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

February 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.

E-Discovery: ISP and Facebook Disclosure Granted

In *Carter v. Connors*, Ferguson J. of the New Brunswick Court of Queen's Bench heard a motion to compel a plaintiff to disclose her home internet use history. In the underlying action the plaintiff had sued the defendant in 2006 for personal injury sustained in a car accident in 2004. She was employed as an administrative clerk at the local hospital, but claimed that she was unable to return to work full time because of the soft tissue injuries she had suffered in the accident. While the plaintiff was being discovered by defendant's counsel, she disclosed that she had a home internet account with Bell-Aliant as her ISP and that she maintained a Facebook profile. Defence counsel then requested an undertaking that records of the plaintiff's internet usage be disclosed (specifically, it appears, the time spent using the internet), from the date of the accident forward. Plaintiff's counsel refused on the basis that the request constituted an invasion of the plaintiff's privacy. Defence counsel made a motion to have the records disclosed and further requested that the disclosure isolate the time the plaintiff spent on Facebook. The plaintiff resisted the motion on the basis that the records were not relevant and on the privacy argument.

Justice Ferguson first reviewed the general law regarding relevancy of evidence, citing leading jurisprudence to emphasize that the relevancy of particular evidence is a function of its relationship not only to the material issues in the case but also to the other evidence. However, since at any stage in a case the potential for relevance may depend upon other evidence which will be adduced later in the proceeding, the threshold for relevance is necessarily a low one. His Lordship then noted that the relevant New Brunswick Rules of Court regarding discovery contain the obligation to disclose anything "which relates to the matters in question," and reviewed the leading cases of the New Brunswick Court of Appeal on the scope of relevancy in the discovery context. This caselaw emphasized that, given that the rationale behind discovery was to avoid trial by ambush and allow each side to ascertain the other's case—in order to drive the potential for settlement—the threshold for relevancy was necessarily a modest one. Distilling the authorities, Ferguson J. concluded:

> Thus, the touchstones for relevancy determination at the discovery stage are: 'a semblance of relevancy' or that: 'the answer may lead to the discovery of admissible evidence.' It is thus clear that the common law admissibility requirements of relevancy in the trial context have been further reduced at this early point in the proceedings (para. 25).

Turning to the issue of privacy, Justice Ferguson noted that while the *Charter*-based right to privacy is not directly applicable in civil proceedings between private parties, the Supreme Court of Canada has directed that the common law should develop in accordance with *Charter* values. This made privacy, and a reasonable expectation thereof in a core of biographical information, relevant in civil cases, though the law that arises from the general foundational principles is shaped differently in this context. Reviewing a number of reported chambers decisions regarding disclosure of computer, internet and Facebook use, he remarked:

> It is clear from these judgments that the success of an application to retrieve an individual's electronic computer data principally depends upon the degree of intrusion into the private lifestyle choices and electronic activity of the Internet user as well as the probative values of the information sought. … A separate issue concerns the

likelihood that third party privacy rights may be affected by any disclosure. Third party privacy rights are to be given special attention when those third parties are not parties to the legal proceedings (paras. 36-37).

Turning to the motion, Justice Ferguson ruled that the requested information met the "semblance of relevancy" test "by possibly providing a window into what physical capacity the Plaintiff has to keyboard, access the Internet and communicate with family friends and associates on Facebook and thus what capacity she may have to work. In that sense: "It may lead to the discovery of admissible evidence", the threshold required for the evidence to be produced" (para. 40). Moreover, the scope of the actual request did not threaten to reveal intimate lifestyle details. However, he stated: "If the questioning attempts to delve deeper into the Plaintiffs lifestyle as it pertains to these subjects, relevancy and privacy, it will require a re-examination of the reasonable limits of such questioning. For example, included in that assessment will be the extent to which an individual may claim a reasonable expectation of privacy in the use of social networking site electronic data" (para. 39). The finding was further buttressed by the fact that, having launched the proceeding, the plaintiff had essentially consented to intrusions into what would otherwise have been her private information, and that her overall privacy was protected by the implied undertaking of confidentiality. Moreover, the defendants had agreed to pay the costs of the disclosure. The motion was granted.

