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

February 5, 2009

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

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

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

Criminal Law: Police Use of Request for Information under Privacy Legislation Rather than Search Warrant Approved

The Saskatchewan Provincial Court has decided that police are entitled to use a request under the provincial Freedom of Information and Protection of Privacy Act (FIPPA) rather than a search warrant to obtain the name and address of a subscriber from an Internet Service provider with the decision in *R. v. Trapp*. A police constable was conducting computer undercover monitoring of peer-to-peer file sharing for pornographic images. In the course of the investigation, she identified "an unknown person at an unknown location, at the noted time, using IP address 207.47.225.82 issued by SaskTel ... in possession of information which may identify the person responsible and the location of evidence used in committing the noted Criminal Code offence". Saskatoon Police Services then sent a letter to SaskTel, entitled "Request for Account Information pursuant to a Child Exploitation Investigation" under s. 29(2)(g) of FIPPA. That section provides that

> 29(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30.
>
> (2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed: ...
>
> (g) to a prescribed law enforcement agency or a prescribed investigative body:
>
> (i) on the request of the law enforcement agency or investigative body;
>
> (ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and
>
> (iii) if any prescribed requirements are met;

In response to the request, Sasktel sent the police the accused's name, address, telephone number, and email addresses. The accused was eventually arrested and charged with possession of child pornography. He argued that the use of FIPPA to obtain this information had violated his section 7 Charter right, because the provision was vague, and his section 8 *Charter* right, because it had been an unreasonable search and seizure.

The accused relied on the Ontario decision *R. v. Kwok*, which on similar facts had found a section 8 breach. However, the trial judge in *Trapp* concluded that there was no violation of either section 7 or section 8. The judge found that the section provided sufficient guidance for legal debate: there was no real room for confusion over the meaning of "prescribed law enforcement agency" or any other terms, and so the section was not vague.

The potentially more complicated issue was the section 8 question, and the issue of whether the police ought to have sought a warrant rather than use FIPPA. The information obtained was private and personal information, it was argued, and in the absence of privacy legislation the police would be required to obtain a warrant. The accused argued that proceeding under FIPPA rather than the Criminal Code made the search unreasonable.

The trial judge accepted the Crown's argument, based on the Supreme Court decision in *R. v. Plant* and the Saskatchewan Court of Appeal decision in

R. v. Cheung that there was no section 8 violation. In each of those cases police had obtained information about an accused without a warrant: in *Plant* electrical consumption records had been provided by the power company and in *Cheung* a Digital Recording Ammeter (DRA) had been attached to the accused's power lines to detect cycling patterns. In each case the courts had concluded that the information obtained did not reveal any intimate details about the accused's lifestyle or go to the biographical core of personal information. The same rationale, the trial judge held, applied here, and so no warrant was necessary. In addition, the trial judge accepted the argument that, based on five factors enumerated in *Plant*, no warrant was needed here: the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated. The Crown had argued, and the trial judge accepted, that the information, the accused's identity, was public information, that SaskTel had a contractual relationship with the accused which was not a confidential one, that the information was in the hands of SaskTel and was obtained non-intrusively, and that the offence in question was a serious one. (Note that in *R. v. Tessling* the Supreme Court of Canada explicitly overruled *Plant* on whether seriousness of the offence was a relevant consideration: see para 64.) Accordingly as in *Plant* and *Cheung* there was no need for a warrant, and the police were entitled to obtain the information through a FIPPA request.

Domain Name Disputes

In *Bowring & Co. Inc. v. Eric Maddeaux*, a 3-member CIRA Panel (Donovan, Lametti and Tawfik, Chair) considered a dispute over the domain name bowring.ca. The Complainant ("Bowring") is an Ontario company with head offices in Toronto, which operates a chain of retail stores in Canada. It obtained a number of registered Canadian trademarks using the word BOWRING by assignment from the receiver of the former owner, Tereve Holdings, in November 2005. It maintains several websites which use the mark (e.g. bowring.com) to market its stores and wares. The Registrant ("Maddeaux") is an individual who resides in Mississauga. He registered the domain name when the former registration by Tereve lapsed in June 2006. Bowring had brought a previous complaint against Maddeaux regarding the domain name in 2007, but the Panel (whose decision was reported on in an earlier issue of this Newsletter) ruled that Bowring had made out neither the "Canadian Presence" requirement under the CIRA Policy, nor had it established rights in the mark in Canada, and thus the complaint had been dismissed. Bowring had negotiated unsuccessfully to purchase the domain name from Maddeaux. Maddeaux argued that by bringing this second proceeding Bowring was acting in bad faith under 12.6 of the Rules and requested costs.

