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

July 27, 2006 / 27 juillet 2006

IT.Can NEWSLETTER/BULLETIN

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.

INTERNET – POSTING OF HATE SPEECH

The Federal Court has sentenced Tomasz Winnicki to nine months in jail for contempt of court, after he failed to comply with a court order requiring him to stop posting hate speech on the internet. A complaint had initially been brought against Winnicki to the Canadian Human Rights Commission in September 2003, claiming that he was discriminating on the basis of religion by communicating messages on Vanguard News Network (described by the trial judge as "a sort of right wing, neo-Nazi chat room") that would likely expose persons of the Jewish faith to hatred and/or contempt. A hearing was commenced in August of 2005, and an interlocutory injunction preventing Winnicki from posting similar messages was issued on October 4, 2005. The Canadian Human Rights Tribunal (CHRT) rendered its decision in that matter on April 13, 2006. Winnicki had continued to post messages to the internet prior to the Tribunal's decision, and so the issue in this case was whether he was in contempt of court for the postings during the period between October 4, 2005 and April 13, 2006. The Court found that he was, and that a nine month sentence was the appropriate disposition.

To be convicted of contempt, the court held, it would need to be shown that Winnicki knew of the existence of the court order, and that he breached it. The question of knowledge was found easily proven. The accused had been self-represented at most stages of the proceedings, including at the hearing at which the interim injunction had been granted, and he had been mailed a copy of the decision. Further, the actual messages that formed the subject matter of the contempt charge made reference to the court order, so there was no real basis to doubt that Winnicki knew of the injunction.

The messages posted during the period of the injunction were very similar to those which were the subject of the initial CHRT hearing, alleging the existence of a Zionist conspiracy, that Jews dominate all levels of government, and that multiculturalism was a policy conceived by Zionists to perpetuate non-white immigration. The messages were also extremely derogatory of Blacks and all non-white immigrants. Literally, the messages posted during the period of the injunction commented on multiculturalism (to the extent that postings such as "FUCK MULTICULTURALISM!!! FUCK YOU LIBERALS!!! MULTICULTURALISM IS SHIT!!!" can be described as "commentary"), but the court had no difficulty finding that they were in breach of the order nonetheless:

> ¶ 46 It is evident that both the form and substance of the messages are the same. They have the same vile content and the unrelenting message of hatred for Jews and contempt for people of the Black race and/or immigrants. The obvious subterfuge to talk about 'multiculturalism' instead of 'Jews' or 'J(emoticon)(emoticon)Z' or 'ZOG' instead of 'Jews' does not deceive anyone.

There was an issue in the case, however, as to whether it had been sufficiently proven that it was Winnicki who had posted the messages. Among other claims, Winnicki argued that there was no proof that he was the same person as the Tomasz Winnicki posting on the Vanguard News Network website, that someone else posing as him could have posted the messages, and that if he had posted messages, they could have been altered

or edited by other persons. None of these arguments persuaded the trial judge.

The judge noted that, if the Tomasz Winnicki in front of him had not posted the messages, it was difficult to understand why he had never advanced that defence at any previous stage of the various proceedings. Further, several of the postings made explicit reference to the existence of the Federal Court injunction. As a result, the judge had no doubt that "the poster Tomasz Winnicki on the VNN website is one and the same as TW against whom Justice de Montigny issued the restraining order" (para 31). Further circumstantial evidence that the accused had posted the messages himself came from his name and city, his signature line, and the icon representative of his messages being posted along with them. These facts, combined with the poster's clear knowledge of the terms of the injunction, satisfied the judge that Winnicki had posted the messages.

On the basis that Winnicki's behaviour was "wilful, contemptuous, repetitious, and contumacious" (para 49), and that he had shown a total lack of respect for the Court and no remorse for the contempt, the court sentenced him to imprisonment for nine months.

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT – DISCUSSION PAPER

The Office of the Privacy Commissioner of Canada has published a Discussion Paper concerning *PIPEDA*. That legislation is subject to a mandatory review every five years, and so a review is scheduled for 2006. The Privacy Commissioner has invited comments on a series of issues that it perceives should be addressed, to assist it in drafting its submission to Parliament.

The Discussion Paper notes that under *PIPEDA* the Commissioner has a limited discretion to initiate complaints and conduct audits, and that it can disclose information concerning personal information management practices. However, it has no authority to issue binding orders requiring organizations to change their practices, nor any ability to award damages. The Commissioner's role is largely limited to negotiating settlements: any binding results can only be obtained through application to the Federal Court. The Discussion Paper questions whether the Commissioner's current role, which might be seen as having the advantages of flexibility and accessibility, should be continued, or changed to one involving order-making powers, which might be seen as more effective.

The Discussion Paper also raises questions concerning the extent to which private data should be protected from collection and distribution to government and investigative bodies without the consent of the individual. At present, because of changes made to *PIPEDA* following the incidents of September 11, 2001, air carriers and travel agencies can collect personal information about customers without their knowledge or consent, for use by government-run airline passenger screening systems. This information, the Paper notes, can be secretly collected for the purpose of making a disclosure:

- that is required by law;
- to a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that it suspects that the information relates to national security, the defense of Canada or the conduct of international affairs; or
- on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization suspects that the information relates to national security, the defense of Canada or the conduct of international affairs.

