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

October 28, 2004

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

The Annual Report on the Use of Electronic Surveillance 2003 has been released by the Minster of Public Safety and Emergency Preparedness. Under Part VI of the *Criminal Code*, procedures are set out for law enforcement to obtain judicial authorization to conduct surveillance of private communications to assist in criminal investigations. The Report addresses the use of electronic surveillance by law enforcement.

Employment

In *Mediamix Marketing Group Inc. v. Whalen* the defendant's employer claimed that the plaintiff had infringed its e-mail and internet policy by transmitting a list of the company's clients to her home computer two days before her employment at the company ended, and the defendant left to join a competitor company. Dawson J. of the Ontario Superior Court rejected the claim based on the internet use policy, noting that the policy prohibited sending Mediamix data to third parties, and did not capture the transmission to the employee's home computer. He also noted that the plaintiff had not established that the defendant, who had worked primarily in a clerical position, was in a fiduciary relationship.

The defendant had signed a non-competition clause with a term of one year from the termination of her employment with the plaintiff company. Dawson J. observed that "the business they are involved in is fiercely competitive and that there is no customer loyalty". (at para 5) As a consequence information about customer identity and contact information could hardly be considered confidential information. In the circumstances, he found that the non-competition clause would unduly limit the defendant's ability to work in the industry. The requested injunction was denied.

Evidence

In *Mazur v. Corr*, [2004] ABQB 752 (not yet available online) a family law dispute, Lee J. of the Alberta Court of Queen's Bench noted that, in the civil context, there were "few restrictions on the admissibility of recorded conversations even if they constitute eavesdropping." (at para 12) Lee J. went on to note that technology has largely overtaken previous legal provisions requiring the taping of phone conversations to be known by the person being recorded.

Jurisdiction

In *Lewis v. King*, the English Court of Appeal dealt with libel claims relating to material posted on a website. The server where the material was stored was located in California. While it was accepted that a libel had occurred, the main question for the court was an issue of *forum conveniens*. The claimant, Don King is a U.S. citizen and resident. The first defendant, Lennox Lewis is a British citizen principally resident in New York. The second defendant, Lewis' promotion company, is based in Nevada, and the third defendant, a lawyer who acts for Lewis and the promotion company, is based in New York. At the time of the appeal, the actions against Lewis and the promotion company had been settled, leaving only the action against the New York lawyer, Burstein.

The Court of Appeal noted that the starting point in the analysis is to determine where the tort has been committed. Since the web postings had been accessed in England, the alleged defamation could be said to have occurred in the U.K. However, the Court also noted that the more tenuous the connection between the claimant and the jurisdiction, the less important the first consideration becomes. The

Court also considered the special circumstances of internet defamation, and the importance in such cases of considering "the global picture" (at para 28). Stopping short of creating a "free for all" for libel claimants, the Court nonetheless noted that "a global publisher should not be too fastidious as to the part of the globe where he is made a libel defendant." (at para 31). The Court also noted that "in an Internet case the court's discretion will tend to be more open-textured than otherwise; for that is the means by which the court may give effect to the publisher's choice of a global medium." (para 31)

The Court rejected out of hand an argument that the court should opt for the jurisdiction to which the defendant has targeted its publications. In the Internet context, the court reasoned, the defendant "has "targeted" every jurisdiction where his text may be downloaded." (para 34) The Court concluded that in allowing the action to proceed in the U.K., the judge below had followed the appropriate approach of taking an overall view of the appropriate forum.

Privacy

The most recent federal Privacy Commissioner *PIPEDA* decision involves a company's use of biometrics for authentication purposes. In Finding #281, employees complained that the company was forcing them to consent to the collection of their voice print for the purpose of accessing business applications used for logging work-related information and for absence reporting. Security, efficiency and cost-effectiveness were the reasons provided by the company for implementing the system. While the employees expressed concern that the system could be used to spy on them, the voice print could not be used for one-to-many authentication or to identify an employee other than when she logs onto the system. The complainants further objected to being prompted to provide a reason for calling in sick.

On the first issue, the Assistant Privacy Commissioner was satisfied that the purposes for which the business applications with its voice password technology were introduced met the reasonableness standard under s.5(3), namely security, efficiency and cost. She agreed that a voice print was "an encroachment upon the person" because the employer was collecting unique behavioral and physical characteristics. However, on balance, the voice print, in and of itself, and in these circumstances, did not reveal much personal information; the use solely for one-to-one authentication purposes "was fairly benign"; and the voice print was not "unduly invasive." According to the Assistant Commissioner, the Company had communicated its purposes to employees and put appropriate safeguards in place, thus complying with Principles 4.2 and 4.7. Further, she found the company to have met the consent requirements under Principle 4.3 because the purposes for the voice password were reasonable, had been explained to the employees and "an alternative concurrent system would not ensure the desired level of security." Therefore, the Assistant Privacy Commissioner concluded that the complaint relating to the collection of personal information by the use of biometric technology was not well-founded.

On the issue of the absence-reporting application, the Assistant Commissioner found that the system should not be prompting employees to provide the medical reason for their absence. In her view, this was excessive and not necessary for the purposes identified and thus, contrary to Principle 4.4. However, given the company's agreement to amend this application, this portion of the complaint was resolved.

The Ontario government has enacted the *Health Information Protection Act* taking effect November 1, 2004. Aimed at keeping personal health information of patients private, confidential and secure, the new health privacy law imposes rules relating to the collection, use and disclosure of personal health information

Spam

Anti-spam legislation has been reintroduced in the Senate. Bill S-15 gives the Minister of Industry the authority to establish an Internet Consumer Protection Council responsible for setting standards for its members and procedures aimed at reducing spam. The proposed Bill creates a "no-spam list" and makes it an offence to send spam to a person whose address is on the list. Wherever a message is initiated, if it is received by a person in Canada, the proposed

legislation deems it to have been sent to that person and the act of sending it is deemed to have been carried out in Canada. Bill S-15 provides stronger penalties for messages that involve pornography, explicit sexual activity, attempted fraud and that target children as receivers. It also establishes a civil cause of action for sending excessive spam.

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.