Mutual Legal Assistance: Seized Images of Hard Drives Sent to France

In *Attorney General of Canada (France) v. Tfaily*, the appellant obtained leave to appeal the order of Ontario Superior Court of Justice that electronic images of the hard drives of two computers seized from her be sent to France. The computers were seized in accordance with warrants obtained under s.12 of the *Mutual Legal Assistance in Criminal Matters Act* R.S.C. 1985 C. 30, s. 12(1). According to the appellant, the warrants could not have been issued for want of reasonable and probable grounds. The appellant argues that there was no evidence that her common law spouse, Mr. Diab, was communicating via e-mail with other suspects regarding a plot to blow up a Paris synagogue. Disagreeing with the appellant, the court held the appellant already conceded that her common law spouse was part of a terrorist plot. The court held that given the surrounding circumstances, including but not limited to the spike in communication between Mr. Diab and his ex-wife who was associated with a terrorist group responsible for the attack and given that "he was taking steps to have some of his communications go undetected", there was a reasonable basis for the judge to conclude "that there is practical and reasonable probability that Mr. Diab was in communication by e-mail with other members of the terrorist plot" (para. 3). On the appellant's contention that there were insufficient grounds that Mr. Diab may have been communicating through the appellant's seized computer, the court disagreed. It held that the evidence that "Mr. Diab and the appellant lived together at the residence from where the laptop was seized, that they both taught at the same university where the second laptop was, that the appellant had an office in the building there, that Mr. Diab had been seen leaving the building" … provided sufficient basis for the order made by the issuing judge (para. 5).

Domain Name Disputes

In *Canadian Security Association v. 1687734 Ontario Inc. o/a Trademark Protection*, a 3-member CIRA panel (Groom, Josefo and Scassa, Chair) heard a dispute regarding the domain name canasa.ca. The complainant ("CSA") is a Markham, Ont.-based non-profit organization which advocates for suppliers of commercial and residential alarm systems, and is also engaged in analysis, education and research relating to the alarm and security industry. It registered the mark CANASA with CIPO in 1998, and it provided evidence that it has used the mark CANASA in Canada since 1976. It registered the website canasa.org in 1996 and operates this site as part of its business. The registrant ("Trademark") is a Hamilton, Ont.-based company, which registered the domain name on 1 June 2005.

The registrant requested and received an extension of the time period in which it was required to file its response to the complaint; however, when the

response was received it was not in compliance with the CIRA Domain Name Dispute Resolution Rules (the "Rules"). Specifically, the response failed to indicate either contact information or a preferred method of communication (Rules 5.2(a) and (b), respectively), and also failed to certify that the information in the response was complete, accurate and in good faith, and that it was willing to submit to the jurisdiction of a provincial superior court in the event of a dispute (Rule 5.2(i)). Despite being informed of and attempting to correct some of the deficiencies, Trademark never provided the certification required by Rule 5.2(i). The Panel characterized this as "not merely technical..." but "a substantive element of non-compliance" (para. 9). Accordingly, under Rule 5.6 the Panel decided the dispute on the basis of the complaint only.

The Panel turned first to the issue of whether the domain name was "confusingly similar" to a mark in which CSA had rights, per 3.1 of the Policy. It observed that, considered without the .ca suffix the domain name was identical to CSA's mark. It noted: "Since CANASA is a coined word that has been used by the Complainant since 1977, the Registrant's use of an identical mark in its domain name is likely to be mistaken for the Complainant's mark" (para. 23). Turning to the issue of whether Trademark had "no legitimate interest" in the domain name per 4.1(c) of the Policy, CSA had produced evidence that the website in question, while currently parked, had previously resolved to a pay-per-click site, which had links related to various aspects of CSA's business, including "Home Security Systems" and "Home Alarm System." There were also links which actually used CSA's company name, such as "Join Canasa" and "Canasa Members." The Panel held that none of the criteria for legitimate interest had been met: Trademark had not been licensed to use the Mark; the domain name was a coined word which was neither descriptive of goods and services nor generic; there was evidence that Trademark had used the website to divert users searching for CSA's site to Trademark's site; and the domain name was neither a legal name of Trademark's business nor a relevant geographical name. The Panel therefore ruled that, in accordance with the applicable standard of proof, CSA had produced "some evidence" to ground a finding of no legitimate interest.

The Panel finally turned to the issue of whether the registration had been made "in bad faith" per 3.7 of the Policy. On the evidence the Panel was able to reach the conclusion that the domain name had been registered for the purpose of preventing CSA from registering its mark as a domain name, and that Trademark had engaged in a pattern of such behaviour, per 3.7(b) of the Policy. This was grounded on CSA's evidence that Trademark owned a large number of .ca domain names that contained third party marks, such as eatons.ca and antiqueroadshow.ca, as well as evidence that Trademark's contact person, Lofaro, was the director and founder of a company that had been ruled in 2006 to have engaged in registering domain names in bad faith. The Panel also found, per 3.7(c) of the Policy, that registration had been done primarily to disrupt the business of CSA, as a competitor of Trademark. The Panel noted that a finding of intention to prevent registration under 3.7(b) was not mutually exclusive of, and in fact could be used to support, a finding under 3.7(c). The kind of confusion created by Trademark's website was "clearly disruptive of the Complainant's business, as it is a scheme that necessarily trades upon the goodwill in the targeted company's Mark" (para. 47). Trademark was clearly a competitor of CSA, given that the website in question both contained information that could lead users to think they were on CSA's website and attempted to divert users trying to find CSA to other websites, on a pay-per-click basis. Accordingly, bad faith had been made out. The domain name was ordered transferred to CSA.

