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

October 30, 2008

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.

Domain Name Decisions

"endermowear.ca"

In *LPG Systems S.A. v. Distribution4web*, sole CIRA panellist Myra Tawfik considered a dispute over the domain name endermowear.ca. The Complainant ("LPG") is a company based in France which deals in products and services relating to beauty, fitness and health care. It has a Canadian market and has registered in Canada the trademarks ENDERMO, ENDERMOLOGIE and ENDERMOTHERAPIE. It also has a pending application to register the mark ENDERMOWEAR, relating to a new line of bodysuits. The Registrant ("Distribution") carries on business in Montreal, offering products and services similar to that of LPG. It had previous dealings with LPG, at one point having tried to become an authorized Canadian distributor of LPG's products but having been refused. It registered the disputed domain name in February, 2007. Distribution had some correspondence with the Panel, but ultimately did not respond to the complaint.

Panellist Tawfik first considered the requirement under 4.1(a) of the CIRA Policy that a Complainant prove that the disputed name is "confusingly similar" to the Complainant's mark. She found that: "ENDERMO is a coined word and is an inherently distinctive trademark. The domain name incorporates in whole the Complainant's Mark ENDERMO and adds the descriptive word 'wear' at the end" (p. 5). Since LPG and Distribution dealt in similar products and services, an internet user could easily be confused into thinking that LPG and the domain name were associated. In ruling that confusing similarity had been made out, she also accepted as persuasive (though not binding) the fact that Distribution's applications to registered the mark "ENDERMOWEAR" with both CIPO and the US Patent and Trademark office had been refused, because the proposed mark was confusing with LPG's mark "ENDERMO."

The Panelist then considered whether the registration was made "in bad faith," under 4.1(b) and 3.7 of the CIRA Policy. She noted that Distribution had caused the disputed domain name to resolve to a website which offered products for sale that were in direct competition with LPG. She further found that Distribution was aware of LPG's marks prior to registration of the domain name, and had in fact acknowledged on its own site that "ENDERMOLOGIE" was LPG's registered trademark. Moreover, LPG had been using "ENDERMOWEAR" as an unregistered mark since 2002 and Distribution had not opposed its application to register the mark. She held that the purpose for this was the disruption of LPG's business, which constituted bad faith under para. 3.7(c).

Finally, Panelist Tawfik turned to whether LPG had provided some evidence that Distribution had "no legitimate interest" in the domain name, under 4.1(c) and 3.6 of the Policy. She easily found that none of the criteria for good faith could be made out in this case: "The Registrant had no right in the Marks at the time of registration of the domain name, it was not acting in good faith in registering the domain name and it is making a commercial use of the domain name. Finally, the domain name is not the legal name of the Registrant nor is it the geographical name of the location of its business" (p. 7). The disputed domain name was ordered transferred to LPG.

International Cases of Interest: Does Providing Computer Password Constitute Admission of Guilt?

In *R. v. S. and A.*, the England and Wales Court of Appeal (Criminal Division) heard an appeal involving

the compulsion of encryption keys in a terrorism prosecution. S. and A. had been charged with various terrorism offences, and investigation of each had turned up discs, hard drives and a laptop containing encrypted data. Each was served with a notice under s. 58 of the *Regulation of Investigatory Powers Act* (RIPA) which compelled them to provide the keys for accessing the encrypted data. Both refused to comply, and each applied for a stay of charges on the submission that " 'the requirement to provide information to the police under Part III of RIPA constituted an impermissible infringement of the … privilege against self-incrimination' and contravened article 6 of the European Convention of Human Rights" (para. 9). They appealed the trial judge's dismissal of the application to the Court of Appeal (Criminal Division).

