l'Association canadienne du droit
des technologies de l'information

May 26, 2005

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Anne Uteck and Teresa Scassa of the Law and Technology Institute of Dalhousie Law School.

Les auteurs du présent bulletin sont les professeurs Anne Uteck et Teresa Scassa de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie.

Criminal Law

In *R. v. Missions* 2005 NSCA 82 (not yet available online) the Nova Scotia Court of Appeal considered an appeal from a conviction for possession of child pornography. The appellant argued that the trial judge had erred on a number of grounds which included a failure to accord sufficient weight to the testimony of an expert witness regarding the possibility that the illicit files had been downloaded in error and without the knowledge of the accused, and that the judged had relied entirely upon circumstantial evidence to infer that the accused had knowledge of the existence of the materials. The computer and zip drives in question were accessible to a number of other people besides the accused.

The court ruled that the trial judge did give sufficient weight to the evidence of the expert witness, and found that it was reasonable in the circumstances to conclude that the accused had not accidentally downloaded 64 separate images and stored them in four separate locations. Roscoe J.A. noted that "[t]he normal inference that one intends the natural consequences of one's actions is applicable to computer usage just as it is to any other human activity…" (at para 21). She noted that the storage of the images on four separate disks, the file structure of the disks, and the titles of the images all supported a conclusion that the activities resulting in the storage of the material were intentional. Roscoe J.A. also found that the trial judge's conclusions that it was the accused who had downloaded the images and not any of the others who had access to the computer were reasonable.

Freedom Of Expression

In *R. v. Bryan*, the majority of the B.C. Court of Appeal overturned a lower court decision which had found that s. 329 of the *Canada Elections Act*, which prohibited the publication or communication of election results from one electoral district before the closing of all polling stations in other electoral districts, violated s. 2(*b*) of the *Charter* and could not be saved under s. 1. As a result of the lower court decision the conviction of Paul Bryan for disseminating electoral results over the Internet had been overturned. The majority of the court of Appeal restored the conviction.

Rowles J. noted that it was clear that s. 329 infringed the freedom of expression. However, she found that, based on the reasoning of the Supreme Court of Canada in *Harper v. Canada (Attorney General)*, the evidence put before the trial judge was sufficient to find the limitation justified under s. 1 of the *Charter.* Although the respondent had argued, inter alia, that the publication ban had been rendered obsolete by advances in communications technology, Rowles J. took the view that "difficulty in enforcement of the publication ban is irrelevant to the constitutional question." (at para 64). Saunders J. in dissent disagreed on this point, noting that modern technology has created two classes of Canadians: those who can get around the publication ban, and those who cannot. She wrote: "In my view, the information differential between those with "a way around the provision" and those reliant on the common media, is a secondary deleterious effect of s. 329, in the context of the current voting scheme." (at para 105).

Intellectual Property/Privacy

The Federal Court of Appeal has released its much awaited decision in *BMG Canada Inc. v. John Doe*. The case arose as an application for an order to compel Internet Service Providers to disclose the identities of a number of users who were allegedly

involved in a significant volume of music file-sharing over the Internet. The motions judge had refused to grant the order, and in doing so, had made a number of statements about copyright law that suggested the file sharing activities were legal.

The Federal Court of Appeal upheld the decision below with respect to the denial of the order. However, its decision was largely confined to issues relating to the sufficiency of the factual information presented in support of the application.

Sexton J.A. for the unanimous court set the decision in the context of the competing interests in protecting copyright works and in maintaining citizen privacy. He stated that "the issue is whether the identity of persons who are alleged to infringe musical copyright can be revealed despite the fact that their right to privacy may be violated." (at para 5)

The Court of Appeal found that there was no palpable and overriding error by the Motions Judge with respect to Rule 233 which permits a court to "order the production of any document that is in the possession of a person…". The Court of Appeal agreed that the information sought by the applicants in this case did not exist as a "document" that was in any person's possession. The information might exist, but was stored in a range of computer logs and tapes. Further, the Court accepted the ruling of the motions judge that the applicants had failed to comply with Rule 81, which required affidavits to be "confined to facts within the personal knowledge of the deponent". In this case, the Court accepted that "[m]uch of the crucial evidence submitted by the plaintiffs was hearsay". (at para 21) Sexton J.A. expressed the concern that the hearsay evidence suggesting a link between particular pseudonyms and IP addresses created "the risk that innocent persons might have their privacy invaded and also be named as defendants where it is not warranted." (at para 21).

