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

March 26, 2010

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.

Possession of Child Pornography in the Internet Context

The Supreme Court of Canada has handed down a major decision with respect to the meaning of "possession" in the context of internet usage with its decision in *R. v. Morelli*. The accused was charged with possession of child pornography. A computer technician had arrived unannounced at his house to install a high speed internet connection. The computer was located in a spare bedroom where the accused's three-year-old daughter was playing with toys on the floor. The technician observed two links among the accused's browser favourites with names suggesting that they linked to child pornography websites, and also saw a pornographic image on the computer. In addition the technician noticed home videos and a webcam that was connected to a videotape recorder and was pointed at the toys and the child. When the technician returned the next day, the toys had been cleared away, the webcam was pointing at the desk, and the computer's hard drive had been formatted. The technician was suspicious because of these facts, and two months later, after speaking with his mother, reported these facts to social services. Social services in turn reported the matter to the RCMP. Two months after that, the RCMP obtained a search warrant to seize the accused's home computer and look for evidence of possession of child pornography. At trial, the accused challenged the constitutionality of the search on the basis that the search warrant was improperly issued. This argument was unsuccessful at trial and he was convicted. He renewed the argument before the Saskatchewan Court of Appeal, which upheld his conviction. The accused then appealed to the Supreme Court of Canada.

In a 4-3 decision, the Supreme Court accepted the accused's argument and found that the warrant had been improperly issued. They concluded that the search therefore violated section 8, and concluded that the evidence should be excluded under section 24(2). As a result they entered an acquittal.

Of particular interest is the Court's discussion of the concept of "possession" in the particular context of possessing an image on a computer. Possession, they noted, required both knowledge and control. The necessary degree of control could not be established by showing that the accused had used a web browser to view an image stored in a remote location on the internet. Whether considered from the point of view of actual possession (keeping an item in one's own physical custody) or constructive possession (keeping the item in another place for one's own benefit), merely viewing a website did not constitute possession.

The Court noted that the concept of possession had developed in relation to physical, concrete objects, and that its extension to virtual objects presented conceptual problems. They drew a distinction between an image file and its decoded onscreen visual representation. The concept of possession, they held, necessarily related to the former and not to the latter. That is, "possession of an image in a computer means *possession of the underlying data file*, not its mere visual depiction" (para 19, emphasis in the original).

They reached this conclusion for several reasons. First, they noted that the *Criminal Code* contained separate offences of possessing child pornography and accessing child pornography: if merely viewing images was possession, the latter offence would have been unnecessary. Second, they noted that possession normally implied an ability to transfer the item in question to someone else. Sharing a link to a website did not amount to transferring an item:

> it is indeed the underlying data file that is the stable "object" that can be transferred, stored, and, indeed, possessed. (para. 29)

A person seeking a search warrant relating to possession of child pornography, they therefore concluded, needed to show a justice of the peace reasonable grounds to believe that offending data files would be found on the accused's computer, not simply that the computer had been used to view offending images stored elsewhere.

The dissenting judges would have adopted a more expansive definition of possession in the internet context. In their view:

> [140] This case does not require the Court to elaborate on the distinctions between accessing and possession of prohibited material. Suffice it to say that the question before us turns not on whether the accused has merely viewed the material, but on whether evidence of control over the material could be found in the computer that was to be searched. Accessing does not necessarily require control, and possession does not necessarily require viewing. Therefore, for the purposes of the offence of possession, viewing might be one way to prove knowledge of the content, but it is not the only way. Similarly, viewing might be one way to prove control, but it may not be sufficient — the circumstances in which the material was viewed would need to be proven. Control, not viewing, is the defining element of possession.
>
> [141] Therefore, even if an accused does not actually download offending material, possession is established if the accused has control over the material for his or her use or benefit or for that of someone else. The record does not indicate that the reviewing judge was provided any evidence on caches. However, there is now abundant legal literature in which the authors have discussed caches, temporary Internet files, and deleted material that can be retrieved, all of which may, under relevant circumstances, constitute evidence of possession. The degree of control might be established on the basis, for example, of the displaying of the images and the ability to select, cut, enlarge, print, forward or share images…

The majority of the Court also addressed the specific issue of whether possession could be established on the basis that copies of the image files might be found in a computer's cache. In general they rejected this possibility. Possession requires both knowledge and control. Where above the majority found that a computer user did not have control over images in remote locations, here the majority concluded that a computer user will not have knowledge of items in the cache:

> [36] On my view of possession, the automatic caching of a file to the hard drive does not, without more, constitute possession. While the cached file might be in a "place" over which the computer user has control, in order to establish possession, it is necessary to satisfy *mens rea* or fault requirements as well. Thus, it must be shown that the file was *knowingly* stored and retained through the cache.
>
> [37] In the present case, the charge is not based on the appellant using his cache to possess child pornography. It is hardly surprising as most computer users are unaware of the contents of their cache, how it operates, or even its existence. Absent that awareness, they lack the mental or fault element essential to a finding that they culpably possess the images in their cache. Having said that, there may be rare cases where the cache is *knowingly* used as a location to store copies of image files with the *intent* to retain possession of them through the cache.

