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

September 8, 2005

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

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

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

Criminal Law

R v. T.S.R. (Alberta Court of Appeal): The Accused, T.S.R. pled guilty to three counts of possession of stolen property under $5000; two counts of possession of housebreaking instruments; one count of break and enter into a dwelling house to commit indictable offence and one count of assault causing bodily harm. A DNA order which is now appealed was made in respect of the last charge and pursuant to s. 487.051(1)(a) of the Criminal Code. This offence occurred while the accused (appellant) was on release on other charges and while on probation for unrelated offences. The appellant was 16 years old at the time of sentencing and at the time the DNA order was granted. He expressed remorse for the offence and voiced concern over the impact the DNA order would have on his life.

The Court held that the substantive test for ordering DNA samples is the same for both adults and young offenders but its application defers in the case of young offenders. According to the Court, pursuant to section 487.051(1)(2) of the *Criminal Code*, "the balancing of factors for young persons is an exercise that must be undertaken in the light of the goals sought to be achieved under the *Young Offenders Act* or the *Youth Criminal Justice Act*" (para 10). The Court noted that the Youth Criminal Justice Act did not provide for the removal and destruction of information in convicted young offender's index and his/her bodily substances at the time of destruction of his/her record. However, the predecessor legislation, the *Young Offender's Act*, so provided. Thus, the appellants' case was that because of this anomaly his privacy and security interests are by far placed out of balance with public interest in the protection of society under the *Criminal Code*. The Court held that the disparity in the provisions of the *Youth Criminal Act* and *Young Offenders Act* was a manifest case of legislative oversight. Even though this omission appears to be plugged in Bill C-13 (First Session, Thirty-eight Parliament, 53 Elizabeth II, 2004), the Court is still in a position to directly rectify it in so far as the intention of the legislature is quite clear. It also noted that pursuant to section 21 of the Bill "when the young person's youth record is destroyed so is his DNA" and as such, the appellant will not be adversely affected (para.14). It held, while dismissing the appeal, that the circumstances of the case clearly supported the making of the DNA order.

Computer Law

Bryan v. Janikowska (Alberta Provincial Court): The Plaintiff and the Defendant entered into an elaborate agreement for the sale of the plaintiff's Calgary-based business, "Spy City", including its miscellaneous inventory, notably: product lists; customers and supply lists; sales and marketing surveys; files; spread sheets; computers; office furniture; goodwill and trademark. Spy City was in the business of selling "spy stuff" which included surveillance equipment, cameras, VCR's optical equipment, night vision binoculars and monocular, bullet proof vests, etc." The parties agreed to a purchase price of $55,000 payable by installments, details of which were specified in the agreement. The Defendant declined to pay the last installments of $10,000 for reasons of Plaintiff's alleged breaches of the contract. In the Plaintiff's suit to recover the outstanding amount, the Defendant counterclaimed against the plaintiff for the sum of $14,133 on several grounds. Of particular interest is the inclusion of a Point-Of-Sale software system by the Plaintiff in the transaction. The system was offered to the Defendant "as is" with the option for the latter to sign any required contract for back-up technology if it so desired (para. 36). This offer, which the Defendant accepted, included a Risk "After Closing Clause" to the effect that upon completion of the deal, assets and inventory items will be at

purchaser's sole risk. Shortly after the Plaintiff had familiarized the Defendant with the operations of the point of sale software, the system crashed. The Plaintiff refused to take responsibility for the crashed software which was one of the bases for the Defendant's counterclaim.

On this point, the Court held that "Ownership of a computer does not constitute entitlement to use the software loaded onto the computer … There is no evidence of assignable warranty by the software provider, let alone by the licensee, which the plaintiff was likely not. Some software is sold "as is" without a warranty of any kind. To expect the Plaintiff to warrant software which might have not been warranted by the software provider would be unfair in circumstances where its lawyer alerts the Purchaser's solicitors to the need to enter into a contract with the software [sic] supplied for software support" (para 45).

E-mail and Evidence

Stewart v Knoll North America Corp. (British Columbia Supreme Court): The Plaintiff was terminated from the Defendant's employment without cause and the issue arose as to what would have been the length of appropriate notice given regard to the peculiar nature of the relationship between the parties. The Defendant claimed to have made an offer to settle which was capable of mitigating the Plaintiff's claims for special costs. Plaintiff counsel sought to explore the entire history of pre-trial motions before the jury in order to support the claim that the Defendant deliberately frustrated the plaintiff from proving her case that the termination was for a wrongful cause and thereby justified an independent action for punitive damages. The Court, per Humphries J., declined to sanction this approach but instead allowed questioning the conduct of the Defendant on the search for documents and document disclosure to enable the Plaintiffs to argue that "the jury should draw an adverse inference against the defendant as to unfairness or bad faith in the manner of dismissal" (para. 27). The Plaintiff later sought to have the Defendant's statement of defence struck out because of false affidavit and large scale concealment or non-disclosure of documents containing their relationship with the Plaintiff. The Court dismissed the motion to strike out but noted that "there were indeed problems with the defendant's document production. There was evidence before the jury that e-mails, automatically deleted after 90 days, had not been retained even though the action was started within 90 days of dismissal" (para. 29).