The Panel first had to determine whether the previous unsuccessful complaint barred Bowring from revisiting the same claim. Noting that neither the Policy nor the Rules prohibited this, the Panel ruled that it was appropriate to hear this complaint because the previous ruling had been on a procedural point and had not addressed the substance of Bowring's claim. It took the view, however, that there might be circumstances in which a Panel should decline to hear a repeated complaint, such as where the Complainant's purpose was to harass or intimidate a registrant. Turning to the merits of the claim, the Panel held that Bowring had rights in, and had used, the BOWRING marks since the November 2005 assignment, and thus had rights to the mark in question. The domain name was identical to the mark, and thus was "confusingly similar" to the mark under 4.1 of the Policy. As to whether Maddeaux had registered the domain name "in bad faith," the Panel noted that the evidence disclosed that he "clearly engages in a pattern of registering domain names in order to prevent those who have trademark rights in the name from registering it as their domain name" (p. 5). The Panel took explicit note of other CIRA decisions which found that Maddeaux generates revenue through his registered domain names by a per-per-click arrangement that redirects users to advertising by competitors of the mark holders. This constituted bad faith. The Panel rejected Maddeaux's argument that he intended to use the domain name for a jewelry site he had yet to develop, stating "a vague and unsubstantiated intention to use the domain name at some unspecified date is insufficient to dispel the evidence of bad faith" (p. 6).

The Panel finally concluded that Bowring had discharged its onus of providing some evidence that Maddeaux had "no legitimate interest" in the domain name, noting that none of the six legitimate interest criteria in 3.6 of the Policy applied to Maddeaux's use. The domain name was ordered transferred to Bowring, and given that finding the Panel held that it did not have to address Maddeaux's claim for costs.

Privacy: Federal Commissioner Finds CHRC Did Not Hack Internet Connection

The Office of the Privacy Commissioner of Canada (OPC) recently rendered a decision regarding the complaint of Ottawa resident Nelly Hechme that officials with the Canadian Human Rights Commission (CHRC) had hacked into her wireless internet connection and used her internet pseuydonym to post messages on white supremacist websites. It was widely reported last spring that during a hearing dealing with allegations of hate messages against Toronto resident Mark Lemire, CHRC investigator Dean Steacy admitted he had posted racist messages under the pseudonym "jadewarr." In response to a subpoena, Bell Canada linked the name to Hechme and her personal information was filed as evidence at the hearing. In media statements, Hechme (who lives very close to CHRC headquarters) indicated that she felt her encrypted internet connection had been hacked. She made a complaint with OPC pursuant to the *Privacy Act*.

In her findings, the Privacy Commissioner noted that in these circumstances Hechme's IP address constituted "personal information" under section 3 of the *Privacy Act* and thus was properly a subject of inquiry. However, she found that there was "no evidence that the CHRC ever collected or improperly used, disclosed or retained the complainant's personal information," or even that the CHRC knew about Hechme prior to the Lemire hearing. She cited evidence from "technical experts" to the effect that "most likely, but without certainty, the association of the complainant's IP address to the CHRC was simply a mismatch on the part of a third party, which could have occurred in a variety of ways not involving the CHRC." However, no finding could be made as to how this use of Hechme's information had actually occurred. Accordingly, the complaint was ruled to be "not well-founded."

Privacy Commissioner releases Guidelines for Processing Personal Data Across Borders

The Office of the Privacy Commissioner of Canada (OPC) has issued a set of "Guidelines for Processing Personal Data Across Borders". In part the guidelines are a recognition of the fact that the OPC is limited by jurisdiction, and so cannot directly regulate third parties in other jurisdictions which have data about Canadians. However, the OPC is able to regulate the Canadian organizations which transfer the information out of the country, and so the guidelines focus on that approach. There is no prohibition preventing organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. In such cases, the information is not regarded as disclosed to a third party: it has simply been transferred in order to comply with one of the original purposes for which it was gathered, such as providing 24 hour customer support. In that event no addition consent for the transfer is needed. However, the organization which originally gathered the information remains responsible for seeing to it that the information is still adequately safeguarded despite the transfer.

In particular, the guidelines state:

> The transferring organization is accountable for the information in the hands of the organization to which it has been transferred.
>
> Organizations must protect the personal information in the hands of processors. The primary means by which this is accomplished is through contract.
>
> No contract can override the criminal, national security or any other laws of the country to which the information has been transferred.
>
> It is important for organizations to assess the risks that could jeopardize the integrity, security and confidentiality of customer personal information when it is transferred to third-party service providers operating outside of Canada.

Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.

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 Robert Currie, 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 Robert Currie, 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.