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

March 24, 2011

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: Privacy in Work Computers

In *R. v. Cole* the Ontario Court of Appeal addressed the issue of the amount of privacy a person can expect in a work computer. The accused was a teacher at a high school, and had some responsibility for supervising the school's network. A school technician who was also monitoring the network had observed an unusual amount of activity between the accused's computer and the network, and so he remotely accessed the accused's hard drive to perform a virus scan. In the course of doing so the technician discovered a hidden folder called "new folder" and opened it, where he saw nude pictures of a female student in the school. It transpired that the accused had discovered these photographs when he had been monitoring student accounts, and he had downloaded them to his hard drive. The technician took a screen shot of the laptop and showed it to the principal. At the principal's request, the technician downloaded the photographs to a disc. The next day the principal asked the accused to hand over his computer, which a School Board technician subsequently accessed and examined. That examination turned up a large number of pornographic images in the laptop's temporary internet files: these too were copied to a separate disc. The School Board then provided the two discs and the laptop to the police, who examined the data on each disc and had the contents of the laptop analysed: the police did not obtain a warrant before doing so.

The Ontario Court of Appeal held that the accused had a reasonable expectation of privacy in the laptop, even though it was owned by the School Board. However, they held that the School Board had been entitled to conduct the examinations of the laptop that it undertook, and so those examinations did not violate the *Charter*. Turning over the disc with the pictures of the student also did not violate the *Charter*, and the police were entitled to look at that disc. However, the police were not entitled to look at the disc containing the temporary internet files or to examine the laptop without obtaining a warrant, and so that action had violated the *Charter*. The Court of Appeal concluded that the illegally obtained evidence should be excluded.

The question of a reasonable expectation of privacy hinged on consideration of factors which had been set out by the Supreme Court in a number of cases. The laptop did belong to the School Board, but that fact did not defeat the accused's reasonable expectation of privacy claim. It was understood that teachers (who had exclusive possession) were allowed to use the laptops for personal reasons as well as work, and it was understood that they might store personal and private information on them. There was no clear understanding of whether the school's acceptable use policy applied to teachers. Further, even if the laptops could be examined to enforce school regulations, that would not mean that there was no expectation of privacy:

> [42] ... the fact that a computer technician could access the hard drives of the laptops does not negate a reasonable expectation of privacy, just as the existence of a master key does not destroy the reasonable expectation of privacy in a rented apartment or in a bus locker.

Accordingly, the Court of Appeal concluded that the accused did have a reasonable expectation of privacy in his work computer.

Having a reasonable expectation of privacy in a work computer, however, did not mean that the accused could expect that no data on the computer could ever be examined by anyone. In this case, when the

technician remotely accessed the accused's hard drive and look in the hidden folder, he was acting within the scope of his authority to maintain the school's network: that is, he had "a specific reason for opening the folder that directly related to his role of maintaining the network" (para 57). That examination therefore did not violate section 8 of the *Charter*. As soon as the technician looked in the hidden folder the nude images were in plain sight, and no further level of examination such as would be necessary with written personal information was necessary. The technician acted reasonably in taking the information he discovered to the principal.

The principal and the School Board were also authorised to act as they did, as matters of enforcing school rules or dealing with a disciplinary matter. This included the School Board's action in examining the temporary internet files on the accused's computer:

> [64] ... the school board had an ongoing obligation to take steps to ensure a safe and secure learning environment for its students and to protect the students' privacy rights. The search of the laptop and preservation of the evidence for an internal discipline procedure was an obvious means to do so. Although there was no suggestion that the images copied from the temporary internet files depicted any student or were obtained from the school network, presumably they would be evidence potentially relevant to the purpose of the appellant's possession of the student's photographs or to whether this use of the computer contravened the school board's Policy and Procedures Manual.

The same was not true, however, of the actions of the police. Although the School Board was entitled to examine the material for internal disciplinary purposes, that did not mean that the police were also entitled to do so without a warrant. The fact that the laptop was owned by the School Board and that the School Board had consented to the search did not defeat the accused's reasonable expectation of privacy. In that event examining the laptop constituted a search and so a warrant was required.

The Court of Appeal, however, distinguished the disc with the nude images of the student from the disc of the temporary internet files and the laptop. The latter two engaged the accused's privacy interests (by containing personal information or by exposing his internet browsing habits) and the fact that his reasonable expectation of privacy had been lost for some purposes (the internal discipline matter) did not mean it was lost for all purposes.