While acknowledging the potential national security concerns, the Discussion Paper raises the issues that these provisions are not, on the wording of the section, restricted to air carriers and travel agencies, and that there are no limits on the amount or sources of information, nor the time period during which it is collected. Further, the organization need not have any legitimate business purpose for collecting the information. The Paper questions whether private sector organizations ought to act as personal information collection agents for the government,

whether records should be created solely for the purpose of providing them to government, and, if so whether the current authority to collect personal information without the knowledge or consent of the individual is broader than necessary.

On a similar issue, the Paper questions the current *PIPEDA* provisions permitting organizations to disclose personal information, without the knowledge or consent of the individual, to an "investigative body". That term is not defined in the Act, and instead individual bodies are confirmed by regulation as falling within the definition. Two agencies were listed when PIPEDA was introduced, but there are now roughly 75 listed "investigative bodies". The Paper questions whether it would be better to move to a definition of that term, rather than deal with each potential "investigative body" individually. It also raises the possibility that the Act could be phrased in a different way, speaking more about investigative purposes rather than investigative bodies, as a way of dealing with the issue.

The Discussion Paper also raises some potential gaps in *PIPEDA* which might be filled. It notes that at present the Act only covers the actual collection, use or disclosure of personal information: attempts to collect personal information are not covered. As a result, individuals have no recourse against organizations which have unsuccessfully tried to gather and disclose personal information. The Paper raises the question as to whether such willful attempts ought to be regulated. Similarly PIPEDA does not create any duty to notify on the part of organizations that have suffered security breaches, though clearly such breaches could have privacy implications for individuals.

A number of other questions are also raised in the Paper, including:

> Should *PIPEDA* be amended to deal with "blanket consent?"
>
> Should *PIPEDA* be amended to allow the transfer of personal information from an organization to a prospective purchaser or business partner? If so, what restrictions should apply?
>
> Does the current accountability principle in *PIPEDA* sufficiently protect personal information when it crosses borders?
>
> If not, how might *PIPEDA* better protect that information?

Comment on the issues raised by this Discussion Paper at the IT.Can Blog

TORONTO WIFI NETWORK – TRACING USERS

Toronto Hydro Telecom's plans to create a WiFi network giving blanket coverage of the downtown Toronto core, which it says will be the largest ubiquitous WiFi coverage zone in Canada, have been delayed. The announced plans involve installing radio access points on street lighting poles as a method of covering any existing dead zones, in order to create coverage through the six square kilometer area bounded on the east by Jarvis Street, on the west by Spadina Avenue, on the south by Front Street and on the north by Bloor Street. The service was initially expected to be fully functional by December 31st, 2006, and will operate free of charge for the first six months. The first phase, covering the area between Front Street, Queen Street, Church Street and Spadina Avenue was to have been completed in July, but it has now been announced that it will not be operational until September 7. The delay resulted from concerns by the Toronto Board of Health, which was concerned whether radio signals blanketing the area would a health risk, and by police, who expressed concerns that the free trial of the service could make it impossible to track illegal activity carried out over the web. To satisfy the latter concern, users of the free trial will be required to register a password which will link the user to his or her cell phone records.

WARRANTLESS SEARCH – SNIFFER DOGS

The Supreme Court of Canada's decision in *R. v. Tessling*, that the use of a FLIR did not impinge on a reasonable expectation of privacy and therefore did not constitute a search, continues to have an unsettled

impact on criminal law. In the wake of *Tessling* several lower courts had applied its reasoning to find that the use of sniffer dogs did not constitute a search. In Alberta, this contradicted the conclusion which had been reached by the Alberta Court of Appeal, pre-*Tessling*, in *R. v. Lam*. The Ontario Court of Appeal recently decided that *Tessling* did not lead to that conclusion, and that the use of sniffer dogs was indeed a search (see the discussion of *R. v. A.W.* in the May 5, 2006 newsletter. The Alberta Court of Appeal has now returned to the issue, upholding a lower court decision and deciding in *R. v. Brown* that the effect of *Tessling* was implicitly to overturn the earlier decision in *Lam*.

The Court of Appeal noted that *Lam* had not been explicitly overturned, but that the key points to its reasoning had been addressed and varied by *Tessling*. The reasoning in *Lam*, they said, was that any police interference with or intrusion on a reasonable expectation of privacy was a search, that there was a reasonable expectation of privacy in a locker, and that the dog's sniffing "saw into" the private area of the locker, using a technique which went beyond what human senses would detect. That syllogism could no longer be supported in light of *Tessling*, they held. The Supreme Court had created hierarchies of expectation of privacy in that decision, weakening the first and second steps, and had decided that not all information obtained in public about the contents of a private place is a search, weakening the third step. As a result, the syllogism was no longer reliable reasoning. The Court of Appeal stressed that it was not making a decision about dog sniffing in general:

> ¶ 38 …There cannot be a rule of law now that dog sniffs of luggage in lockers are always a s. 8 search, or that they never are.

Tessling required that each situation be considered on its own facts, the court held, and in this case they were merely determining that the trial judge had not made an error of law in deciding that the particular dog sniff in question was not a search.

Comment on the issues raised by this case at the IT.Can Blog.