parliament was looking at blank audio tapes as the cause of the harm to rightsholders and had been made aware of proposals in other countries (including the U.S.) to extend the levy to the hardware which recorded and played these blank audio tapes. Nevertheless, Parliament chose to limit the levy to blank medium.” *Canadian Private Copying Collective v Canadian Storage Media Alliance* 2004 FCA 424

Liability for Private Copying

“However, it seems clear that if it had, the subject matter of the sale or disposition was a digital audio recorder or a device as the Board called it, but not a medium as defined. In the absence of such a sale, no liability can arise for the levy. In my respectful view, it is for Parliament to decide whether digital audio recorders such as MP3 players are to be brought within the class of items that can be levied under Part VIII. As Part VIII now reads, there is no authority for certifying a levy on such devices or the memory embedded therein.” *Canadian Private Copying Collective v Canadian Storage Media Alliance* 2004 FCA 424

Will the Supreme Court grant leave to appeal?

Protecting TPMs

- Section 1201(a) does not “cover the circumvention of a technological measure that controls access to a work not protected under [the Copyright] title. And if we’re talking about ball point pen cartridges, printer cartridges, garage doors and so forth, we’re talking about works not protected under this title.”
- All three liability provisions of this section of the DMCA require the claimant to show that the “technological measure” at issue “controls access to a work protected under this title,” see 17 U.S.C. § 1201(a)(2)(A)–(C), which is to say a work protected under the general copyright statute, *id.* §102(a). To the extent the Toner Loading Program is not a “work protected under [the copyright statute],” ... the DMCA necessarily would not protect it. *Lexmark Int’l Inc. v Static Control Components Inc.* 72 U.S.P.Q.2d 1839 (6th.Cir.2004)

Protecting TPMs

“The DMCA does not create a new property right for copyright owners. Nor, for that matter, does it divest the public of the property rights that the Copyright Act has long granted to the public. The anti-circumvention and anti-trafficking provisions of the DMCA create new grounds of liability. A copyright owner seeking to impose liability on an accused circumventor must demonstrate a reasonable relationship between the circumvention at issue and a use relating to a property right for which the Copyright Act permits the copyright owner to withhold authorization-as well as notice that authorization was withheld. A copyright owner seeking to impose liability on an accused trafficker must demonstrate that the trafficker's device enables either copyright infringement or a prohibited circumvention...” *Chamberlain Group, Inc v Skylink Technologies, Inc.* 2004 US App. LEXIS 18513 (Fed.Cir. Aug. 31, 2004)

Copyright Enters the Public Domain

- Copyright law is no longer an arcane subject of interest only to special interest groups and key industries.
- Scope of rights, exemptions and limitations are seen as directly affecting individuals.
- There is a growing questioning about the proper scope of copyright
- Copyright reform is seen (wrongly) as a “zero sum game”.
- See, Marybeth Peters “Copyright Enters the Public Domain” April 29, 2004 Journal, Copyright Society of the USA Vol 51, No 4 Summer 2004

Scope of Public Domain

- *Kahle v Ashcroft* 72 USPQ2d 1888 (D.Cal.2004)
- Internet Archive and its chairman Brewster Kahle et al refused declaratory judgment that the Copyright Renewal Act of 1992 (“Copyright Renewal Act”), the Sonny Bono Copyright Term Extension Act (“CTEA”), the Copyright Act of 1976 (“1976 Act”), and the Berne Convention Implementation Act (“BCIA”) were unconstitutional.
- Kahle alleged that the copyright system denies public access to orphan works, without creating any countervailing benefit either to authors or the public at large.
- Because the US copyright system contains no mechanisms to create and maintain useful records of copyright ownership, people who would like to distribute or use orphaned works—digital libraries, or creators who would like to include the work in their own creative expression—often are unable to clear rights.

Scope of Public Domain

- *Luck's Music Library, Inc. v Gonzales* (D.C.Cir. May 24, 2005)
- Constitutional challenge to US amendments that protected foreign works that had fallen into the public domain by a commercial firm archive (Moviecraft) that preserves, restores and sells old footage and films.
- Argument that amendments were unconstitutional as they did not provide significant incentives for authors to create works.
- See also, *Golan v Gonzales* 2005 WL 914754 (D.Colo.April. 20, 2005) and *Eldred v Ashcroft* 537 U.S. 186 (2003)

Proposals for Copyright Reform

Need For Law reform

“In the United States, unlike Canada, detailed legislation has now been enacted to deal specifically with the liability of Internet intermediaries; see the *Digital Millennium Copyright Act* ... Australia has enacted its *Copyright Amendment (Digital Agenda) Act 2000* ... The European Commission has issued a number of directives ... Parliament's response to the [WIPO] *Copyright Treaty* ... remains to be seen. In the meantime, the courts must struggle to transpose a *Copyright Act* designed to implement the *Berne Convention*...of 1886, as revised in Berlin in 1908, and subsequent piecemeal amendments, to the information age, and to technologies undreamt of by those early legislators.” *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13