The disc with the nude images, however, was different. The Court of Appeal held that handing it over was the functional equivalent of handing over an envelope containing pictures: looking at the pictures in the envelope would not constitute a search. They said:

> [80] However, different considerations apply to the disc with the screen shot and the images of the student. Given that the photographs were taken from the school's network, using the school's computer and were the subject of the privacy interest of a student, the appellant had no personal privacy interest in the data. The photographs were found by the technician in plain view, while engaged in permissible access. They were lawfully seized by the principal and transferred to police. As the functional equivalent of photographs in an envelope, the police did not need to conduct a further search of this evidence. Because the appellant had no privacy interest in the photographs themselves (as opposed to the presence of those photographs in the laptop), the delivery of the disc to police was not a seizure. This transfer is analogous to the transfer of the drugs found in the student's pocket by the vice-principal in *M.R.M.* In that case, the police did not require a search warrant to open the baggie and retrieve the drugs. Thus, the viewing of the photographs and the screen shot on the disc by police in this case was not a search or seizure within the meaning of s. 8 of the *Charter* and that evidence should not have been excluded by the trial judge.

The Court of Appeal ordered the exclusion of the evidence obtained through the police search of the disc containing the temporary internet files and the laptop, and remitted the matter back for trial.

Dynamic IP Addresses, Wireless Routers and ITOs

In *R. v. Smith*, 2011 BCSC 316 (no hyperlink available) the accused had been subject to a search warrant which had discovered child pornography in a shared folder on the hard drive of his computer. He argued that the search warrant should be quashed on the basis that the Information to Obtain (ITO) was misleading and did not justify the issuance of the warrant. The trial judge, on a voir dire, rejected this argument.

The accused's argument was based primarily on two claims. First, he argued that the ITO was misleading because it created the impression that the IP address linked to his home address was a static one, when in fact it was a dynamic IP address. Had this fact been disclosed, he argued, the issuing justice would not have had a basis for issuing the warrant. In addition, the accused argued that the ITO failed to disclose that a police officer had detected wireless Internet networks near the applicant's home: the implication of this fact, he argued was that could have accessed those wireless signals and downloaded the pornographic images.

With regard to the IP address, the ITO had stated that the accused's ISP used static IP addresses. Having a static IP address would be significant, since the police had accessed the shared folder associated with the IP address on more than one occasion and had observed child pornography. In fact the accused's ISP used dynamic IP addresses, and so this fact should have been disclosed. However, the trial judge concluded that there was no intention to mislead, and that the error was not one which undermined the warrant. A more accurate statement would have been that the IP addresses were dynamic, though as a matter of practice within the experience of the officer, a user's IP address typically would not change over a period of many months. It would have been preferable if the ITO had stated that, but that did not mean that there the ITO did not provide a basis for issuing the warrant.

This was particularly so, the judge held, given the other evidence linking the IP address to child pornography. The judge noted that every digital image has a unique and unalterable alpha-numeric identifier, referred to as a "hash algorithm". The hash values of a large database of child pornography images are known to the police. Further, through the use of a program called GnUC, the police can process IP addresses and record each time a given IP address downloads an image with one of those hash values. Further, that software can generate a historical report for a specific IP address, showing the dates and times that the computer was logged on to Gnutella and child pornography with know has values was shared by the computer. In this case, that historical report showed that over a period of roughly one year the IP address had a "hit count" of 319. Given those facts, which were reported in the ITO, it was difficult to claim that the ITO did not disclose reasonable grounds for the warrant.

The non-disclosure of wireless networks was also not a material non-disclosure leading to the quashing of the warrant. The police had conducted a wireless scan and discovered 20 networks in the vicinity of the accused's house, four of them unsecured. It was also conceded on the voir dire that the police did not know whether the accused's computer was on one of those unsecured networks. This information had not been included in the ITO and was arguably relevant because it raised the possibility that someone else had downloaded the child pornography associated with the IP address.

However, the trial judge concluded that the warrant should not be quashed. The police had not been obligated to conduct the wireless scan at all, which had been done as an afterthought. Generally speaking, the fact that another person was using the accused's wireless network (if that were true) would not allow that person to gain access to the hard drive of his computer. Based on the evidence presented, the trial judge concluded that there was some possibility for a sophisticated user who was knowledgeable about the wireless router's coding to gain some access to a computer linked to it, but that this was highly conjectural. Although it would have been preferable to disclose the existence of unsecured networks, the failure to do so was not fatal.

Further, had the information about wireless networks been disclosed, it would not have changed matters. The only way to establish the likely innocence or guilt of occupants of the location, the trial judge held, would have been to examine the computers, router

and any other electronic storage devices inside the location. Regardless of this fact, therefore, the trial judge held, the police's investigatory route would have been the same. The ITO was not found to be inadequate and the warrant was not quashed.

Unjust Enrichment and Email Communications

In *Rubin v. Gendemann* (no hyperlink available) the Alberta Court of Queen's Bench dealt with a claim of unjust enrichment in the context of a breakdown in the relationship between the two parties. The two had lived in a common law relationship (or as an "adult interdependent partnership", to use the language of the Alberta legislation) and Rubin was claiming a share of the assets (a series of properties) that Gendemann had accumulated during the five and a half year period. Gendemann resisted the claim, arguing that Rubin had not contributed in any meaningful way and therefore that he was not unjustly enriched by her actions.

