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

September 8, 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.

E-Discovery: Dealing with "Over-Disclosure"

In *Pro-Sys Consultants Ltd. v. Infineon Technologies AG*, Justice D.M. Masuhara presided over a chambers motion regarding electronic and documentary discovery. The underlying litigation was a class action over an alleged international price-fixing conspiracy by the five defendants. Two recent decisions by the British Columbia Court of Appeal had changed the law so that it was possible that some part of the plaintiff's claims in this case could be struck. The two appellate decisions were under pending leave applications to the Supreme Court of Canada and the defendants had moved for a "pause" in the action while these leave applications were determined, since the outcome of the leave applications and potential SCC decisions could greatly affect the instant case. On a cross-motion, the plaintiff argued that the defendants had not properly provided their lists of documents and, to the extent they were provided, they were not properly searchable. The parties had been negotiating and working together in the background, attempting to iron out various problems with the e-discovery aspects of the case, but there had been no agreement between the parties under BC's *Practice Direction re: Electronic Evidence*. The defendants had provided their documents on a hard drive provided by the plaintiff and did so using the Summation litigation software as the plaintiff had requested. The total documentary disclosure was something in the order of 1.8 million pages.

The plaintiff identified numerous problems with each defendant's disclosure, but the heart of the argument was that the defendants had provided "a data dump" rather than a deliberate selection of relevant and non-privileged documents. Some documents were under-described, some incomplete and/or lacking attachments, some lacking metadata, some duplicative. An affidavit by the plaintiff's Summation litigation support consultant described one defendant's disclosure as "by far the worst case of a complete mess of a production" that she had seen in her 13 years' experience. The plaintiff also noted that some of the disclosure had originated from related litigation in the US and argued that this was partly responsible for the problems, in that too much reliance was being placed upon the US attorneys and paralegals. The plaintiff argued "that counsel having conduct of the case before this Court must lay eyes upon each document that is in the hands of their respective defendants to ensure that what is produced is consistent with the Rules" (para. 24), and asked for various means of better disclosure of documents.

Many of the defendants did not generally contest the plaintiff's characterization of their disclosure but argued that it was adequate and that they were still working to improve it. Some attributed the size of the disclosure to the breadth of the plaintiff's requests, while others noted that some of the problems the plaintiff noted could be solved by using mechanisms within Summation itself. They further argued that the proportionality principle in Rule 1-3(2) of the BC Rules of Civil Procedure "warrants some leeway in their disclosure requirements" (para. 27), as did the need for a litigation pause to await the SCC applications. The cost of full compliance with the plaintiff's requests ranged by defendant from tens to hundreds of thousands of dollars.

In his decision, Justice Masuhara held that the pending SCC decisions were a significant factor in how an order should be shaped: "In the absence of these two decisions, the requirements on the defendants to meet the specifications for disclosure would be more acute. In balancing the interests requiring the defendants to incur the costs of

conducting all of the additional work requested by the plaintiff *at this stage* is not warranted" (para. 41, emphasis in original). This was supported by the fact that there were Summation features that could solve some problems, that some of the defendants had carefully considered relevance in their disclosure, and that the defendants were undertaking to have their technical staff continue to work with the plaintiff's technician to problem-solve. One defendant was ordered to provide OCR text files to the plaintiff, a practice the judge described as "common for disclosing parties." Another defendant was ordered to provide descriptions with regard to its two sets of disclosure, the court remarking "It is not an answer to say that because the documents do not contain metadata a proper list cannot be produced or to say that a proper list is not required because the documents are OCR readable" (para. 43).

Justice Masuhara rejected the plaintiff's argument that counsel for the defendants must lay hands upon and review every document disclosed. While emphasizing that counsel was responsible for the disclosure and would be held to the usual standards of professional responsibility and diligence, requiring full duplication of effort would be inefficient and not in keeping with the principle of proportionality. However, the evidentiary record did not adequately describe the oversight that present counsel had exercise in relation to the production made. "As a result, defence counsel are directed to provide a detailed description of their own assurance measures taken, such as instructions given to those relied upon, oversight employed, reviews of relied upon counsel's methods, and verification methods used, to ensure that the rules of this Court have been properly communicated and applied in the disclosure relied upon" (para. 47).

Electronic Record Evaluation by Revenue Canada

The British Columbia Court of Appeal has granted leave to appeal in a case considering the extent to which Revenue Canada officials are entitled to engage in electronic records evaluation under their audit powers, in *R. v. He*. The three accused ran a restaurant called Sushi Man, whose records were examined by Revenue Canada. The examination was part of the "Electronic Records Evaluation Pilot Project", which was being conducted by the office's Electronic Commerce Audit Specialists. The Pilot Project focused on restaurants, convenience stores and small supermarkets which met particular criteria and were in prescribed locations in Canada. Sushi Man's business records were seized, copied and reviewed by CRA officers in accordance with the "research survey project", which resulted in criminal charges being laid.