The Court of Appeal took the view that where the issue was the identity of the persons who were infringing the plaintiffs' copyrights, rule 238 was "broad enough to permit discovery in cases such as this." (at para 25), and that other rules could permit substituted service or no service at all in appropriate circumstances. Further, Sexton J.A. noted that "a court could, in cases such as the present, limit the discover to the submission of written questions which could be followed by written answers, limited to revealing only the identity of the users complained of, or such other limitations as the court might consider necessary". (at para 26). Sexton J.A. also noted that an equitable bill of discovery was available in circumstances such as those in this case. He disagreed with the Motions Judge that the plaintiff would have to provide evidence of a prima facie case. Instead, Sexton J.A. ruled that the proper test is "whether the plaintiff has a bona fide claim against the proposed defendant." (at para 32) In this case, this would involve an indication "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." (at para 34). In addition, there would have to be "clear evidence to the effect that the information cannot be otained from another source such as the operators of the named websites (KaZaA, et al)." (at para 35) and that "consideration would have to be given to the costs incurred by the respondents in assembling the information." (at para 35).

On the issue of privacy, Sexton J.A. noted that such rights "are significant and they must be protected" (at para 38), and that the "delicate balance between privacy interests and public interest has always been a concern of the court where confidential information is sought to be revealed". (at para 39) In striking the balance in this case, Sexton J.A. noted that intellectual property laws are "designed to ensure that ideas are expressed and developed instead of remaining dormant." (at para 40). In the context of the Internet, he notes that "[t]his 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 be that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights." (at para 41) Thus, where there is a bona fide claim that unknown persons are infringing copyright, the balance lies towards disclosure, as long as any invasion of privacy is kept to a minimum. Sexton J.A. noted that because delays in requesting information about identities may increase the likelihood of error, any such delays "might well justify a court in refusing to make a disclosure order." (at para 43).

The Federal Court of Appeal chided the motions judge for the comments he made with respect to copyright law, noting that such conclusions about the law should not have been made at such an early stage in the proceedings. Sexton J.A. noted in particular that although the motions judge made reference to s. 80(1) of the *Copyright Act* as legitimating the downloading of songs, he "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." (at para 50) Sexton J.A. also noted that the motions judge failed to 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." (at para 51) He also noted that the motions judge seemed to suggest a requirement for a "positive act" in order to find that there had been a distribution of the works under the *Copyright Act*, where such a positive act is not clearly required by the legislation. Finally, Sexton J.A. also noted the insufficiency of the analysis given to the possibility of "secondary infringement." Although the Court of Appeal made no findings with respect to the law on these issues, they also made it clear that the findings of the judge below should not have been made, and should not be considered in any further litigation on the issue.

Privacy

The federal Privacy Commissioner has released two new findings under *PIPEDA*. Finding #298 involved a store employee disclosing a customer telephone number to a third party. Although the company had appropriate practices in place to protect its customers' personal information, the Assistant Privacy Commissioner held that the employee had inappropriately disclosed the complainant's personal information without her consent contrary to Principle 4.3 and thus concluded that the complaint was well-founded. In Finding #299, the Assistant Privacy Commissioner dealt with a complaint arising from a third party fraudulently cashing a convenience cheque in his name. She goes on to find the bank in contravention of Principles 4.6 for failing to record accurate information and Principle 4.7.1 in not providing adequate safeguards to protect personal information. Of note, another issue raised during the investigation related to the bank's telephone interactive voice response system. However, the Assistant Privacy Commissioner was satisfied that the bank had appropriate measures in place to protect account information with respect to its telephone verification procedures.

The Alberta Information and Privacy Commissioner released Investigation Report P2005-IR-004 involving the use of video cameras in the workplace. The complainant, a former employee, claimed that R.J. Hoffman Holdings Ltd. (Hoffmans), an organization operating oilfield maintenance services, was in violation of the *Personal Information Protection Act (PIPA)* by improperly collecting personal information without his consent through the use of video surveillance cameras. The complainant alleged that the Hoffmans managers had intercepted a private verbal communication between him and another employee which was then used as grounds for his dismissal from the company.

Video surveillance cameras were installed throughout Hoffmans' two locations. There was no audio, zoom or pan capability on any of the cameras. The cameras only recorded when movement was detected. Videotape was stored for one month and then automatically erased. Footage could be viewed via the Internet, by entering a password unique to the organization and then observing the images on a computer. The Operations Manager is the only employee with access to the password or the video feed. The reasons cited by Hoffmans for using video surveillance were safety, security, loss prevention and employee performance management.

Since the cameras did not have audio capacity and thus no capacity to collect private communication, the complaint of improper collection of the individual's private communication was not a breach of *PIPA* because there was no collection of the private communication. Notwithstanding, according to the AIPC "the complaint raises important issues regarding the reasonableness of collection of other information about indentifiable individuals (images) through the use of video surveillance for the purpose of managing the employment relationship." Accordingly, three questions were addressed.