The Court, however, declined to find that there was massive non-disclosure of documents which if rectified would facilitate the proof of "allegations of wrongful doings by the defendant surrounding the plaintiff's dismissal" (para 40). The Court held that in order to find a reprehensible conduct in regard to "failure to produce documents, it must be useful to be able to assess if such documents were relevant to an issue before the court" (id.) The Court declined to draw the inference that the Defendant's conduct was deserving of rebuke through special costs.

Labour Law

University of Alberta Non-Academic Staff Assn. (NASA) v. University of Alberta (Alberta Labour Relations Board). Some NASA members applied for but failed to obtain posted positions. Through NASA, they sought to question the interview and selection process. To determine if there was sustainable basis for their members' grievances, NASA requested relevant information from the Governors of U of A, the employers, but did not receive all it wanted. Relying on the Freedom of Information and Protection of Privacy Act (FOIPP), the employers declined to provide some information specifically requested by NASA. The Board declined NASA's request to, *inter alia*, declare that there has been a violation of the Collective Agreement and for an order on the employers to provide the requested information forthwith.

According to it, "the matters at issue before the Board do not raise issue of statutory proportions. It is first necessary that an arbitrator determine the effect, if any, FOIPP may have upon the Employers' obligation to make disclosure under clause 38.01(b) [of the Collective Agreement] and, in particular provide NASA copies of the documents it has requested" (para.15). The present dispute and the means for its resolution is covered by the Collective Agreement hence the Board's interference at this stage would be premature.

Privacy

A recent Report issued by the Alberta Information and Privacy Commissioner involved a complaint against SAS Institute (Canada) Inc. (SAS) alleging personal information was collected in contravention of the *Personal Information Protection Act* (PIPA). The complainant had unsuccessfully applied for a position as an Administrative Assistant/Receptionist with SAS. She was required to consent to a credit check when she applied for the position and subsequently complained that the organization's collection of her personal credit information was not reasonable under the circumstances and expressed concern about the security of her personal information held by BackCheck, the organization contracted by SAS to conduct background checks. The organization stated that its purposes for collecting the complainant's personal credit information included: (1) to assess the applicant's suitability to manage petty cash; (2) to minimize credit card fraud; and (3) to validate employment history. The Investigator agreed that the organization may have legitimate interests in collecting personal credit information about potential employees for these purposes in some circumstances. However, in this case, the collection of personal credit information was not reasonably required to determine the complainant's suitability to manage petty cash; was not reasonably required to minimize the potential for corporate credit card fraud; and collecting a credit report that may contain significant amounts of unrelated personal information to verify employment history is "an unreasonable collection of extensive personal information." According to the Investigator, the complainant "was applying for employment, not a credit card." Under s.11 of PIPA, personal information may only be collected for purposes that are reasonable and to the extent that is reasonable for meeting the purposes for which the information is collected. In the Investigator's view, the amount and type of information collected in these circumstances was "over and above the extent reasonable for meeting its purposes." As well, the organization had more effective and less intrusive means to achieve its purposes.

With respect to the issue of security of the complainant's personal information, the Investigator considered the issue of personal information being held by BackCheck and maintained in files or databases in the United States. Based on the information provided by SAS and BackCheck's privacy policy, the Investigator was satisfied that SAS had implemented reasonable measures to ensure personal information collected on its behalf by BackCheck is safeguarded as required under s.34 of PIPA.

Several recommendations were made in the Report. First, that SAS review the responsibilities of the position when hiring to ensure the collection of personal credit information is reasonably required. Second, if the information is reasonably required, revise the consent form to clearly state all of the purposes for the collection. Third, job postings and advertisements should clearly state that credit checks may be required of successful candidates. Finally, in accordance with an earlier Investigation Report, SAS make clear to potential employees that providing Social Insurance Numbers is optional.

The Privacy Commissioner of Canada has released Finding #311 involving a private investigator hired by an insurance company videotaping and recording the complainant's activities. The complaint alleged that personal information was collected without her knowledge and consent in violation of Principle 4.3 of PIPEDA. The complainant had filed a lawsuit after a motor vehicle accident. According to the insurance company representing the other driver, her testimony at the discovery hearing and her medical reports revealed discrepancies and inconsistencies with respect to the injuries claimed. The private investigator, hired by the insurance company to record and observe the complainant on a day-to-day basis, followed the woman for three weeks, conducting surveillance at her home, work and shopping. The private investigator prepared a report detailing the surveillance and this information, including the videotape was used in court. Consistent with the decision in *Ferenczy v. MCI Medical Clinics* (2004) 70 O.R. (3d) 277, the Assistant Privacy Commissioner agreed that when an individual commences a lawsuit, there is an implied consent that the other party to the action may collect information required to defend itself against the suit. Thus, when the woman commenced the action and when discrepancies and inconsistencies arose with respect to the injuries being claimed, in the Assistant Privacy Commissioner's view, the complainant gave

her implied consent to the collection of her personal information. She concluded that the complaint was not well-founded. However, according to the Assistant Privacy Commissioner, implied consent has limitations. Implied consent "does not authorize unlimited or uncontrolled access to an individual's personal information, but only to the extent it is relevant to the merits of the case and the conduct of the defense." In this case, the collection of the complainant's personal information was limited to what was necessary for the other party to the action to defend itself in the suit.

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, Teresa Scassa and Chidi Oguamanam 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, Teresa Scassa et Chidi Oguamanam à l'adresse suivante : it.law@dal.ca