Need For Law reform

“The rapid evolution of digital network technology, notably the Internet, has compelled a re-examination of the operation of the Act. Significant improvements in speed and bandwidth in particular have permitted the Internet to become an efficient and relatively low-cost platform for creating and disseminating all types of copyright material, regardless of their size or format (e.g., software, music, film). One consequence of this development has been the advent of peer-to-peer file-sharing mechanisms which has made it possible to share copyright material at little or no cost, often without the authorization of rights holders.” *Statement, Government Statement on Proposals for Copyright Reform (March 2005)*

Everyone Wants Change

- “Though the Act has proven adaptable to changing technologies, there is uncertainty as to how some of its aspects apply in the Internet environment. Rights holders seek clarity in terms of the scope of their existing rights and the adequacy of their protection on-line. Users and intermediaries face uncertain copyright liability for some of their activities. Many of the provisions of the Act relating to educators and researchers did not contemplate uses in an Internet environment. Moreover, not all collective societies and rights holders have been able to adapt their business models to deal with the Internet and provide access efficiently and at reasonable cost.
- In these circumstances, rights holders, Internet intermediaries and users have all pressed the Government to update and clarify the copyright framework.” *Statement, Government Statement on Proposals for Copyright Reform (March 2005)*

Interested Parties Disagree on What Changes Are Required

“Copyright law is complex and contentious, more than ever now in the Internet environment. Every country around the world that has introduced or contemplated measures similar to those proposed by the Government has struggled to address the Internet challenge.”

Government of Canada, Frequently Asked Questions,
March 2005

Object of Copyright Reforms

- “Canada's Copyright Act needs to be updated and clarified to address the challenges and the opportunities of the Internet and digital technology generally.”
- “Amendments will: enhance protection of works in the on-line environment, both to address infringement and to enable the development of new business models; enable use of the Internet as a tool for learning and research; and, clarify Internet service provider (ISP) liability.”
- “The enhanced protections will be provided through the implementation of the obligations set out in two treaties that were concluded in 1996 at the World Intellectual Property Organization (the "WIPO Treaties").” *Government of Canada, Frequently Asked Questions, March 2005*

Scope of Bill

“...the Bill that will follow in a few months time, is a minimalist approach to reform, the result of political compromise driven in part by inflated and not altogether helpful rhetoric on all sides of the debate, and one which unfortunately leaves several fundamental steps and crucial discussions for future consideration.” (“Gervais “The Realignment of Canadian Copyright Law”)

Making Available Right

- “In conformity with the WCT, the existing exclusive communication right of authors would be clarified to include the making available right. In conformity with the WPPT, sound recording makers and performers would be provided the right to control the making available of their material on the Internet.”
- “...rights holders will have an exclusive right to control the making available of works and other subject matter on digital networks. This will clarify that the unauthorized posting or the peer-to-peer file-sharing of material on the Internet will constitute an infringement of copyright.”
Government of Canada FAQ
- “It will also be made clear that private copies of sound recordings cannot be uploaded or further distributed. Individuals may therefore be subject to legal action for their unauthorized file-sharing activities, but it will be up to rights holders to exercise their new rights...” *Government of Canada FAQ*

Protection for TPMs

- The circumvention, for infringing purposes, of TPMs applied to copyright material would itself be an infringement.
- The circumvention of a TPM will only be illegal if it is carried out with the objective of infringing copyright. Legitimate access, as authorized by the *Copyright Act*, will not be altered.
- Copyright would also be infringed by persons who, for infringing purposes, enable or facilitate circumvention or who, without authorization, distribute copyright material from which TPMs have been removed.
- There will be exemptions for the purposes of security testing or reverse engineering.
- It would not be legal to circumvent, without authorization, a TPM applied to a sound recording, notwithstanding the exception for private copying.”
Statement, Government Statement on Proposals for Copyright Reform
(March 2005); *Government of Canada FAQ*

Protection for Rights Management Systems

“In conformity with the WCT and WPPT, the alteration or removal of rights management information (RMI) embedded in copyright material, when done to further or conceal infringement, would itself constitute an infringement of copyright. Copyright would also be infringed by persons who, for infringing purposes, enable or facilitate alteration or removal or who, without authorization, distribute copyright material from which RMI has been altered or removed.” *Statement, Government Statement on Proposals for Copyright Reform (March 2005)*

