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

October 4, 2007

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.

Civil Procedure: Significance of Metadata

The Ontario Superior Court of Justice has delivered its ruling on the final issue for determination in the defendant's refusal motion in *Hummingbird v. Mustafa*. The issue is in respect of question 8189 in which the defendants seek a disk image or mirror copy of Mustafa's hard drives which he used while employed by Hummingbird. The latter had already used the image of the hard drive to produce documents in their affidavits of documents and supplementary affidavits. Hummingbird opposes Mustafa's request on several grounds, including the claim that the request is superfluous and that the metadata relating to non-relevant documents are not supposed to be produced. Also, it claims that the metadata relating to some of the relevant documents in Mustafa's hard drives have already been produced. It seeks to restrict itself to the production of relevant documents and associated metadata which will not necessarily require the production of Mustafa's entire hard drives. Relying on *Reichmann v. Toronto Life Publishing* (1988), the court affirmed that under Civil Procedure Rules, document includes data and information in electronic form. It held that a disk containing an electronic version of a document that is produced in hard copy form can be required to be produced as a disk or hard drive. The court noted that information available by the possession of a disk may not be available from the product of the disk (the paper copy). On the significance of metadata, the court found that the metadata is akin to "'a time/date stamp' affixed to a letter or the 'fax header' that indicated the time/date of faxing and receipt" (¶9). It rejected the argument that the metadata was not relevant and noted that there is no evidence by the moving defendant to suggest the acceptance of the authenticity of the documents said to be located in the hard drive of Mustafa's computer. The court further found that "there may well be tests that can be taken by parties to determine whether the hard drive has been altered in any fashion that may not be readily ascertained from a hard copy of the material" (¶6).

While noting the Rules required the court to consider the just, most expeditious and least expensive determination of proceeding, the court ordered that Hummingbird has two options: (i) to reproduce the hard drive and make the same available to Mustafa, or (ii) to redact the hard drive in order to filter away any information that is not relevant and then make same available to Mustafa. The court noted that the redaction option is the most expensive even though "there is no evidence to suggest that the non-relevant documents are sensitive, confidential or prejudicial or in any way such that Hummingbird might be entitled to some form of protection" (¶7). Consequently, it ordered Hummingbird to bear the cost of redaction if it chose that option whereas, Mustafa bears the cost of reproducing the entire hard drive which is least expensive should that option be favoured.

Comment on the issues raised in this case at the It.Can Blog

Digital Number Recorder Warrants Upheld

The Quebec Court of Appeal has rejected a constitutional challenge to the digital number recorder (DNR) warrant provisions in s. 492.2 of the Criminal Code with its decision in *Cody. v. The Queen*. The accused was charged with a variety of offences in connection with a conspiracy to import narcotics into Canada through the Port of Halifax. The accused and many of his con-conspirators

worked in various capacities at the Port and arranged for cocaine to be shipped into the country in container ships. Their positions both in the head office and within the container pier allowed them to communicate with one another and arrange to take narcotics from containers and ship them elsewhere in the country. Some of the evidence against the accused was gained through the use of wiretaps, recording conversations between them. However, other aspects of the evidence came from information derived through DNR warrants.

The court described the way in which a DNR is used and the information obtained as follows:

> A digital number recorder (DNR) is activated when the subscriber's telephone is taken "off the hook". Electronic impulses emitted from the monitored telephone are recorded on a computer printout tape which discloses the telephone number dialled when an outgoing call is placed. The DNR does not record whether the receiving telephone was answered nor the fact or substance of the conversation, if any, which then ensues. When an incoming call is made to the monitored telephone, the DNR records only that the monitored telephone is "off the hook" when answered and the length of time during which the monitored telephone is in that position (para. 11).

In addition to this information, though, the trial judge had also noted that use of the DNR warrants allowed other information to be obtained about conspirators, relating to their locations. If a suspect was under physical surveillance but contact was lost, the fact that there was a DNR warrant concerning that accused's cell phone might make it possible to determine what part of the city the accused was in, so that contact could be re-established. Further, at one point information from a DNR warrant made it apparent that one conspirator was traveling from Montreal to Halifax, which allowed physical surveillance of their eventual meeting to take place.

The reason the DNR warrant provisions were challenged was that s. 492.2 of the *Criminal Code* permits such warrants to be issued not only on a lower standard than wiretaps, but on a lower standard then search warrants generally. Where a search warrant requires that the police have "reasonable grounds to believe" that evidence will be obtained, DNR warrants are available on the lower standard that "there are reasonable grounds to suspect" an offence has been or will be committed and information could be obtained through the DNR. The accused argued that this standard was too low and therefore violated s. 8 of the *Charter* forbidding unreasonable search and seizure.

The Quebec Court of Appeal rejected this argument for several reasons. First, they noted that the DNR warrant provisions had been introduced by Parliament in response to the Supreme Court of Canada's decision in *R. v. Wise*. In *Wise*, the Court had held that the police could not attach a tracking device to monitor the location of a vehicle without a warrant: however, they said that any such warrant ought to be available on a lower standard than "reasonable grounds to believe". Parliament had subsequently enacted both tracking warrant and DNR warrant provisions, basing both on that lower standard.