Italian Google Video Convictions Rattle Internet Platforms

A Milan court in Italy has convicted three Google officers and acquitted one over a controversial 2006 internet video posting on Google Video. The video was posted just before Google acquired YouTube, and showed a teenager with autism being bullied by four students in front of more than a dozen others. According to the Prosecutors, Google did not have adequate content filters or enough staff to monitor videos. They also contend that by not preventing the content from being uploaded without the consent of the parties involved, Google broke Italian privacy

law. Before Google pulled down the video following complaints, the video remained online for several months. Google led evidence to show that Google Video was controlled in the US but that it promptly removed the video as soon as its attention was drawn to it. The four students implicated in the posting were disciplined by expulsion from the remaining academic year by their school in Turin. Although the victim was later to withdraw his complaint, the City of Milan proceeded to launch a civil action with a Down's syndrome advocacy group.

According to a BBC report, the prosecution argued that allowing the video to be posted violated Italian law. The charges against the officer included defamation and privacy violations. The officers were convicted of the latter charges and absolved of the former. They were given six-month suspended sentences. Google is poised to appeal this decision which has rattled and outraged most in the internet community. Google's chief legal officer is quoted as to have indicated that he "intend[s] to vigorously appeal this dangerous ruling [and that] It sets a chilling precedent". According to him, "If individuals like myself and my Google colleagues who had nothing to do with the harassing incident, its filming or its uploading onto Google Video can be held criminally liable solely by virtue of our position at Google, every employee of any internet hosting service faces similar liability". Similarly, a privacy counsel at Google, Peter Fleischer, casts the ruling as a threat to many internet platforms which may not be able to continue if the decision is not upturned. Fleischer is quoted by the BBC as saying that "I realise I am just a pawn in a large battle of forces, but I remain confident that today's ruling will be overturned on appeal".

Hearsay: Data Analysis of Forensic DNA Expert

In *R v. Tapper*, the accused was charged with multiple counts under the *Criminal Code*, including in particular sexual assault pursuant to s. 271(1) of the *Code*. The complainant, a 13 year old girl at the time of the alleged offences, testified with other prosecution witnesses, that the accused dragged her to the woods near a common hangout in the neighborhood around 1pm on July 26, 2008 and raped her. The police examined the complainant's denim jeans for semen as well as her vaginal and buccal swab as part of their protocol for biological materials. Even though the virginal swab contained no semen, traces of semen were found in the denim jeans after a preliminary testing. The material was subsequently sent to police analytical unit for further examination.

As a result of the DNA profile of the samples obtained from the complainant, a search warrant was issued pursuant to which known sample of the accused's blood was obtained. Through uncontroverted evidence, the prosecution established that all the protocol for the handling of the biological samples and conduct of required tests were followed by very experienced police personnel some whom collected, labeled, processed and analyzed the exhibits before they were turned over to the DNA forensic specialist with the RCMP crime lab in Ottawa. None of those personnel or analysts testified at the trial. But a forensic DNA specialist, Ms. Celestine, whose job does not involve personally dealing or touching the exhibits except to analyze the data sent to her by the analysts, did testify as an expert witness. This particular specialist previously performed the task of analyst and directly dealt with biological materials while conducting DNA testing. Before her current position, she was also involved in developing the protocols used in the RCMP crime lab in Ottawa for the analysis of DNA. Even though she did not at any time supervise any of the work done by the analysts whose data she analyzed in the present case, she testified that she had confidence in their work. The court noted that "she is satisfied that the DNA extracted from the jeans of S.M. [the complainant] matched the DNA from the blood sample of Grant Tapper [the accused] to an accuracy of one in 22 trillion" (para. 41).

For the purpose of this report, the defence case is that the forensic DNA expert's evidence is hearsay and should not be given weight. According to the defence, the expert relied on data not created by her but by other technical analysts who simply fed their electronic data to her computer. Agreeing in part, the court held that "[c]learly, the fact that the final report of Ms. Celestine [the forensic DNA expert] was based on the data she received from analysts and is therefore technically hearsay is not itself an automatic bar to its reliability" (para. 108). In rejecting the defence contention, the court found

that the status of Ms. Celestine as an expert is not contested and noted that "[t]he test here on the reliability of DNA evidence is the civil standard of 'balance of probabilities' and I am satisfied on that basis that the DNA results forming the report of Ms. Celestine is reliable and is permitted to be received as one piece of evidence in this case" (para. 118). Accordingly, the court held further that despite the standard of balance of probabilities, it "must consider the criminal elements in this case as the whole of the evidence beyond reasonable doubt and not on one piece of circumstantial evidence such as DNA alone." (para. 102).