In this particular case the majority found that the search warrant was not properly issued. In part this related to concerns about the selective presentation of information to the justice of the peace: mention was made of the two "favourites" which dealt with child pornography but not of the many other favourites which led to legal pornography. Various other facts, such as that the accused's wife lived with him, that the webcam was not connected to the computer, that the room the child was in was set up as a playroom, and so on, were either omitted or presented in misleading fashion. The Court also held that the warrant application created

the impression that the technician had seen child pornography on the accused's computer which had been erased by the second day. The application referred to the technician seeing "lolita porn" and to that having been erased when he returned. In fact this referred to the listing in the accused's favourites, and was simply the name of the website it linked to. The majority concluded that the information was presented as though the technician had himself seen child pornography – i.e., lolita porn - which was then deleted.

Adding these deficiencies to the fact that the warrant was not sought until four months after the observations were made, and that the accused was reported to have reformatted his hard drive after the first day, the Court concluded that there was no basis for a reasonable belief that evidence of child pornography would be found on the accused's computer. Accordingly they quashed the warrant, and following a section 24(2) analysis they excluded the evidence and acquitted the accused.

Privacy: Aerial Surveillance of Greenhouse Marihuana Grow Operations

In *R. v. Kwiatkowski*, the appellant appealed his conviction for unlawful production of marihuana and possession of same for the purpose of trafficking. While the police was conducting routine aerial surveillance of outdoor marihuana grow operations, an officer spotted a property with greenhouses situated in a suspiciously remote location. The police helicopter flew around the property but not over it at a radius of half a mile. The operating constable used a zoom lens –a type readily available from retail outlets –and saw plants with distinctive green colour through translucent walls of the greenhouses. He observed from one angle a plant he suspected was marihuana through an open door of one of the greenhouses. The officer flew around the property a couple of occasions following the discovery to obtain more photographs.

Later, the lead investigator prepared the information to obtain (ITO) a search warrant. The telewarrant obtained with the ITO authorized the search of the accused's greenhouses and outbuildings. In the process of executing the search warrant, the police caused damage to greenhouses by cutting off the plastic walls thereof. They arrested the appellant and his co-accused, seized several equipment suitable for indoor marihuana grow operations and about 3, 000 marihuana plants. All of these led to the conviction of the appellant.

At the trial court, the appellant argued, among other things, that the police aerial surveillance was a breach of his reasonable expectation of privacy. Similarly, the appellant alleged that police failure to comply with "knock-notice" rule invalidated the execution of the warrant. Also, the appellant faulted the Crown in regard to the veracity and quality of the ITO. He argued that there was a misleading representation regarding the dictation of the odour of marihuana. Further, he charged that references to the opinion of commercial greenhouse operators in the ITO were misleading also.

In upholding the conviction of the appellant by the lower court, the court of appeal agreed that the surveillance technology used in the present case (a camera with zoom capacity) is not an extraordinarily powerful or advanced instrument. It is not fundamentally different from ordinary binoculars. Such a device, the court noted "cannot be realistically likened to a warrantless perimeter trespass ... and did not intrude on the appellant's reasonable expectation of privacy [and] s. 8 [of the *Charter*] is not engaged as the police were not obliged to obtain a search warrant to conduct an aerial search" (41). The court rejected the appellant's invocation of the decision in *Tesling and Kuitenen*. In the latter, the court held that using FLIR technology to fly over the accused's residence at an altitude sufficiently low as to see that one of the men in the compound was urinating violated the accused's reasonable expectation of privacy. In the former case, where the police flew directly over the accused home using FLIR technology and was able to measure the heat emanating from his home, the Supreme Court was inclined to apply the totality of circumstance test to determine whether the accused's reasonable expectation of privacy was breached.

The court distinguished and rejected the application of the two cases in the present scenario. It recognized that the appellant had direct interest in the subject matter of the surveillance because he occupied the property in which the greenhouses

were located. However, the court observed that the police did not conduct surveillance directly over the appellant's property and the technology used by them was not intrusive. Perhaps more importantly, the court found that the presumption or expectation of privacy is reasonable in respect of a person's home which is recognized as a place protected from state intrusion. Such a presumption cannot "extend to translucent non-residential structures located ... a long distance from residence with no actual road leading to it" (para. 39).