Further, the Quebec Court of Appeal held, the information obtained through a DNR warrant was not very intrusive on the accused's reasonable expectation of privacy. The information obtained – the general location from which it was being used or the locations being telephoned – was similar to the information obtained through physical surveillance. The accused's reasonable expectation of privacy was engaged, but this was respected by the need for a warrant at all. The fact that that warrant was available on less than reasonable grounds to believe was justified on the basis that the information obtained (which did not include who used the telephone, whether there was a conversation, or its contents) did not engage a high level of privacy protection.

Privacy Breach Regarding Collected Electronic Information

The Federal Privacy Commissioner and Privacy Commissioner of Alberta have issued a joint report of their investigation into the security, collection and retention of data by TJX Companies Inc., an international corporation which operates more than 250 Winners and HomeSense retail stores

across Canada. The company suffered a data breach late in 2006 as a result of which a great deal of information concerning customers of the stores was compromised. The breach is thought to have occurred through intruders gaining access to the data via the store's wireless local area network at two locations in the United States. The consumer information obtained consisted of credit card numbers along with expiration dates, names, addresses and telephone numbers of customers entered electronically after November 2005, and Canadian drivers' license and other provincial identification numbers with related names and addresses of customers.

The investigation focused on how the loss of information had occurred in the first place, whether TJX ought to have gathered that information, and whether it should have been retained. The Commissioners found the company lacking in all three regards.

The breach occurred despite the fact that the wireless network was protected by WEP encryption. At the time of the breach in 2006 the company was already in the process of changing to a higher encryption standard, since WEP is relatively easily bypassed. However, the Commissioners pointed out that experts (including the Institute of Electrical and Electronic Engineers, which developed WEP in the first place) had been questioning the use of WEP as a secure protocol since 2003. Accordingly they concluded that a breach was foreseeable and that TJX had not complied with the relevant safeguard standards in PIPEDA or its Alberta equivalent PIPA.

The Commissioners also concluded that TJX ought never to have collected much of the data that was lost in the first place. It was reasonable to collect credit card numbers and expiration dates, since that information was necessary to complete a sales transaction. The driver's license and other identification information, however, was only collected in connection with returns of merchandise where a customer did not have a receipt. The company argued that it was necessary to collect unique identifier data along with returns, in order to keep track of "frequent returners" and to protect against fraud. They also argued that collecting this personal information along with providing notice to the returner that additional returns without receipts might not be accepted from a particular individual had a deterrent effect.

The Commissioners acknowledged that the purpose of deterring fraud during the return of goods justified the collection of reasonable information such as names and addresses. However, they held that here TJX was collecting more information than was reasonable. They noted:

> 42. A driver's license is proof that an individual is licensed to operate a motor vehicle; it is not an identifier for conducting analysis of shopping-return habits. Although licenses display a unique number that TJX can use for frequency analysis, the actual number is irrelevant to this purpose. TJX requires only a number—any number—that can be consistently linked to an individual (and one that has more longevity and is more accurate than a name and telephone number).
>
> 43. Moreover, a driver's license number is an extremely valuable piece of data to fraudsters and identity thieves intent on creating false identification with valid information. After drivers' license identity numbers have been compromised, they are difficult or impossible to change. For this reason, retailers and other organizations should ensure that they are not collecting identity information unless it is *necessary* for the transaction.

Accordingly they held that collecting this particular information was not justified.

The third issue related to retention of the data. TJX indicated that it retained the data it collected indefinitely. With regard to the identification information collected, the Commissioners noted that as it ought never to have been collected, retention was also not reasonable. However, TJX had proposed an alternative scheme whereby it would continue to collect driver's license information but immediately convert it through a cryptographic hashing program into a new number, referred to as a "hash value". Storing only this hash value would mean that the actual driver's license number was no longer readable by any TJX employee, but it would still serve as a unique identifier number. TJX proposed to retain those numbers for three years. The Commissioners agreed that this would comply with the legislation

provided the method of encryption met the highest level of industry standards. The Commissioners also agreed that credit card numbers could be retained for the length of time specified in the company's contracts with financial institutions, since this fell under "legal or business purposes". However, retention of information for "troubleshooting" purposes was not justified.