Exemption for ISPs as Intermediaries

“ISPs would be exempt from copyright liability in relation to their activities as intermediaries, namely, their activities as mere conduits for information, their caching activities, their hosting activities, and their information location activities.” *Statement, Government Statement on Proposals for Copyright Reform (March 2005)*

Notice and Notice System

- A "notice and notice" process will be introduced. It will address P2P file sharing.
- Blocking access to material would be required only when ordered by a court.
- ISPs will be required to retain information sufficient to identify the subscribers for a fixed time period.
- For privacy reasons the disclosure of the identity of a subscriber will be by court order.
- The Government will have the power to prescribe the form that must be used in giving notices and to set fees that may be required to be paid by rights holders to ISPs for processing such notices. *Statement, Government Statement on Proposals for Copyright Reform (March 2005); Government of Canada FAQ*

Privacy

Concerns About Privacy

- “My second concern relates to privacy issues. Insofar as is possible, this Court should adopt an interpretation of s. 3(1)(f) that respects end users' privacy interests, and should eschew an interpretation that would encourage the monitoring or collection of personal data gleaned from Internet-related activity within the home.
- Locating the communication at the place of the host server addresses privacy concerns. In general, once the content provider has posted content on a host server, it is available to the public. Owners of copyrighted works and their collective societies can easily monitor such public content by trawling the publicly accessible servers with specially designed software. Privacy concerns are diminished because it is the content provider who has made the information public by posting it on the sever. Although privacy concerns are attenuated, they are not eliminated with the host server test...
- By contrast, the real and substantial connection test, insofar as it looks at the retrieval practices of end users, encourages the monitoring of an individual's surfing and downloading activities. Such habits 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. We should therefore be chary of adopting a test that may encourage such monitoring.” *SOCAN v. Canadian Assn. of Internet Providers* 2004 SCC 13 per Lebel J. (in dissent)

Concerns Over Privacy

“Citizens legitimately worry about encroachment upon their privacy rights. The potential for unwarranted intrusion into individual personal lives is now unparalleled. In an era where people perform many tasks over the Internet, it is possible to learn where one works, resides or shops, his or her financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed. This intrusion not only puts individuals at great personal risk but also subjects their views and beliefs to untenable scrutiny. Privacy advocates maintain that if privacy is to be sacrificed, there must be a strong *prima facie* case against the individuals whose names are going to be released.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Importance of Privacy

- “Privacy rights are significant and they must be protected.”
- “Where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action. However, caution must be exercised by the courts in ordering such disclosure, to make sure that privacy rights are invaded in the most minimal way.”
- “Thus the greatest care should be taken to avoid delay between the investigation and the request for information. Failure to take such care might well justify a court in refusing to make a disclosure order.” *BMG Canada Inc. v John Doe* 2005 FCA 193

Importance of Privacy

“Plaintiffs should be careful not to extract private information unrelated to copyright infringement, in their investigation. If private information irrelevant to the copyright issues is extracted, and disclosure of the user’s identity is made, the recipient of the information may then be in possession of highly confidential information about the user. If this information is unrelated to copyright infringement, this would be an unjustified intrusion into the rights of the user and might well amount to a breach of PIPEDA by the ISPs, leaving them open to prosecution. Thus in situations where the plaintiffs have failed in their investigation to limit the acquisition of information to the copyright infringement issues, a court might well be justified in declining to grant an order for disclosure of the user’s identity.” *BMG Canada Inc .v John Doe* 2005 FCA 193

Importance of Privacy

“In any event, if a disclosure order is granted, specific directions should be given as to the type of information disclosed and the manner in which it can be used. In addition, it must be said that where there exists evidence of copyright infringement, privacy concerns may be met if the court orders that the user only be identified by initials, or makes a confidentiality order.” *BMG Canada Inc. v John Doe* 2005 FCA 193

US Patriot Act's Implications for Outsourcing

- October 29, 2004 BC Privacy Commissioner release report *“Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing”*. (*“Patriot Act Report”*)
- It examined the privacy implications of the US Patriot Act for privacy compliance under BC’s *Freedom of Information and Protection of Privacy Act* R.S.B.C. 1996, c. 165 (*“FOIPPA”*).
- The report was prompted by complaints by unions concerned about the outsourcing of the BC Medical Services Plan administered under the *BC Medical Protection Act* to US-linked private sector service providers.