Examining RIPA, the Court noted that the impugned sections did indeed compel persons to surrender information to the police if such information would make otherwise unreachable data intelligible or accessible. It pointed to a restrictive set of conditions for allowing such an order to issue, which require that: the data in question is already lawfully in police possession; disclosure is necessary for national security or crime prevention purposes because no reasonable alternative means of accessing the data exists; and the obligation imposed on the individual must be proportionate to the intended objective. Turning to a consideration of the privilege against self-incrimination, the Court noted that while the privilege was both deeply-rooted and important it was subject to many qualifications. Of particular importance was both English and European Court of Human Rights jurisprudence which accepted that "the right not to incriminate oneself …does not extend to the use in criminal proceedings of material which may be obtained from the accused through compulsory powers but which have an existence independent of the will of the suspect" (para. 17). On analysis, the Court held, the encryption key was something that existed independently of the will of the person who created it. It employed the analogy of a locked drawer:

> The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral. In the present cases the prosecution is in possession of the drawer: it cannot however gain access to the contents. The lock cannot be broken or picked, and the drawer itself cannot be damaged without destroying the contents (para. 20).

It was possible, the Court commented, that the contents of the electronic devices were illegal (as the police suspected). If this were so then the accused persons' *knowledge* of the key—a means to access illegal material—would itself be incriminating, and this would engage the privilege against self-incrimination. However, the remedy would simply be the exclusion at trial of the fact of how the police obtained the encryption key, i.e. that they obtained it from the accused persons. Ultimately, given the "proportionate and permissible" quality of any interference with the privilege that actually arose, and the presence of substantial procedural safeguards, "[n]either the process, nor any subsequent trial can realistically be stigmatised as unfair" (para. 25). The appeal was dismissed.

Internet Defamation: Is a Hyperlink "Publication"?

In *Crookes v. Wikimedia Foundation Inc.*, the plaintiffs had sued various defendants in defamation, alleging that they had been the victims of a "smear campaign." The main action related to articles regarding the internal politics of the Green Party, which had been published on two websites. This decision of the British Columbia Supreme Court was in a summary trial of the plaintiffs' claim against Defendant Jon Newton. Newton operated a website called p2pnet.net, which "contains commentary on issues surrounding the internet as well as other subjects" (para. 4). Newton had become aware of the defamation actions and had published a general article on internet defamation, which article contained hyperlinks to the articles that were the subject of the main action. Newton's article contained no comments about the other articles or about the plaintiffs, and the plaintiffs conceded that Newton had not written or posted any defamatory words. Their claim was that "posting hyperlinks to websites containing defamatory material constitutes publication of the defamatory words" (para. 6).

Justice Kelleher held that there were two issues to be determined in disposing of the case. First, "are the plaintiffs required to lead evidence that persons

actually followed the hyperlinks and read the words that are complained of?" (para. 13). The defence had argued that since no such evidence had been led, the plaintiffs had not proven the defamation element of publication. The plaintiffs had argued that publication is presumed where statements are broadcast to the general public, relying upon the B.C. *Libel and Slander Act* and earlier caselaw. Kelleher J. disagreed with this position, ruling that "[w]ithout proof that persons other than the plaintiff visited the defendant's website, clicked on the hyperlinks, and read the articles complained of, there cannot be a finding of publication" (para. 20). He noted in passing that English courts require a higher threshold of "substantial publication," but distinguished earlier Canadian caselaw which, to the extent it suggested that simple posting on a website was publication, stemmed from cases where publication was not in issue. He opined: "the mere creation of a hyperlink in a website does not lead to a presumption that persons read the contents of the website and used the hyperlink to access the defamatory words" (para. 24).

Justice Kelleher then turned to the second issue: whether creating a hyperlink to defamatory material amounts to publication. He explicitly agreed with the defendant's argument that hyperlinks, with no other commentary regarding the material linked to, were analogous to footnotes in an article: "[w]here a footnote leads a reader to further material, that does not make the author who provided the footnote a publisher of what the reader finds when the footnote is followed" (para. 28). He buttressed this with a reference to the B.C. Court of Appeal's decision in *Carter v. B.C. Federation of Foster Parents Assn.*, where that court had ruled that a newsletter's publication of a URL of a site containing defamatory material did not constitute "publication" for defamation purposes. Kelleher J. adopted the Court of Appeal's statement in *Carter* that "reference to an article containing defamatory content without repetition of the comment itself should not be found to be republication of such defamatory content" (para. 33). Accordingly, Newton's inclusion of the hyperlinks did not amount to publication. The action was dismissed as against Newton.

Internet Defamation: Is an Internet Posting a Newspaper or Broadcast?