1. Does this collection involve "personal information" or "personal employee information" under the *Act*? If an individual in the frame can be identified then the captured image is "information about an identifiable individual" as defined under s.1(k). It was clear, according to the AIPC, that the individuals being recorded were in fact identifiable and thus the information collected constituted information about an identifiable individual and therefore within the broad category of personal information under the *Act*. Regarding personal employee information, under s.1(j), if an organization reasonably requires certain personal information, and the sole purpose for collecting the personal information is to establish, manage or terminate the employment relationship, then the information is personal employee information. The AIPC was satisfied that Hoffmans was collecting the personal information as prescribed by section 1(j) and therefore, *PIPA* applied.

2. Was the collection reasonably required for the organization's purposes of establishing, managing or terminating the employment relationship in accordance with ss. 15 and 18 of the *Act*? The Investigation Report canvasses Alberta and British Columbia arbitral jurisprudence relating to video surveillance as well as *PIPEDA* decisions on the issue of video surveillance in the workplace. Consistent with the analysis and principles being developed by arbitrators and the Canadian Privacy Commissioner, the AIPC concludes that the collection and use of personal employee information through the cameras is "reasonably required" and "reasonable" for the purposes of safety, security and loss prevention, but the collection and use of personal employee information through the cameras is not "reasonably required" or "reasonable" for the purpose of employee performance management.

3. Did the organization provide adequate notice that the personal information was going to be collected and the purposes for which the personal information was going to be used? The investigation report indicates that the nature and extent Hoffmans had notified their employees about the purposes for the surveillance cameras remained unclear. However, the AIPC finds that Hoffmans failed to give adequate notification as required under s.15(2)(c) because the organization should "explicitly notify employees about the cameras and their purposes" preferably in writing or through a posting in a conspicuous location on the premises.

Professional Responsibility

In *National Bank Financial Ltd. v. Potter* 2005 NSSC 113 (not yet available online) the Nova Scotia Supreme Court ordered counsel for one of the parties to be removed as a result of their access to and use of privileged emails belonging to other parties. The case is a complex one, arising from the collapse of Knowledge House Inc. (NHI), a high tech company. Essentially, National Bank Financial Ltd. (NBFL) alleged that certain defendants in the case engaged in a stock manipulation scheme leading up to the company's collapse.

Scanlan J. noted that as a high tech company, much of the communication at KHI was conducted by email. The company's servers contained a large volume of email messages which included many communications between KHI and its lawyers. After the collapse of KHI, the company's assets, including its computer equipment and servers were sold as part of the bankruptcy proceedings. A contract to remove data from the servers was not carried out, and the server came into the possession of NBFL. The defendants brought an application to strike NBFL's statement of claim, stay the proceedings, and remove counsel for NBFL as a result of the wrongful access of counsel for NBFL to the privileged communications.

Scanlan J. noted that the defendants "were not reckless in terms of their actions in relation to securing the KHI servers." (at para 20). In particular, each email account was protected by password, and the servers were securely stored. Access to the emails on the servers only became possible after what Scanlan J. found to be duplicitous actions on the part of the company to which the servers had been entrusted.

Scanlan J. took the view that NBFL was actually concerned about whether they were legitimately in possession of the contents of the servers. They sought legal advice from their counsel on this issue. In this regard, Scanlan J. noted that "[i]t is perhaps an understatement to say the evidence suggests almost all of the solicitors involved in these proceedings were largely computer illiterate" (at para 24). Scanlan J. was harshly critical of the lawyers for the manner in which they dealt with the issue. He notes that they did no legal research on the subject and comments: "I am reminded of a circle of friends all pointing fingers at the next person. The circle never ends. I am convinced the circle should have stopped at each and every one involved. They all had an opportunity to do the right thing and none of them did." (at para 25).

Scanlan J. made a number of comments about the nature of email. He compared email accounts to personal diaries, and stated that "at a bare minimum one would expect they would include confidential or private information." (at para 30) Beyond that he found that the lawyers for NBFL specifically searched for communications between one of the defendants and his lawyers, and found that "the lawyers involved should reasonably have expected to find privileged communications on the server." (at para 30). He noted that he found it hard to understand the argument of one of the lawyers that the issue of privilege did not occur to him because he was of the view that there was no legal advice being sought or given in the emails, given that the email headers included: "Re: need for legal advice" or "Re: wise counsel required". (at para 34).

