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

December 14, 2006

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Teresa Scassa, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School.

Les auteurs du présent bulletin sont les professeurs Teresa Scassa, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie.

Breathalyzer – Use of Statutory Presumption

The New Brunswick Court of Appeal has reviewed the circumstances in which the statutory presumptions about blood alcohol level can be relied upon by the Crown, in *R. v. Searle*. The police were sent to the scene of a motor vehicle accident at 2:07 a.m., and found a collision between a Ford Taurus and a Mazda 323. The officer was informed that Searle was the driver of the Mazda, and formed the opinion that Searle had driven while his ability to do so was impaired by alcohol. He made a breathalyzer demand and took the accused to a nearby police station for the breathalyzer test. After the accused had consulted with counsel the officer administered the test, but the breathalyzer machine malfunctioned and would not print the result. The officer then took the accused to a different police station, taking two samples there. These latter two samples were taken at 3:55 a.m. and 4:15 a.m..

The central issue on appeal was the requirement in s. 254(3) of the Criminal Code that, in order to make a breathalyzer demand, on officer must believe on reasonable grounds that the person has committed the relevant offence "within the preceding three hours". This condition does not require the Crown to prove that the offence actually occurred within that time: it requires the Crown to prove that the police officer making the demand subjectively believed the offence occurred within that time, and that there were objective grounds making that belief reasonable. If that requirement was not met then the demand was not lawfully made. If the demand was not lawfully made then the presumption in s. 258(1)(c) that the breathalyzer showed the accused's actual blood alcohol level could not be relied upon.

In this case the Court of Appeal held that the courts below had reasoned incorrectly from the evidence on this point. There was evidence from which it could be inferred that the accident had occurred within the previous three hours. However, that evidence did not automatically make it a natural inference that the officer subjectively believed that fact. The Court held at paras 16-17: "It might be that the officer made the demand because he felt that Mr. Searle had been driving while impaired within the last three hours but it may also be that the officer simply did not address his mind to the time element. Crown Counsel did not ask the critical question… A court cannot infer in a vacuum what was in the mind of the police officer. In some cases there may be indicia that the officer actually turned his mind to the time issue but, in this case, there is no evidence that the officer turned his mind to the question".

As a result, the court held, the presumption that the breathalyzer results were correct could not be relied upon, and there was no other evidence of the accused's blood alcohol level. The court therefore overturned the conviction on the charge of driving with a blood alcohol level of over .08%, but returned the matter to the trial judge to now determine the charge of driving while impaired.

Domain Names

In *Black & Decker Corporation v. J. Chapnik Trust*, sole panelist Stefan Martin considered a dispute over the domain name blackanddecker.ca. The dispute proceeded without participation from the registrant.

The complainant is the owner in Canada of a series of registered trade marks incorporating the words "Black & Decker". These registrations substantially predate the registration of the domain name. The panel found that the domain name blackanddecker.ca was identical, and therefore confusingly similar, to the registered marks, apparently dismissing any possible significance of the use of "and" in the name

as opposed to the ampersand ("&") used in the registered trade-marks.

Martin also found that the registrant had no legitimate interest in the domain name. He noted that the domain name had never been used in connection with any wares, services or business. Instead, it was ""parked" at a customized Internet portal in order for the Registrant to benefit from Internet traffic and become eligible for a referral fee." (at para 37) Martin noted that there was no evidence to suggest that a legitimate interest existed under any of the other grounds listed in art. 3.6 of the CDRP.

Martin found that the domain name had been registered in bad faith. He noted that the domain name was "parked" for the purpose of obtaining referral fees, and that the site linked to the name contained links to competitors of the complainant. It also "provided means by which end users could conduct searches and access links to competitors of the Complainant." (at para 43) He noted that the registration of the domain name "has prevented the Complainant from registering the ".ca" domain name for its trade-marks". Martin accepted the complainant's evidence that the conduct of the registrant in this case was part of a pattern of activity. The complainant had provided evidence of at least 6 other domain names registered by the registrant which corresponded to trade-marks owned by others. He ordered the transfer of the disputed domain name to the complainant.

Internet Luring – Sentencing

A 42 year old tax assessor from Winnipeg was sentenced to 15 months imprisonment followed by three years probation for having committed the offence of internet luring in *R. v. Horeczy*. The accused, James Glenn Horeczy, contacted the victims, all girls in their early to mid teens, through internet chat rooms. He had pressed each of them to meet with him to engage in sexual activities, and actually met with two of the girls, though nothing of consequence happened at these meetings. Unusually, the accused had at one point been warned by police not to engage in such activities but continued to do so.