The Ontario Superior Court of Justice has considered the interaction between notice requirements in Ontario's *Libel and Slander Act* and posting on the internet in *Warman v. Grosvenor.* The action was brought by Richard Warman, a lawyer active in human rights work relating to hate propaganda on the internet, in response to a variety of web postings and emails by the respondent, Grosvenor. Over a period of time Grosvenor had sent dozens of emails to Warman and had made dozens of web postings in which he leveled a number of insults against Warman and made various false accusations. These included that Warman was involved in organized crime, had been jailed as a pedophile, and other accusations which the court noted were intended to discredit his personal and professional reputation and to expose him to hatred, contempt and ridicule. Some of the posting also provided Warman's home address and invited others to harass or injure him. Warman brought actions for the torts of defamation, assault, and invasion of privacy.

The court had no difficulty on the facts concluding that defamation and assault were made out. It was less clear, the court said, whether the tort of invasion of privacy existed, but if it did it could only give rise to damages not otherwise accounted for under the defamation and assault actions. Since that would not have been the case, the court declined to decide whether the tort existed.

The potentially complicating issue in the case related to the requirement in Ontario's Libel and Slander Act that a person bringing an action for libel in a newspaper or broadcast must give six weeks' notice in writing of the alleged libel to the originator. Although Warman had given notice relating to some of the internet postings, that notice did not include all of them, nor any of the emails. If that requirement applied, then, the action might be barred with respect to some of the statements.

The court decided, however, that this provision did not apply in the case of postings on the internet. In part this was a simple matter of statutory interpretation, in that an internet posting did not meet the definition of either "newspaper" or

"broadcast". Further, even if they could be classified as broadcasts, they would not be from a station in Ontario, which was a further limiting condition on the requirement. The servers for the relevant internet sites were in California, Italy and Germany. Beyond the simple literal meaning, however, the court also held that the policy behind the notice requirement did not apply. In the case of newspaper articles or broadcasts, the reason for giving the notice was to allow the defendant a chance to retract the statements or issue an apology in order to mitigate damages. That rationale did not really apply to the internet, where there was no viable possibility of complete retraction, since the words could be endlessly repeated and distributed around the globe. Further in this particular case the defendant had continued to post and send emails even after being served with the notice, and so clearly had no wish to try to mitigate his damages.

Reasonable Expectation of Privacy in Cell Phone Tower Information

The extent to which the police are entitled to obtain cell-tower records, disclosing the location of the user of a particular cell phone, was at issue in *R. v. Mahmood*. In a very thorough analysis of the issues of reasonable expectation of privacy, reasonable grounds for a search, and reasonable suspicion for a search, Quigley J of the Ontario Superior Court concluded, based in part on the existence of PIPEDA, that a reasonable expectation of privacy did exist in such records, and found Charter violations in the police's actions. Ultimately, however, he concluded that the evidence found despite these violations should not be excluded.

The case arose in connection with a robbery of a jewelry store. Two men obtained entry to the store, which was accessible only when the owner permitted customers to enter. One of the men was disguised in a burqa in order to appear to be the wife of the other man. Once they were in the store they produced guns, and duct-taped the owner's hands, mouth and eyes. They then admitted a third man to the store, and took from it approximately $500,000 of jewellery and approximately $35,000 in cash. They also removed the store's surveillance system. Although the robbery had taken place during the day there were no witnesses and the store owner could not identify the culprits. The only piece of evidence which existed was a plastic shopping bag which the robbers had left behind, labeled "Amira Islamic Fashions".

One of the investigating officers was of the view, based on his experience with other robberies, that the culprits must have used cell phones in the execution of the plan. As a result the police sought and obtained warrants issued to Bell, Rogers, Telus and Telemobile requiring them to produce all records of all cell phone traffic through the two cell phone towers located in the vicinity of the crime for the hour and a half that preceded the robbery (the "tower dump warrants"). As a result the police received detailed information relating to over 7,000 separate cellular phone subscribers.