Effect of Permitting Data to be Located in the US

“[w]e have concluded that, if information is located outside British Columbia, it will be subject to the law that applies where it is found, regardless of the terms of an outsourcing contract. Therefore, if an outsourcing arrangement calls for personal information to be sent to the US, that information would be subject to the USA Patriot Act while in the US. The applicability of US law would not be limited to Foreign Intelligence Surveillance Act (FISA) orders for the production of “tangible things”. It would also include provisions respecting physical search orders under FISA, national security letters under various US statutes, and other laws that apply to records or information in the US.” *Patriot Act Report at p 132*

Maximus Litigation

- Issues in the case brought by the BC Gov't and Services Union:
- That the Master Services Agreement will require disclosure of personal information in circumstances that will constitute a violation of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 155 (FOIPPA), and is thus *ultra vires*;
- That the release of highly sensitive personal information pursuant to the Master Services Agreement contravenes ss. 7 and 8 of the *Canadian Charter of Rights and Freedoms*. *BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services)*, 2005 BCSC 446

Dealing with FOIPPA

- Maximus Inc. is a United States company carrying on business in the United States. Its wholly owned subsidiary in Canada is Maximus Canada Inc.
- Maximus Canada Inc.'s subsidiary is Maximus BC Health Inc. (Technical Services) which in turn has a subsidiary called Maximus BC Health Benefit Operations Inc. providing services.
- The latter three corporate entities are Canadian companies. Maximus BC Health and Maximus BC Health Benefit Operations Inc. are incorporated in the Province of British Columbia and are restricted by the Articles of Association by operating within the Province of British Columbia.
- In order to isolate those companies from Maximus Canada and Maximus Inc. (U.S.A.) the Master Services Agreement provides that the shares of Maximus BC Health Inc. will be held in trust by a trust company operating in the Province of British Columbia. The beneficial interest in those shares is to be held by Maximus Canada. The trust provision in the contract is one of the default remedies that the Province has in relation to a breach or prospective breach by Maximus.

Dealing with FOIPPA

- “Any examination of FOIPPA leads to the conclusion that the government, as previously stated, has done all within its powers to control the dissemination of information and to ensure that the receipt of information by a public body is reasonably secure in the sense that proper precautions have been made to ensure privacy and confidentiality.
- This statute applies to the two Maximus companies that operate in the Province of British Columbia and their employees. Consequently, my view of the entering into the contract in and of itself does not result in a breach of the statute as the contract in and of itself does not violate any of the statute's provisions. Consequently, I reject the submission that there is a breach of FOIPPA which may result in the Master Services Agreement being declared inoperative.” *BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services)*, 2005 BCSC 446

Charter and Patriot Act

- “I accept that in Canada there is a right to privacy encompassed by s. 7 of the *Charter*.”
- “Although the experts' evidence differs as to whether or not there is a likelihood of a U.S. *Patriot Act* application and order under s. 215 in relation to Maximus U.S. or any of its Canadian subsidiaries, and the effect of that order, in my opinion when one analyzes the contract and the legislation it is clear that parties to this arrangement have taken all reasonable steps to ensure the confidentiality of the information which Maximus will receive in order to discharge its contractual obligations. Privacy is not absolute.” *BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services)*, 2005 BCSC 446

Steps Taken to Preserve Privacy

1. The trust provisions - if a risk of disclosure occurs the Province obtains the shares and operates the system until the risk disappears.
2. Restrictions on use and control of electronic equipment and devices by employees.
3. A \$35M penalty if there is a breach of confidentiality by Maximus.
4. Whistle blowing requirements and protection, contractually and legislatively (FOIPPA).
5. Employee training in respect of their legal duties, disclosure suspected.
6. Extensive FOIPPA provisions to ensure records kept in private and kept in British Columbia.
7. Pursuant to s. 18.8 of the Master Services Agreement, all of the information remains the property of the Province.
8. The contractual provision in clause 17.8 prohibiting disclosure of provincial data.
9. Section 9.4 where Maximus expressly acknowledges and agrees that it is subject solely to the laws of British Columbia and Canada. *BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services)*, 2005 BCSC 446

Privacy R v Tessling

- Whether warrantless use of thermal imaging device violated right against unreasonable search and seizure - Canadian Charter of Rights and Freedoms, s. 8.
- Police using FLIR (Forward Looking Infra-red technology) thermal imaging device to take "heat" picture of accused's home from aircraft without warrant *R v Tessling* 2004 SCC 67

Privacy and Reasonableness of Search

“...the right to be free from examination by the state is subject to constitutionally permissible limitations. First, "not every form of examination conducted by the government will constitute a 'search' for constitutional purposes. On the contrary, only where those state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitute a 'search' within the meaning of s. 8"; ... It is only "[i]f the police activity invades a reasonable expectation of privacy, [that] the activity is a search“... Second, as the language of s. 8 implies, even those investigations that are "searches" are permissible if they are "reasonable". A search will not offend s. 8 if it is authorized by a reasonable law and carried out in a reasonable manner”. . *R v Tessling* 2004 SCC 67