In sentencing the accused, the court noted that internet luring was a type of offence that called for a denunciatory and deterrent sentence, rather than one emphasizing any of the other principles of sentencing. The judge noted that internet access through home computers had made it possible for sexual predators to in effect gain entrance into the privacy of the home through fibre optic cable where they would have been barred entry had they showed up at the door. Although parents are warned to be vigilant about children's computer use, the judge noted that parental supervision can only go so far in monitoring the online activities of a child.

The accused would have received an 18 month sentence were it not for a strict curfew he had been subject to since the time of his arrest. In addition, he was sentenced to three years probation following his release from prison. That probation included terms that he not be involved in any chat room sessions or other real-time internet connections, not possess any computer software designed to eliminate evidence of internet activity, and that he not delete any record of internet activity including recently accessed documents, internet history files, temporary internet folders and cookie files. He was also not to use any computer system other than one owned and regularly monitored by his employer, and was required to allow police or probation officers access to his residence as they request to confirm that he does not possess any computer system at home.

Obstruction of Peace Officer – Blogger as Member of Media

The Provincial Court of New Brunswick has recognized a blogger who was attending the Atlantica Conference at the Saint John Trade and Convention Center to report on it for his website as a person "plying his trade" and therefore having the same status as other members of the media.

The decision in *R. v. LeBlanc* arose in the context of a prosecution for wilfully obstructing a peace officer in the execution of duty. The Atlantica Conference had delegates from the Atlantic provinces of Canada and the New England States. Anticipating protestors, the police had cordoned off areas of the Convention Center, and only delegates wearing nametags were permitted into the roped off area. At a certain point, however, a group of approximately 30 protestors gained entrance to the building through a back entrance, and in the ensuing crush the poles and

ropes separating off an area fell to the ground. The three police officers on the scene called for assistance, with the result that virtually every officer in the city soon arrived, and the situation was brought under control.

After the situation had largely been brought under control, the accused was in the area that had formerly been cordoned off, though the trial judge found that he was not in any way associated with the protestors. Rather, the judge said, he was there with his digital camera, taking pictures of the scene with the intention of posting them on his website. The alleged obstruction was that the accused willfully refused to leave when the police officer told him to do so. The arresting officer testified that the accused was behind him, moving toward him and posing a threat with his camera, and also that he refused a direct order from Sergeant Parks to leave the area.

The trial judge found that the charge was not made out. Video footage had captured the accused's arrest, and from viewing it the trial judge concluded that the accused had not been behind the officer, but off to his right some distance and not moving towards the officer. In fact he was down on one knee taking pictures with his digital camera. The video showed the officer going directly to the accused, pushing him against a wall and pinning him there. There was no sign from the video tape that the conversation the officer purported to have, telling the accused to leave, had ever occurred. Nor was there any evidence of the accused resisting arrest, despite the officer's testimony to that effect.

Rather, the trial judge noted: "For all intents and purposes, Mr. LeBlanc was ostensibly in an area accessible to, and in fact, open to the public when he was taking his photographs. Members of the so called mainstream media were taking photographs and filming in the same area without interference from the police. I believe it's fair to say that the defendant was doing nothing wrong at the time he was approached by Sergeant Parks and placed under arrest. He was simply plying his trade……gathering photographs and information for his blog along side other reporters." The judge had earlier noted that the accused was well-known for his blog, and that the police had made use of information obtained from it to gather intelligence about the potential for protest during the Atlantica conference.

The trial judge also considered the relevance of the accused's occupation: "It may well be asked if Mr. LeBlanc's chosen occupation as a blogger had any bearing on my decision in this case. The answer to that is yes and no. The fact that the defendant was a blogger explained why he was at the Trade and Convention Center taking pictures, while a riot was going on. It could also explain why he was on a first name basis with some of the delegates. It would explain why he was so upset at being arrested, as he obviously considered himself to be a legitimate member of the media who had done nothing wrong." The judge carried on to note, though that even members of "mainstream news organization would be obligated to follow the instructions of a police officer, again provided the officer was acting within the scope of his authority."

Given the conflicts in evidence between the police officer's testimony and the videotape, the trial judge acquitted the accused.