The police had identified a man, eventually one of the accused, who had purchased a burqa from Amira Islamic Fashions. Information relating to his cell phone was found in the tower dump records, and showed extensive phone calls between him and several others during the period just before the robbery. As a result the police put him under surveillance, and he was seen frequently in the company of three other men. Eventually based on that surveillance and based also on information obtained from the tower dump records, the police sought warrants specifically relating to the cell phone files of those four men (the "subscriber records warrants"). Those warrants disclosed extensive communication between the four men in the six weeks leading up to the robbery, and in particular on the day of the robbery.

Based on that information, as well as the surveillance, the police obtained a third set of warrants (the "residential warrants") which were executed at the homes of the various accused. Those warrants led to the discovery of the stolen jewelry and a sum of cash.

The accused argued that the initial tower dump warrants constituted an unreasonable search in violation of section 8 of the Charter, and that the subsequent warrants relied on information obtained through the tower dump warrants, and so would fall along with those. The Crown argued that there was no reasonable expectation of privacy in the information obtained through the tower dump

records, that even if there was the police had reasonable grounds to obtain a search warrant for those records, and further that even if reasonable grounds did not exist the information ought to have been available merely on reasonable suspicion.

The trial judge accepted the accused's argument and concluded that there was a section 8 violation. However, he concluded that the evidence should nonetheless be admissible.

The Crown argued against the existence of a reasonable expectation of privacy by pointing to the minimal nature of the information obtained, and citing various decisions on particular aspects of that information. They argued, for example, that the records disclosed a person's name, or a person's cell phone number, but that those were not part of the biographical core of personal information protected under the "informational privacy" aspect of section 8. They made similar arguments concerning the information about which numbers a cell phone had called, or had received calls from, or about the physical location of the cell phone user. The trial judge rejected this claim:

> 70 The several arguments made by the Crown on these several aspects of the Tower Dump and Subscriber Records Warrants might have been more persuasive were it not that this Court was not faced with those separate factual situations requiring consideration in such a segregated manner. The simple difference here from these cases cited by the Crown lies in the fact that each of these separate aspects of identifiable cell phone usage were obtained in one package at the same time by police authorities from the same search through the same single production of data.
>
> 71 The police did not merely obtain a series of subscriber names and addresses under the Tower Dump Warrants. They did not merely obtain a record of calls made to and received from one or several cell phone numbers. They did not just obtain a general geographic location from which such calls were made or received and when. They obtained all of this information simultaneously for each of the more than 7,000 cell phone subscribers who happened to be in the geographic vicinity of these cell phone transmission towers for the hour and a half preceding the robbery.

In addition the judge noted that the privacy policies of the cell phone service providers prevented personal information about subscribers, and also that under PIPEDA such information could only be released without consent in the face of a subpoena or warrant. In that event the accused (and all other subscribers) subjectively had an objectively reasonable expectation of privacy in the records provided under the tower dump warrants.

That there was a reasonable expectation of privacy only meant that the police were required to have a warrant in order to obtain the records, and of course they had obtained them under a section 487 search warrant. However, such a warrant requires that the police have reasonable grounds to believe that the warrant will produce evidence: it does not authorize "fishing expeditions". In this case, where the warrant was sought on no stronger basis than an investigating officer's belief that the culprits were likely to have used cell phones, the reasonable grounds standard was not met and so the warrant was improperly issued. To a large extent that illegality carried through to the analysis of the later searches based on information obtained through the tower dump records.

However, the trial judge ultimately concluded that the evidence ought not to be excluded. Under section 492.2 of the *Code*, it would have been possible for the police to have obtained dial number recorder warrants concerning the accused's cell phones, and have detected much of the same information. That type of warrant is available merely on reasonable suspicion. That was not the way the police had proceeded, and so the existence of that alternative power did not render the search legal. However, it was an important consideration in allowing the evidence in nonetheless. The trial judge noted that the information could have been obtained legally, and observed:

> 52 To exclude highly relevant, and probative Subscriber Records evidence under subs. 24(2) in the face of what amounts to little more than a technical breach of their *Charter* rights, having regard to the availability of specific statutory authorization to obtain such

> information on a reasonable suspicion basis would, to my mind, bring the administration of justice into disrepute to a far greater extent than the admission of that evidence at their trial.

As a result the fruits of the subscriber records warrants were admissible, which meant that the evidence obtained through execution of the residential warrants was also admissible.