Scanlan J. rejected arguments that the defendants' emails lost their privilege when they were stored on KHI's server. Counsel for NBFL relied on cases involving employee emails stored on employers servers, and the fact that it has been found that there is no reasonable expectation of privacy in such a context. Scanlan J. noted that these documents were more than private, they were privileged. Further, he took the view that to argue that emails lost their privilege if stored on company servers would mean that all email communications from lawyers to their clients would lose their privileged status if stored on law firm servers. He stated: "When it comes to privileged communications, a server is akin to a filing cabinet. Whether that cabinet is at work, home, or in a lawyer's office, it is the nature of the document which affords the special protection, not where the filing cabinet is located." (at para 96). Scanlan J. also rejected the argument that there was a waiver of privilege once the server was sold.

Scanlan J. also dealt with issues relating to other private but non-privileged email communications stored on the servers. Counsel for NBFL had copied entire email directories and provided them to other lawyers and regulatory investigators. Scanlan J. noted that "[c]onfidential documents do not have the same protection as privileged documents. That however does not mean they are subject to a free for all in court proceedings." (at para 131) Although he found that it was not up to the holders of the email accounts to determine what was relevant, only relevant (and non-privileged) emails should be reproduced and distributed. He ruled: "When citizens communicate on business matters or private affairs they should expect that others will not disseminate them in the context of litigation unless they are relevant to the proceedings. The threat of dissemination of private correspondence under the veil of litigation would dampen the enthusiasm of many litigants….To think that irrelevant information could be in any way used as a lever in forcing a party to capitulate or somehow to be influenced by the threat of release of private information would result in an unfair advantage." (at para 132).

In the end result he ordered removal of counsel for NBFL and the striking of any reference to pleadings based on solicitor-client privilege. He declined to order a stay or make a finding of abuse of process.

Spam

Canada's National Task Force on Spam has released its Final Report. The Report, "Stopping Spam: Creating a Stronger, Safer Internet" identifies the need for a "multi-faceted, multi-stakeholder approach" to effectively fight spam. The Report makes a number of recommendations, including proposed legislation to prohibit spam and to safeguard personal information and privacy as well as computers, e-mail and networks. The offences are supported by rigorous penalties. The proposed law would allow individuals and corporations to sue spammers and hold the businesses whose products or services are being promoted through

spam accountable. As well, the Report calls for more resources to appropriate agencies for the purposes of administering and enforcing anti-spam legislation. Other key recommendations include a centre of expertise on spam to oversee the coordination of all the spam initiatives, support law enforcement and receive complaints; ISPs, network operators and e-mail marketers voluntarily adopt the industry best practices developed by the Task Force; Task Force partners continue to enhance the Stop Spam Here website content for the purposes of public education; and because most spam reaching Canadians comes from outside the country, the Task Force recommends that the government continue its efforts to harmonize anti-spam policies and to improve cooperation in enforcing anti-spam laws internationally. Minister of Industry David Emerson congratulated the members of the Task Force on Spam commenting that if Canada is going to "reap the full benefit of a strong e-economy" it must "rid the Internet of the scourge of spam." In his view, "these recommendations merit strong consideration."

This newsletter is intended to keep members of IT.Can informed about Canadian legal developments as well as about international developments that may have an impact on Canada. It will also be a vehicle for the Executive and Board of Directors of the Association to keep you informed of Association news such as upcoming conferences.

If you have comments or suggestions about this newsletter, please contact Professors Anne Uteck and Teresa Scassa at it.law@dal.ca.

Disclaimer: The IT.Can Newsletter is intended to provide readers with notice of certain new developments and issues of legal significance. It is not intended to be a complete statement of the law, nor is it intended to provide legal advice. No person should act or rely upon the information in the IT.Can Newsletter without seeking specific legal advice.

Le présent bulletin se veut un outil d'information à l'intention des membres d'IT.Can qui souhaitent être renseignés sur les développements du droit canadien et du droit international qui pourraient avoir une incidence sur le Canada. Le comité exécutif et le conseil d'administration de l'Association s'en serviront également pour vous tenir au courant des nouvelles concernant l'Association, telles que les conférences à venir.

Pour tous commentaires ou toutes suggestions concernant le présent bulletin, veuillez communiquer avec les professeurs Anne Uteck et Teresa Scassa à l'adresse suivante : it.law@dal.ca

Avertissement : Le Bulletin IT.Can vise à informer les lecteurs au sujet de récents développements et de certaines questions à portée juridique. Il ne se veut pas un exposé complet de la loi et n'est pas destiné à donner des conseils juridiques. Nul ne devrait donner suite ou se fier aux renseignements figurant dans le Bulletin IT.Can sans avoir consulté au préalable un conseiller juridique.