Finally, the court found that the alleged discrepancies in the ITO were not misleading and that the warrants could still have been issued without them. On the police failure to comply with the knock-notice, rule, the court held "[t]he source of the rule derives from the same privacy interests that animate s.8 – that a person's home is protected from the forces of the Crown ...The emphasis has always been on the sanctity of the home or dwelling house and the police duty to announce their presence and purpose before forcing entry into a dwelling house" (para. 55).

Saving Public Interest Commentary from Safeguard Order

In *Takefman v. Bier*, the appellant appeals the judgement of the Quebec Superior Court (District of Montréal) in which the court granted the respondent's motion for a safeguard order. The order enjoined the appellant to cease and desist from communicating directly orally and/or in writing with the respondents, including electronic communications such as e-mail and text messages. The second order enjoined the appellants to cease and desist from communicating in writing, including electronic communications such as e-mails and text messages, any comments and statements to any third parties concerning the respondents by name or reference thereto, save and except to his legal counsel and staff.

The appellant and respondent were long term acquaintances. On the basis of their relationship and at the suggestion of the respondent, the appellant bought shares in a company in which the respondent had interest. It turned out to be a bad investment and the appellant felt that he was a victim of false representation. After the appellant's initial threat to sue, both parties reached a settlement in which additional shares were provided to the appellant at no cost. Following further loss of value in the stock, the appellant embarked on sending "various e-mails to the respondents and common friends, which the respondents considered smear campaign" while for the appellant the e-mails were intended to ensure that "everyone knows the real truth" (para. 8). The respondent filed complaint for criminal harassment against the appellant but the latter was acquitted for want of evidence. Meanwhile, subsequent attempts by the respondents to obtain a safeguard order against the appellant were not successful until the present order which the appellant now appeals. The court found that appellant's 'e-mails apparently carried heavy toll for the respondents: loss of sleep and weight, attempted suicide, etc" (para. 10)

In allowing the appeal in part, the appeal court held that the first order of the lower court (i.e. enjoining the appellants from sending e-mails to the respondents and to cease what the latter considered a form of harassment) was "perfectly valid in the context revealed by the evidence" (para 18). The court noted that "[t]he problem here is with the second order. It is too broad" (para 19). Setting aside the second safeguard order, the court of appeal noted among other things that:

> [I]t fringes upon the appellant's freedom of speech by preventing him from expressing, in writing, any comments whatsoever about the respondents. One may consider that the appellant has abused his freedom of expression by disclosing aspects of the private life of the respondents with regard to matters that are not of public interest in any way and may constitute clear violation of the respondent right to privacy guaranteed by s. 4 of the Quebec Charter of Rights and Freedoms recognized at art. 35 and 36 Civil Code of Quebec. However, the order also prevents the expression of commentary with regard to the financial services provided by the respondents, which may be of public interest (para. 21).

Validity of Electronic Signature on Police Ticket

In *London (City) v. Caza*, pursuant to the implementation of a new technology which allows

for the issuance of electronically based Provincial Offences Notices as a replacement of the traditional carbon-paper based multiple copy paper ticket, a London Police Service officer personally served a certificate of offences (a.k.a tickets) for various offences on three individuals in the course of his duty. To issue the ticket, the issuing officers had to access the police computer system using their password. They would then fill relevant data fields, including charging statute, section, fine, and signature. The ticket are then issued electronically on a Form1 document and the operating electronic device affixes an e-signature in the signature box which is located on the lower left section of the ticket on behalf of the issuing officer. After this, the ticket is then printed and a copy is provided to the alleged offenders as did the officer in this case.

The tickets were subsequently filed with the administrative office of the Ontario Court of Justice in London. They remained in possession of the court administration for the statutory 15-day period in which the respondents had the opportunity to contest them. Sitting in Chambers, subsequently, a Justice of Peace examined the tickets to determine "if they were complete and regular on their face, pursuant to s. 9.1(2) of the *POA* [*Provincial Offences Act*]". Not satisfied, he proceeded to quash the ticket on the basis of that they contained "no signature of provincial offence officer".

In overturning the decision of the Justice of Peace, the court (Morissette, J.) examined the relevant statutes and regulation, and specifically noted that s. 76.1 of the *POA* provides that a Certificate of Offence may be completed and signed by electronic means in accordance with the regulation" (para. 20). The court noted further that the regulation "made under the *POA* and titled 'Electronic Documents' [] specifically provides for the electronic generation of Certificate of Offence documents and the electronic signing of them when issued pursuant to the *POA* as they were in the matter before the court" (para. 23).

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.

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