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

February 3, 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.

Contracts

In *Logix Data Products Inc. v. Ace Rivet and Fastener Inc.*, [2005] O.J. No. 244, Fragomeni J. of the Ontario Superior Court of Justice considered a claim by the plaintiff for unpaid invoices amounting to just over thirteen thousand dollars. The defendant argued that the plaintiff sold it a computer program that it "knew or ought to have known would be of no use to Ace and that it made serious misrepresentations about the capabilities of the program" (at para 1) so as to induce the defendant to purchase the program. In a decision that turned largely on Fragomeni J.'s assessment of the evidence and credibility of the witnesses, he ruled in favour of the defendant that there were misrepresentations as to the capabilities of the software that was sold.

Criminal Law

In *United States v. Ruggeberg*, the accused was being held in British Columbia for his alleged criminal conduct in Texas under a Detention Order made pursuant to the provisions of the Canadian *Extradition Act*. The British Columbia Supreme Court had concluded that the Detention Order was necessary to ensure Ruggeberg's attendance in Court. Ruggeberg sought review of the Detention Order and release from custody. The Court held that he had shown a material change in circumstances and cause as to why his continued detention was not justified or necessary to ensure his attendance in court. Of particular interest, one of the conditions attached to Ruggeberg's release was that he was required to wear an electronic monitoring device. According to the Court, since this technology is now available in British Columbia, Ruggeberg can be electronically monitored "so that his unexplained or unapproved absence from his Vancouver address will be immediately known."

The Ministry of Public Safety and Emergency Preparedness recently announced two cyber security initiatives. First, Canada is the first signatory to an agreement with Microsoft's Security Corporation Program, a global initiative aimed at reducing the risk of cyber threats that potentially impact shared critical infrastructures. Second, the Canada Cyber Incident Response Centre (CCIRC) has been established as a centralized point to deal with cyber threats. Also, several senior federal Ministers and the RCMP participated recently in the launch of Cybertip.ca, a tipline for reporting online child pornography.

Language

In *Procureur Général du Québec c. Produits Métalliques C.M.P. Ltée*, the Cour du Québec ruled that the defendant company was guilty of violating arts. 52 and 143 of the Charter of the French Language by virtue of having created a web site that was in English only. The defendant was also cited for several other violations of the language law, including not having provided French language versions of software and other computer materials that were used in the business.

The defendant explained that its delays in its francisation program were largely due to the fact that Nortel was a major client, and that Nortel's decline in fortunes had had a significant impact on the defendant's company. The Court noted that the offences were strict liability offences to which only a defence of due diligence was available. While it acknowledged that the defendant company had suffered a period of significant difficulty between 2001 and 2004, it nonetheless did not justify the lack of response by the company, in the period between 1994 to 2001, to repeated notices from the Office de la langue française regarding its francisation program.

The court noted that this lack of action for a 7 year period could not support a defence of due diligence.

Privacy

In a recent OPC Finding, it was ruled that requiring bank customers to declare citizenship was not a violation of *PIPEDA*. The case involved a number of account holders of a bank who complained they were asked to indicate whether they were American citizens. The bank was a subsidiary of a U.S.-based holding company and classified as a "controlled foreign corporation" for the purposes of the U.S. income tax law. As such, it was required to comply with the IRS regulations with respect to information reporting for American citizens. The request by the bank to the account holders outlined the purpose for collecting the information and how it would be used. If an account holder did not declare themselves as a non-resident of the United States, it is presumed they are a U.S. citizen and the bank would disclose the personal information of the account holder. The Assistant Privacy Commissioner concluded that the complaint was not well-founded because the bank met the reasonableness standard under s.5(3) and complied with Principles 4.2 and 4.4 by identifying the purposes for which the information was being collected and the collection of personal information was limited to the specified purposes. While it did not form part of the complaint, the Assistant Commissioner did go on to express concern with respect to the bank's disclosure of personal information. If a customer did not fill out the declaration and thus was presumed to be a U.S. citizen, the bank would disclose personal information to the IRS without the consent of the customer. This, in the Assistant Commissioner's view, would contravene Principle 4.3 which requires that the knowledge and consent be obtained for the collection, use and disclosure of personal information. It was, therefore, recommended that the bank review its disclosure policy to ensure it is in compliance with *PIPEDA*.

The Working Party On The Protection of Individuals With Regard to the Processing of Personal Data, an independent European Advisory body on data protection and privacy, has released its Opinion addressing the level of protection ensured in Canada for the transmission of Passenger Name Record (PNR) and Advance Passenger Information (API) from airlines. It concludes that Canada has an adequate level of protection pursuant to the European Privacy Directive on the protection of individuals regarding the processing of API and PNR transferred from airlines to the Canada Border Services Agency concerning any person arriving in Canada.

An Ontario health care facility contacted the Information and Privacy Commissioner concerning its obligations under the new *Personal Health Information Protection Act* (*PHIPA*) after there had been an inadvertent disclosure of patients' person health information occurring when a nurse at the facility posted photographs on a personal website. The photographs of employees of the facility showed the names of five patients behind a nursing station and some contained photographs of the patients. Under the *Act*, where personal health information is accessed by unauthorized persons, the health information custodians are required to notify the individuals involved. The IPC and health care facility decided against notification for several reasons, including, it was unclear how many third parties actually accessed the website, the health care facility was not identified on the website so there would be no way of linking the patients to the particular facility, and it was unlikely the patients had been harmed in any way by the disclosure. In order to fulfill the requirements under *PHIPA*, the health care facility agreed to place a note in the patient's file regarding the disclosure and the patients would be informed personally by their health care providers.

In Bothwell v. Ontario (Minister of Transportation), [2005] O.J. No. 189, the applicant Bothwell sought judicial review of the decision of the Ministry of Transportation to deny his requested exemption from the requirement to have a photograph on his driver's licence. His request for an exemption was argued on religious grounds. While he had in past years consented to a Polaroid photograph being used, his objection was to the taking of a digital photograph. The Court summarized his position as follows: "[the applicant] believes that the taking of a digital photograph of the face and having that image entered in the drivers licence database is the causing of one to deliver an

exact copy or express image from the face which is referred to in Revelations Chapter 13, and that its effect is to mark the person whose picture is taken for the Anti-Christ." (at para 20) The Court accepted the respondent's position that the applicant did not meet the burden of establishing that "a sincere religious belief prevents him from submitting to the requirements of a driver's licence photo." (at para 13) On cross examination, the applicant admitted to owning a computer and using email, but indicated he had no religious objection to email or the internet. The applicant also had his own website, on which there appeared various digital photos, including a photograph of his daughter. The applicant had raised concerns about privacy, suggesting that digital photo information might be shared by government departments, and perhaps transmitted globally. Ultimately, the Court concluded that his real concerns were privacy concerns and not religious ones.

Securities Law

In *Hogan v. B.C. (Securities Commission)* the B.C. Court of Appeal considered an appeal from the administrative penalty imposed on the appellant by the B.C. Securities Commission. The appellant had been found to have used the Internet "to disseminate misrepresentations about five companies and conduct blatant and highly effective manipulations of the markets for their shares." (at para 5) The Court applied a reasonableness standard to the decision of the Commission. The appellant argued that the amount of the penalty was high in relation to penalties assessed in other cases of stock manipulation. The Commission took the view that the penalty was appropriate "given the ease with which Mr. Hogan perpetrated his scheme through the Internet, and the serious ramifications conduct of this kind would have on the public if not dealt with by a significant financial penalty." (at para 12) The Court of Appeal declined to find that the penalty was unreasonable.

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.

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