Information Privacy

- “The cases have come to distinguish among a number of privacy interests protected by s. 8. These include personal privacy, territorial privacy and informational privacy.”
- “Informational privacy has been defined as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”: A. F. Westin, *Privacy and Freedom* (1970), at p. 7. Its protection is predicated on ‘the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain . . . as he sees fit.’” . *R v Tessling* 2004 SCC 67

No Per se Rule for Informational Privacy

“In my view, with respect, the reasonableness line has to be determined by looking at the information generated by *existing* FLIR technology, and then evaluating its impact on a reasonable privacy interest. If, as expected, the capability of FLIR and other technologies will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist.” *R v Tessling* 2004 SCC 67

The "Totality of the Circumstances" Test

(1) Did the Respondent Have a Reasonable Expectation of Privacy?

1. What was the subject matter of the FLIR image?
2. Did the respondent have a direct interest in the subject matter of the FLIR image?
3. Did the respondent have a *subjective* expectation of privacy in the subject matter of the FLIR image?
4. If so, was the expectation *objectively* reasonable? In this respect, regard must be had to:
 - a. the place where the alleged "search" occurred;
 - b. whether the subject matter was in public view;
 - c. whether the subject matter had been abandoned;
 - d. whether the information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
 - e. whether the police technique was intrusive in relation to the privacy interest;
 - f. whether the use of surveillance technology was itself objectively unreasonable;
 - g. whether the FLIR heat profile exposed any intimate details of the respondent's lifestyle, or information of a biographical nature. *R v Tessling* 2004 SCC 67

US Cases Not Persuasive

“The United States Supreme Court declared the use of FLIR technology to image the outside of a house to be unconstitutional in *Kyllo v. United States*, 533 U.S. 27 (2001), based largely on the "sanctity of the home" (p. 37). We do not go so far. The fact that it was the respondent's home that was imaged using FLIR technology is an important factor but it is not controlling and must be looked at in context and in particular, in this case, in relation to the nature and quality of the information made accessible by FLIR technology to the police.” *R v Tessling* 2004 SCC 67

No Protection Against FLIR Searches

“I do not regard the use of current FLIR technology as the functional equivalent of placing the police inside the home.... I do not accept that s. 8 is triggered by a FLIR image that discloses that heat sources of some unknown description are present inside the structure, or that the heat distribution is uneven. Certainly FLIR imaging generates information *about* the home but s. 8 protects people, not places. The information generated by FLIR imaging about the respondent does not touch on "a biographical core of personal information", nor does it "ten[d] to reveal intimate details of [his] lifestyle" (*Plant*, at p. 293). It shows that some of the activities in the house generate heat. That is not enough to get the respondent over the constitutional threshold.” *R v Tessling* 2004 SCC 67

No Protection Against FLIR Searches

“External patterns of heat distribution on the external surfaces of a house is not information in which the respondent had a reasonable expectation of privacy. The heat distribution, as stated, offers no insight into his private life, and reveals nothing of his "biographical core of personal information". Its disclosure scarcely affects the "dignity, integrity and autonomy" of the person whose house is subject of the FLIR image (*Plant*, at p. 293).” . *R v Tessling* 2004 SCC 67

E-Commerce Issues

Dealing with Spam

- “During the past year, the Task Force has come to appreciate that spam is much more than a mere nuisance. Spam is increasingly associated with activities that are intended to mislead and deceive, to violate privacy, to make unauthorized use of consumer or business equipment, to cause harm to computers or networks, to commit fraud or to steal personal information.
- During this same period, spam and these other kinds of threats have begun to spread from Internet email to instant messaging and wireless communication services.” *Stopping Spam: Creating a Stronger, Safer Internet*, Industry Canada May 2005

Dealing with Spam

“The federal government should establish in law a clear set of rules to prohibit spam and other emerging threats to the safety and security of the Internet...by enacting new legislation and amending existing legislation as required.”

Stopping Spam: Creating a Stronger, Safer Internet,
Industry Canada May 2005

Dealing with Spam

- To this end, the following email activities and practices should be made offences in spam-specific legislation:
- the failure to abide by an opt-in regime for sending unsolicited commercial email;
- the use of false or misleading headers or subject lines (i.e. false transmission information) designed to disguise the origins, purpose or contents of an email, whether the objective is to mislead recipients or to evade technological filters;
- the construction of false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit other offences listed);
- the harvesting of email addresses without consent, as well as the supply, use or acquisition of such lists; and
- dictionary attacks. *Stopping Spam: Creating a Stronger, Safer Internet*, Industry Canada May 2005

Consumer Protection

- Ontario implements Internet Template through regulations to the *Consumer Protection Act 2002*, *Effective July 2005*
- *See esp. Sections 31-33 O.Reg. 17/05*

Does UECA Legislation Oust Common Law?