In large part the dispute centred on the credibility of the evidence of each party, and for the most part the judge found Gendemann's evidence to be more reliable and more consistent with the other evidence. Most of the dispute concerned whether Rubin had contributed in material ways to the upkeep or organization of the other properties: the trial judge found that she had not. Part of the dispute, however, concerned Gendemann's use of Rubin's email account in connection with some of the purchases or other aspects of property maintenance.

Gendemann described himself as a "luddite", did not use email, and did not have a home email account. He did have a work email address for his profession as a psychiatrist, but that was managed by his assistant. Rubin claimed that she provided critical assistance in the purchase and management of some of the various properties via her email account and email communications. Gendemann testified that all the properties he purchased came to his attention through independent means. He did use Rubin's email at home because he did not have an email account by asking her to act as a contact point in relation to a number of different issues.

The trial judge concluded from the emails that although many people communicated to Gendemann and Rubin, but that the emails did not reveal any kind of managerial function by Rubin. The trial judge concluded that this use of Rubin's email did not provide the foundation for an equitable claim: rather, it was:

> the equivalent of Rubin taking telephone messages for Gendemann, where those messages arrived at a jointly used and shared telephone number. Certainly, secretaries take and relay messages as a part of their employment, but here the 'load' on Rubin cannot elevate the joint use of her email account to anything approaching that level. The kind of activity here represents a courtesy, not some kind of professional or demanding obligation. (para 239)

E-Discovery: Data Filtering Unnecessary When Implied Undertaking Will Do

In *Animal Welfare International Inc. v. W3 International Media Ltd.*, Justice T.C. Armstrong of the British Columbia Supreme Court heard a motion by the plaintiff to settle conditions to be attached to the production of electronic documents by the defendant, and to compel other electronic documents from the defendant. In the underlying litigation, the plaintiff claimed that the defendants had failed to account for profits earned through an internet-based animal supplies company operated by both parties. On a previous motion, the Court of Appeal had upheld an order that the defendant produce customer lists for both of the business's websites, but left the conditions of production to be settled by the chambers judge. The defendant argued that the lists contained a great deal of confidential and sensitive customer information, including addresses and credit card numbers. It requested that the data be given to a technical expert who would obscure the confidential information, code the data and then produce a list of customers. This process would be paid for by the plaintiff. The defendant noted that the confidential information was not required by the plaintiff for the action, and moreover the plaintiff was a non-resident corporation with no presence in Canada; therefore, the implied undertaking of confidentiality would provide "no real protection" (para. 14).

The plaintiff responded that: the lists were the plaintiff's property in any event; the confidentiality agreement with customers specifically anticipated disclosure of information in any legal action; and its principals were professionals and would abide by the implied undertaking. Also, the lists could contain as many as 40,000 customers, and processing the data would be disproportionately expensive. Justice Armstrong observed that the privacy interests of third parties to litigation should be balanced in crafting any discovery order. Noting that he had considered both the object of the Civil Procedure Rules and the principle of proportionality in Rule 1-3(2), he ruled: "Preventing the general disclosure of sensitive information of third parties, such as addresses and credit card information, where production is not necessary in advancing the litigation, would appear to be a prudent step in protecting these interests. This may be protected by the implied undertaking. I am satisfied it is not necessary to order redacting particularly sensitive information in this proceeding" (para. 23). Nonetheless, he further ordered the principals of the plaintiff company to "sign confidentiality agreements providing for the protection of any third party information contained in the documents" (para. 24).

Google Books Settlement Rejected by New York Court

In a recent decision, Judge Denny Chin of the U.S. District Court (Southern District of New York) has rejected a settlement deal reached between Google Inc. and a large group of authors and publishers in litigation over the former's "Google Books Project." As part of the project, Google scanned millions of books which were made accessible in "snippet" form for online searching. The overall goal is to have a universal database of books in full text available on Google. While many of the scanned books were in the public domain, many were not and authors and publishers holding copyright in these works began a class action against Google. A settlement agreement was reached between Google and many of the copyright holders, which was preliminarily approved in November 2009. A "fairness hearing" was held before Judge Denny in February 2010, the legal question under the class actions legislation being whether the settlement was "fair, adequate and reasonable."

In a heavily-footnoted 48-page decision, Judge Denny concluded that the agreement could not be approved. He noted that many copyright holders had opted out of the class action and objected to the settlement agreement; also "hundreds of class members objected to the [agreement]. A few wrote in its favour. The Department of Justice ('DOJ') filed a statement of interest raising certain concerns...Amici curiae weighed in, both for and against the proposed settlement" (p. 5). Judge Denny summarized his conclusions as follows:

> While the digitization of books and creation of a universal digital library would benefit many, the [agreement] would simply go too far. It would permit this class action…to implement a forward-looking business arrangement that would grant Google significant rights to exploit entire books, without permission of the copyright owners. Indeed, the ASA would give Google a significant advantage over competitors, rewarding it for engaging in wholesale copying of copyrighted works without permission, while releasing claims well beyond those presented in the case" (pp. 1-2).

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.