Sentencing: Criminal Sanction for Internet Defamation

The Ontario Superior Court of Justice has delivered its ruling in *Beidas v. Pichler*. In that case, the plaintiff sued the defendant, Pichler and others on allegation of on-line defamation. The defamatory material allegedly impugned the efficacy of transgender surgery which the plaintiffs received by way of therapeutic intervention for medically diagnosed gender identity disorder. One of the plaintiffs, Davis, was Pichler's former physician. Earlier in the proceedings, the plaintiffs obtained an order restraining Pichler from continued publication and dissemination of the offensive materials. It is the case of the plaintiffs that the defendant was in violation of that restraining order in its subsequently varied form which narrowed the application of the order to "prohibition from publishing any materials which may tend to identify the plaintiff". Meanwhile, the defendant's appeal from this varied order was pending at the time of the present proceeding. Specifically, the defendant, Pichler, is alleged to have sent an e-mail to 11 individuals that violated the terms of the varied restraining order. That e-mail referred to the plaintiffs by name and contained information that they claimed to be false. In moving for Pichler to be cited for contempt, the plaintiffs have served four individuals with summonses to witness in support of the contempt motion. Apart from securing the subsisting injunction, the plaintiff filed a complaint for criminal harassment against Pichler for which he was arrested and subsequently charged on five counts. He was however entered into a recognizance of bail subject inter alia to a term of publication prohibition in the terms of the restraining order. Shortly, the criminal charges were withdrawn in exchange for Pichler entering a peace bond. Following this development, the defendant sent an e-mail to 11 identified individuals wherein he narrated the history of the criminal charges and concluded that "there was little evidence to support the allegations of harassment and [the Crown] was of the opinion that the matter should not be prosecuted further" (¶ 9). The plaintiffs argue that that this offensive correspondence was in contempt of court order. Among other things, they seek to have Pichler incarcerated for alleged breach of a court order in the substantive civil proceedings.

In his defence, Pichler argues that upon the termination of the criminal proceedings all he wanted to do (and actually did) was "to notify his friends and clients about how things turned out; that he did not view what he was doing as "publication" and that he does not believe that he breached the order" (¶13). The court found that the success and failure of the contempt motion will turn on how it (the court) interprets the restraining order; specifically on whether the order encompasses the conduct of the defendant and what he intended and did not intend when he sent the e-mail. The court also found that in order to assist it in making such determination, the onus is on the party who has served the summonses and not on the party moving to quash them to prove that the witnesses summoned will offer relevant evidence. Here the court noted that the proceeding for which evidence is sought is the contempt motion and not the defamation action. Thus, "the test for contempt requires the moving party to show beyond reasonable doubt that the order was personally served and the party who contravened the order intentionally committed the act" (¶19) prohibited. The court expressed a reservation over the plaintiffs' inclination for criminal sanction given that the case involves "private dispute between private individuals". Moreover, it noted that "[n]o evidence was tendered to demonstrate that the e-mail has been disseminated by any of the recipients in a more public way or that any of them has sought to publish the content of the e-mail in a more general way" (¶24). After examining the four summoned witnesses, the court held that the plaintiffs failed woefully to establish the relevance of their evidence to the issue before the court, namely whether the defendant's e-mail amounted to intentional public defiance (of a criminal nature) of the court order in issue to warrant the sanctions sought by the plaintiff in this case.

Taxation and Computer Law: Production of Information

The Federal Court sitting in Toronto had delivered its ruling in *eBay Canada Ltd. v. Canada (Minister of National Revenue)*. In this case the applicants, eBay Canada and eBay CS Vancouver Ltd. applied for the review of an *ex parte* order that required them to provide the Minister with certain documented information for persons having a Canadian address in the applicants' record. The targets were members of the eBay community who qualified for the applicants' Canadian PowerSeller program in 2004 and 2005. The relevant pieces of information, which were required in their original forms, included those that dealt with accounts and merchandise. The crux of the appellants' case is that even though they have access to the requested information in Canada, they neither owned nor possessed in Canada or elsewhere any such information relating to the PowerSeller program. They maintain that such information was held in computer data facilities outside Canada, especially in San Jose, California. According to them, the ownership of the information resided with the US eBay Inc and eBay AG, the Swiss company, which is the wholly owned subsidiary of the US umbrella company. The key issue for determination was whether s. 231.2 of the *Income Tax Act* allowed the making of an order requiring the applicants as Canadian residents to make available to the Minister information to which they have access in Canada even if it was electronically stored in facilities owned by parties located outside of Canada.

In answering this question in the affirmative, the court held the approach of strictly construing tax statutes must be substituted with a modern approach to statutory interpretation which gives regard to reasonableness in regard to the statutes object and purpose. In this regard, the court took into consideration the fact that s. 231.2 was enacted in response to the court's restriction of the previous provision on Minister's access to information relevant to tax liability to only specific individuals. It held that the section is directed at permitting the Minister to engage in a fishing expedition and to broadly require "any person" to provide "any information" in so far as such information related to the administration and enforcement of the *Act*. The court noted that in the past, a bank manger located in Canada has been required to divulge information about a Canadian tax payer in the Bahamas which was lodged in the bank manager's memory (*R v. Spencer, 1985)*). Consequently, there is nothing spectacularly different as to "the reach of s. 231.2 when information, though stored electronically outside Canada, is available to and used by those in Canada" (¶23). In the court's opinion: "[F]rom the point of view of the realities of today's world, such information cannot truly be said to "reside" only in one place or be "owned" by one person. The reality is that the information is readily and instantaneously available to those within the group of eBay entities in a variety of places … [the information] is 'both here and there'"(¶23).

Comment on the issues raised in this case at the It.Can Blog.

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.