“Having looked at the provisions of the ETA, I agree with the submissions made by SMI. Whilst the statute does make it plain that electronic records will be adequate to satisfy legal rules relating to writing and signature in most commercial matters, its conservative approach in not extending these provisions to contractual matters falling within s 6 of the CLA does not mean that, as a matter of law, electronic means of communication cannot satisfy the requirements of s 6. The ETA does not change the common law position in relation to s 6 of the CLA. Whether an e-mail can satisfy the requirements for writing and signature found in that provision will be decided by construing s 6(d) of the CLA itself and not by blindly relying on s 4(1)(d) of the ETA.” *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*, [2005] SGHC 58

Does E-Mail Constitute a Writing?

“I therefore find that the e-mail correspondence which constituted the memorandum of the contract (as specified in [73] above) was “in writing” for the purpose of s 6(d) of the CLA. I am pleased to be able to come to this conclusion which I think is dictated by both justice and common sense since so much business is now negotiated by electronic means rather than by letters written on paper and, in the future, the proportion of business done electronically will only increase. I think that the ordinary man in the street, who not only conducts business via computer but who is being encouraged to use technology in all areas of life and to become more and more technologically proficient, would be amazed to find that the law would not recognise a contract he had made electronically even though all the terms of the contract had been agreed and the parties were perfectly *ad idem*. If parties who negotiate electronically do not wish to be bound until a formal document is signed, they can have recourse to the “subject to contract” endorsement that can easily be added to their e-mail correspondence”. *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*, [2005] SGHC 58

Signature Requirements in E-mails

- “I am satisfied that the common law does not require handwritten signatures for the purpose of satisfying the signature requirements of s 6(d) of the CLA. A typewritten or printed form is sufficient. In my view, no real distinction can be drawn between a typewritten form and a signature that has been typed onto an e-mail and forwarded with the e-mail to the intended recipient of that message.
- One minor difficulty in this case is that Mr Tan did not append his name at the bottom of any of his e-mail messages. All his e-mail messages, however, including the message dated 4 February 2003 and sent to Ms Yong, had, near the start thereof, a line reading “**From:** “Tan Tian Tye” <tian-tye.tan @schenker.com>”. Mr Tan confirmed in court that he had sent out those messages. There is no doubt that at the time he sent them out, he intended the recipients of the various messages to know that they had come from him. Despite that, he did not find it necessary to identify himself as the sender by appending his name at the end of any of the e-mails whether the messages were sent to his colleagues or to third parties like Mr Heng. I can only infer that his omission to type in his name was due to his knowledge that his name appeared at the head of every message next to his e-mail address so clearly that there could be no doubt that he was intended to be identified as the sender of such message. Therefore, I hold that the signature requirement of s 6(d) is satisfied by the inscription of Mr Tan’s name next to his e-mail address at the top of the e-mail of 4 February 2003.” *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*, [2005] SGHC 58

Signature Requirements in E-mails

“I recognise that one person’s e-mail facility can, in some cases, be accessed by a third party who can then send out messages which purport to be authentic messages from the owner of that e-mail address. If that happened, the owner of the address would be entitled to dispute the authenticity of the messages purportedly sent by him. That is not the case here. Further, such dispute would be as to the person who initiated the message and would not be decided on the basis of whether the message bore a signature.” *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*, [2005] SGHC 58

Enforceability of Web Wrap Agreements

- At issue was the validity of an exclusive arbitration clause added to the contract between the parties by Paysystems by posting it on its website.
- The original contract was amended on October 23, 2003 (adding an exclusive arbitration clause) by Paysystems which added the following notice to the opening screen of the site:
 - Your continued use of my Paysystems Services is subject to the current version of the My Paysystems Agreement.
 - This agreement was last updated December 18, 2003.
 - Please [click here](#) to review.
 - *Aspencer1.com Inc. v. Paysystems Corporation*, 500-22-101613-043, 31 January 2005, Court of Quebec

Enforceability of Web Wrap Agreements Against Automated Agents

“Cairo argues that forum selection clauses must be reasonably communicated for a party to be bound by its terms, seeking support from *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2dCir. 2002)... Unlike the circumstances in *Specht*, Cairo admits to actual knowledge of CMS’s Terms as of at least “the day before CMS sent its letter threatening legal action on November 1, 2004.”...Moreover, Cairo’s repeated and automated use of CMS’s web pages can form the basis of imputing knowledge to Cairo of the terms on which CMS’s services were offered even before Cairo’s notice of CMS’s cease and desist letter. See *Register.com*, 356 F.3d at 401-02 (imputing knowledge of web site’s terms of use to repeated user of *Register.com*’s database). Thus, even accepting Cairo’s allegation that it did not explicitly agree to CMS’s Terms of Use, the Court finds that Cairo’s use of CMS’s web site under circumstances in which Cairo had actual or imputed knowledge of CMS’s terms effectively binds Cairo to CMS’s Terms of Use and the forum selection clause therein.” *Cairo, Inc. v Crossmedia Services, Inc.* (N.D.Cal. Apr. 1, 2005)