Privacy & Data Security

The Office of the Alberta Privacy Commissioner has issued a *Report of an Investigation Concerning a Stolen Laptop Computer*. A mental health therapist who worked for Calgary Health Region's Collaborative Mental Health Program (the Program) had had a laptop computer stolen from her home. The computer had been taken home for the purposes of work, and her house was locked at the time of the break-in. She immediately reported the theft, but the laptop was never recovered. The laptop contained a database which included 1094 patient records. The patients were all under 6 years of age, and the information stored in the database was fairly detailed and of a confidential nature.

The investigator noted that it was the practice of the Program to provide its workers with laptop computers so that they can work while away from the office. This is necessary because of the high volume of work done away from the office. The issues he specifically considered in his investigation were whether any health information was collected, used or disclosed in contravention of s. 58(1) of Alberta's *Health Information Act*, and whether the work had failed to safeguard the information in contravention of s. 60 of that Act.

Section 58(1) of the Act requires that the collection, use or disclosure of health information must be limited to an amount "that is essential to enable the custodian…to carry out the intended purpose." In this case, the workers typically would upload the entire patient database onto their laptops, would add their field notes to the laptop, and would update the database on return to the office. The database contained the records of current and past patients. While acknowledging that in some circumstances, reference to the older case files might be necessary, for the most part, "the therapists' need to view files other than those associated with their current caseload is the exception, rather than the rule. There is no general need to view the entire database while in the field." (at para 18) He noted that the database had been configured in such a way that it was difficult to download only a portion of the records. He concluded that "[i]n establishing a business process where the entire database was downloaded by workers…the custodian failed to meet its duty to use health information in a limited manner, contravening HIA section 58(1)." (at para 21)

In considering the issue of the Calgary Health Region's responsibility to safeguard information, the investigator divided his analysis into two parts. He considered first whether the CHR had adequately identified the risks associated with using laptop computers. He then assessed the safeguards that had been put in place.

He noted that s. 60 required data custodians to protect against "reasonably anticipated" risks. In his view, this would require a risk assessment to be carried out. The investigator noted that risk assessments are features "found in all information security best practice guidelines and standards." (at para 26) He found that while the CHR conducted risk assessments regarding the use of laptops in other business areas, it had not carried out a risk assessment for this Program. In his view, a Privacy Impact Assessment would have revealed the risk to the data, and could have led to the implementation of measures (such as encryption) which would have mitigated the risks of using laptops in this manner. He noted that since the theft of this computer, the CHR had introduced the use of Virtual Private Network technology which allowed for secure remote access to the central database, thus eliminating the need to download data onto laptop computers.

The investigator noted that some security measures had already been in place, and he assessed their sufficiency. He noted that since the risk of theft of laptop computers was high special measures were required. The CHR had a set of Laptop Security Practices in place, and the investigator found these practices to be sound. However, in this case, the amount of data on the laptop computer was more than was necessary. The locking cable attached to the laptop computer had not been in use when it was stolen, and the CHR's policy was not explicit about the need to use the locking cable, even in the worker's own home. He noted as well that the two passwords securing access to the database did not meet CHR's password standards. The CHR's policy on data encryption had also not been implemented in this case. With respect to these encryption policies, the investigator noted:

> Rather than systematically implementing encryption in areas of high risk, CHR's policy points users to a website that offers free encryption software for download. In my view, it is not reasonable to count on non-technical employees to determine whether they need encryption software, download it, configure it and use it properly. For a large organization such as CHR, cryptographic controls should be implemented at the enterprise level based on a risk analysis and should be centrally managed and supported. (at para 41)

Overall, the investigator found that while CHR's policies "reflect a "defense in depth" strategy, their implementation does not." (at para 43) He noted that "if the security measures outlined in policy had been implemented, I would likely have concluded that they were reasonable, but in this case I cannot." (at para 43)

The investigator found that risks to individuals posed by the theft could not be ruled out, and, particularly given the sensitivity of the information, it was appropriate to notify the affected individuals. The investigator expressed satisfaction with the cooperation of the CHR, with the steps taken to deal with the breach, and with the steps taken to address security issues on an ongoing basis. The report

concludes with a set of general recommendations regarding the use of mobile computing technology in the health sector.

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 Teresa Scassa, Chidi Oguamanam and Stephen Coughlan 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 Teresa Scassa, Chidi Oguamanam et Stephen Coughlan 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.