The trial judge found that this seizure of Sushi Man's record was not authorized by the statute and therefore that the search violated the section 8 right of the accused. The trial judge excluded the evidence and therefore acquitted the accused. This decision was upheld on the first level of appeal, and the Crown sought leave to appeal to the British Columbia Court of Appeal.

The trial judge had relied on authority governing section 231.2 of the *Income Tax Act* which holds that Revenue Canada may only be undertake an examination of a taxpayer's records in furtherance of a "genuine and serious inquiry" into the tax liability of a particular individual. In the case in question, however, Revenue Canada had been proceeding under its powers in section 231.1 rather than 231.2. The appeal judge had acknowledged this but had concluded that the same requirement applied. The appeal judge held that section 231.1 was more intrusive than section 231.2, and therefore that the same requirement should apply. In addition it was held that Revenue Canada could simply require a taxpayer to produce its books and records for inspection under s. 231.1 and achieve the goals of 231.2 as a way of avoiding the "genuine and serious inquiry" requirement if the same condition did not apply to both.

The British Columbia Court of Appeal granted leave to appeal. They noted that the test for leave was that (a) the error alleged is a question of law, (b) the issue raised is one of importance, and (c) the appeal has a reasonable possibility of success. The issue in the case was one of statutory interpretation, which was a matter of law, and there was a reasonable possibility of success. With regard to the importance of the issue, the Court of Appeal held:

> It is also my view that what might be considered the routine use of electronic

> technology employed in tandem both as a means of monitoring compliance with a self-reporting tax system and as a means of securing evidence for criminal prosecution has ramifications that engage the interests of justice, including the privacy interests that underpin s. 8 of the *Charter*. (para 14)

Internet Child Pornography Sentencing Factors

The Newfoundland Court of Appeal has given some direction relative to sentencing in internet child pornography cases with its decision in *R. v. Johnston*. Following a national investigation of internet protocol addresses through which child pornography images were shared, the accused's IP address had been identified as a candidate for suspected child pornography files over one hundred times. The police obtained a search warrant, as a result of which the accused was found to be in possession of twenty child pornography videos. The accused pleaded guilty to a charge of possession of child pornography and received a sentence of 15 months incarceration, along with other conditions. The accused appealed his sentence, holding that the trial judge had improperly considered some factors to be aggravating and therefore had erred in principle in imposing sentence. The Court of Appeal granted the appeal.

One of the factors the trial judge had taken to be an aggravating factor was "the nature of the crime itself which involves the victimization of children and the utter destruction of their lives": the Court of Appeal held this was an error. For something to be an aggravating factor in a particular case, they held, there must be other cases in which it was not present. That could not be the case with regard to the nature of the offence, which established the appropriate range of sentences, but could not be considered aggravating.

The trial judge also erred in taking the fact that the accused was a retired police officer into account as an aggravating factor. The Court of Appeal concluded that present employment or even recent retirement as a police officer could be aggravating. Here, though, the accused had retired 17 years previously after an exemplary 30 year career, and so his former employment was not an aggravating factor.

In considering a fit sentence for the accused, the Court of Appeal compared the facts of the case to other child pornography sentencings. Among the factors they considered relevant (either by way of similarity to or difference from other cases) was that the accused had downloaded free videos rather than paying for them and so had had no part in "feeding the international market in child abuse" (para 48). They also took into account the relatively small size of the accused's collection and the relatively less depraved nature of the content, which involved no violence other than that inherent in the sexual activity itself. In light of the various mitigating factors, the Court of Appeal concluded that a sentence of 10 months was appropriate.

Online Banking Security

The United States District Court of Maine has considered the level of security which must be provided by banks in connection with electronic banking (under the *Uniform Commercial Code* (UCC) of the United States) with its decision in *Patco Construction v. People's United Bank*. Patco used the electronic banking services of the bank and had signed a user agreement in that regard. Over a period of roughly a week, someone made a series of unauthorised withdrawals from Patco's account. These withdrawals totalled $588,851, though the bank succeeded in blocking $243,406 of this amount.

Under the UCC Patco, rather than the Bank, would be required to bear this loss if it were shown that: (i) Patco and the Bank had agreed to a security procedure; (ii) that security procedure was commercially reasonable, and; (iii) the Bank accepted the payment orders in question in good faith and in compliance with the security procedure and any relevant written agreement or instruction of Patco. The largest issue in the case was whether the second criteria was met: were the bank's security procedures reasonable? The judge concluded that they were, and therefore that the bank was not liable for the loss.

The bank's security procedures for online banking consisted of several features. It required the use of customer IDs and passwords as well as individual user IDs and passwords, in addition to challenge questions which could be triggered in various ways. Further the system monitored the IP address from which transactions were initiated and purported to

monitor other aspects of the behaviour of the user. The system was meant to monitor what the user knew, what the user had and what the user was.