Enforcement of Standard Web Contracts in Europe

- Court finding following changes not enforceable:
- AOL's unilateral right to modify the agreement, even though the right was subjected to 30 days' notice to the subscriber, and even though the subscriber could terminate the agreement within that period;
- tacit, rather than explicit, acceptance of the subscriber to changes in the payment terms;
- AOL's right to unilaterally terminate the agreement in the event of "risk" of non-payment;
- The cap of AOL's liability equal to the last six months of fees;
- The right of AOL to invoice reasonable attorney's fees in the event of a subscriber's breach;
- The requirement that the subscriber constantly update his or her personal data, failing which the agreement is automatically terminated without notice;
- The right of AOL to transmit the subscribers' personal data to third parties without prior consent;
- Tacit, rather than explicit, acceptance of general terms by the subscriber;

Enforcement of Standard Web Contracts in Europe

- The right of AOL to terminate the contract at its convenience;
- The requirement that the subscriber pay fees for the remaining term of a definite term agreement if the subscriber chooses to terminate early;
- The right of AOL to suspend or terminate the agreement without prior notice for minor breaches;
- The right of AOL to add 15 seconds to each invoiced connection;
- Exoneration of AOL from all liability for service interruptions and errors, as well as many other events;
- Limitation of AOL's liability for the replacement of a defective CD-ROM;
- A statement that termination of the agreement is the subscriber's sole remedy in the event of AOL's breach; and
- Presumption of acceptance of notice sent by email two days after their delivery. This was deemed too short a time period. *AOL Bertelsmann Online France v. UFC Que Choisir et autres*, *Cour de Cassation*, 3/904), Summarized in 10 ELRA 350.

What is a Document?

- 233. (1) On motion, the Court may order the production of any document that is in the possession of a person who is not a party to the action, if the document is relevant and its production could be compelled at trial.
- “The information sought by the plaintiffs may be buried in logs and tapes but is not presently in a readable format. Since the documents in a readable format do not currently exist and would have to be created, Rule 233 has no application. The Rule contemplates the production of documents which are “in the possession of a person”. It cannot be said that documents which do not exist are in the possession of a person.”
BMG Canada Inc. v John Doe 2005 FCA 193
- Should the rule be amended to deem any document that does not exist but can be produced from a machine readable record to be a document?
See, *Correctional Service of Canada v Yeager* 2003 FCA 30 (interpreting S4(3) of the *Access to Information Act*).

Admissibility of Internet Evidence

- “On the view which I take of the merits of the appeal with respect to the counterclaim, there is evidence to support the trial judge's position without having to rely upon the evidence taken from the internet. As a result, anything which I might say about the admissibility of this evidence would be unnecessary to the decision in the appeal. I might add that, in my view, the record is not sufficiently developed to provide an adequate factual underpinning for an informed consideration of the legal issues raised by the use of the internet as a source of documentary evidence.
- In light of this, is it preferable to leave the issues surrounding the admissibility of evidence originating on the internet to be dealt with at a time when the record is more fully developed and the issue is necessary to the outcome of the appeal. Given that I choose not to address these issues, it follows that I take no position on the trial judge's approach to the question of internet evidence.” *WIC TV Amalco Inc. v. ITV Technologies, Inc.*, 2005 FCA 96
- Will the Supreme Court grant leave to decide the issue?

Admissibility of Computer Records

- Appeal arises out of a ruling concerning the admissibility of banking documents upon which the Crown relied to support its case against the appellant who was convicted of fraud-related charges.
- The outsourcing of some of the functions by Symcor for bank with respect to maintaining records of cheque transactions raises questions about the admissibility of prints of cheques made from microphotographic film or microfiche that is neither made by nor kept in a bank.
- The question is whether prints of cheques made from microfiche were admissible in evidence under either s. 29 or s. 31 of the *Canada Evidence Act*.
- If not, the further question is whether, in the circumstances, the prints were admissible on some other basis. *R. v. Lemay*, 2004 BCCA 604

Admissibility of Computer Records

- Print-outs not admissible under Section 31 of Canada Evidence Act.
- Section 31- cheques were admissible for all purposes that the original cheques photographed would have been admissible on proof that, (i) *while the cheques were in the custody or control of the Bank*, (ii) photographic film was taken (iii) to keep permanent records, and (iv) *the cheques were destroyed in the presence of a bank employee, or were lost, or delivered to the society. R. v. Lemay, 2004 BCCA 604*