The system generated a "risk score" for each transaction. Prior to the fraudulent transactions all risk scores for Patco's transactions had had scores between 10 and 214, a higher score indicating a higher risk. The fraudulent transactions all attracted scores in the 700s, which were considered high risk. The bank was capable of manually checking transactions which had high risk scores but did not at the time do so. It was only when some of the transferred money was returned because it had been sent to non-existent accounts that the bank notified Patco, at which point Patco indicated that it had not authorised the transactions. In each case, however, the transaction had been made by someone who had the customer ID and password, a correct user ID and password, and who correctly answered all the challenge questions which were posed.

There was some dispute over how the transactions came to be made and the point was not settled, but the likeliest explanation seemed to be a key-logging program on Patco's computer which had detected the necessary information.

Patco argued that the bank's security procedures were not reasonable for several reasons. First, it argued that the bank ought to have manually checked high risk transactions, rather than simply have them trigger challenge questions. Further, Patco argued that the bank had acting unreasonably in setting a dollar limit for when challenge questions were asked. Through the relevant time period, the limit which would cause a challenge question to be asked was $1: in other words, challenge questions were asked for every transaction.

Patco argued that this was unreasonable for two reasons in particular. First, it effectively neutralized other aspects of the bank's security system. If the only effect of finding a high risk transaction was to trigger the use of a challenge question which would inevitably have been asked in any event, then detecting high risk transactions was purposeless. Second, Patco argued that setting such a low dollar limit increased the frequency with which users were required to enter the answers to challenge questions, which increased the likelihood that malware would detect those answers.

The judge agreed that checking high risk transaction manually rather than simply having them trigger challenge questions would have been better, but held that that was not the question: the bank only needed to have behaved reasonably, which it had. The judge also noted that the default setting for challenge questions was $1000, and that even if that setting had been left in place Patco would have been required to answer them for virtually every transaction it conducted. Indeed, even if the dollar limit had been set at $16,000 the challenge question would have been asked almost every time.

The judge also noted that Patco had agreed, under the terms of service, to monitor its accounts daily, which was part of the security procedure adopted by the bank. Patco had not done so, and indeed had logged in to its account six times during the week in which the fraudulent withdrawals were being made without detecting them. In the end the steps taken by the bank were not optimal but were reasonable, and so they were not liable.

Domain Name Decisions

"bellapierre.ca"

In *Excite Group Inc. v. Zucker International Marketing Inc.*, a 3-member CIRA panel (Cooke, Freedman and Wotherspoon, Chair) heard a dispute over the domain name bellapierre.ca. The Complainant ("Excite") is a California-based company which manufactures and sells mineral-based cosmetics in Canada and the US. It owns the CIPO-registered trademark BELLA PIERRE, pursuant to its application for registration in January 2010 and actual registration in March 2011. The Registrant ("Zucker") is a Toronto-based company which formerly was a distributor of Excite's products. It registered the domain name in October, 2006.

The Panel first noted a procedural issue which had arisen early in the proceedings. On 27 June 2011 the Panel had received an "unsolicited" letter containing further arguments and accompanying draft affidavit from Excite. The deadline for filing submissions had passed, but Excite noted that it would file the affidavit as additional evidence if invited to do so by the Panel, a discretionary decision which is provided for under 11.1 of the CIRA Domain Name Dispute Resolution Rules. Zucker sent an unsolicited letter

of objection. The Panel noted 1.1 of the CIRA Policy which states its own purpose to be resolution of disputes "relatively inexpensively and quickly," and decided that, "in the circumstances" it would not invite either party to submit additional evidence or argument, and would not consider Excite's material.

The Panel then turned to what it characterized as the dominant issue, which was whether Excite had rights in the relevant trademark prior to the registration of the domain name; as its CIPO registration of the mark antedated the registration of the domain name, the complaint could only proceed if it had been using the mark in association with wares, services, business or a non-commercial activity before October 2006 (Policy 3.3 and 3.5). Excite's Complaint stated that the mark had been used in Canada since August 2006, and the affidavit of its CEO reiterated this statement. Excite had also filed a printout from CIPO indicating that Excite claimed to have been using the mark in Canada since 2006. Zucker did not file any evidence in response but argued that Excite's "bald assertions" did not constitute evidence of use that would satisfy its onus to produce "evidence of use." The Panel ultimately accepted Zucker's argument on this point:

> A simple assertion by a complainant that it has carried on business under a trade-mark or has used a trade-mark in commerce, without details regarding the specific manner in which the trade-mark was used in association with wares, services or a business, is not sufficient, because it does not allow the Panel to make a finding of fact that the trade-mark was "used", as that term is defined in Policy paragraph 3.5. (para. 33)

Accordingly, transfer of the domain name was denied and the Complaint dismissed.

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