Admissibility of Computer Records

- Print-outs not admissible under Section 29 of Canada Evidence Act.
- Section 29- the entries shown on the prints of the cheques the Crown tendered were admissible as *prima facie* proof of the entries and of the transactions recorded if (i) the entries shown on the cheques in the prints were true copies of entries, (ii) *made in the ordinary course of the Bank's business*, (iii) *in records kept in a bank*, (iv) that at the time the entries were made, (v) *were one of the Bank's ordinary records*, (vi) *in its custody or control*. *R. v. Lemay*, 2004 BCCA 604

Admissibility of Computer Records

- “The principled approach to the admission of hearsay evidence is now well established through a line of cases decided by the Supreme Court of Canada...:
- In those cases, the court developed an approach that recognizes hearsay as being substantively admissible for the truth of its content when it is both necessary and sufficiently reliable as those considerations may be assessed in the circumstances of any given case.” *R. v. Lemay*, 2004 BCCA 604

Admissibility of Computer Records

“Whether the microfiche record is sufficiently reliable to have been admitted to prove the transactions recorded is a question of whether, in the circumstances, there were sufficient guarantees of trustworthiness to meet what the authorities recognize as the threshold of admissibility... Threshold reliability of hearsay evidence which is determinative of admissibility, as opposed to the ultimate reliability of the evidence or the truth of the contents, is seen to have two aspects to be assessed: whether the circumstances tend to negate inaccuracy and fabrication and whether the circumstances provide the trier of fact with a satisfactory basis for evaluating the truth about the facts to be proven.” *R. v. Lemay*, 2004 BCCA 604

Admissibility of Computer Records

“The reliability of the microfiche record appears to me to be largely beyond question on both counts. The circumstances are such that there is no basis to question the accuracy of a record that consists of microphotographs of cheques made by Symcor for the Bank. The clearing and recording function that Symcor performs is a matter of the ordinary course of daily business that the Bank has engaged it to perform. There can be no suggestion of any motive Symcor could have to falsify the record of cheque transactions it keeps for the Bank.” *R. v. Lemay*, 2004 BCCA 604

Admissibility of Computer Records

“Further, the circumstances provide the trier of fact with a sound basis for evaluating the truth about the transactions recorded. The circumstantial guarantees of trustworthiness are compelling, so much so that it is difficult to envision any real danger associated with hearsay evidence in a microphotographic record of cheques that can be seen to have been negotiated and cleared. The uncontroverted evidence is that all cheques negotiated at the Bank are, in the normal course of the Bank's business, sent to Symcor to be cleared and recorded on microfiche. The microfiche record is the Bank's permanent record of cheque transactions and the record must accordingly be accepted as completely reliable by the Bank, by its customers, and by those who audit and regulate its business.” *R. v. Lemay*, 2004 BCCA 604

Toronto Computer Lawyers Group: A Year in Review

Barry B. Sookman
May 31, 2005

The right people. The right results.™

McCarthy
Tétrault

mccarthy.ca

Vancouver

Pacific Centre,
Suite 1300, 777 Dunsmuir Street
P.O. Box 10424
Vancouver BC V7Y 1K2
Tel: 604.643.7100
Fax: 604.643.7900

Calgary

Suite 3300, 421 - 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403.260.3500
Fax: 403.260.3501

London

One London Place
Suite 2000, 255 Queens Avenue
London ON N6A 5R8
Tel: 519.660.3587
Fax: 519.660.3599

Toronto

Toronto Dominion Bank Tower
Suite 4700, Box 48
Toronto ON M5K 1E6
Tel: 416.362.1812
Fax: 416.868.0673

Ottawa

The Chambers
Suite 1400, 40 Elgin Street
Ottawa ON K1P 5K6
Tel: 613.238.2000
Fax: 613.563.9386

Montréal

Le Windsor
1170, rue Peel,
Montréal QC H3B 4S8
Tel: 514.397.4100
Fax: 514.875.6246

Québec

Le Complexe St-Amable
1150, rue de Claire-Fontaine, 7e étage
Québec QC G1R 5G4
Tel: 418.521-3000
Fax: 418.521.3099

New York

25th Floor, One New York Plaza
New York NY 10004-1980
USA
Tel: 212.785.6410
Fax: 212.785.6438

United Kingdom & Europe

5 Old Bailey, 2nd floor
London EC4M 7BA
England
Tel: +44 (0)20 7489 5700
Fax: +44 (0)20 7489 5777

mccarthy.ca

McCarthy
Tétrault