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

July 24, 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.

Admissibility of Solicitor-client Emails

The Ontario Superior Court of Justice dealt with the issue of admissibility of solicitor-client communications conducted by email in *Eizenshtein v. Eizenshtein*. The parties were involved in divorce proceedings. The husband had subsequently become involved with a woman, Saffer, who was frequently at his house, though she did not live with him. Saffer had occasional access to the husbands' computer, with his consent. At some point his relationship with Saffer ended, and Saffer gave printed copies of email communications between the husband and his solicitor to the wife.

There was disagreement over how Saffer came to have copies of the emails. Saffer's version (as relayed through the wife) was that the husband permitted Saffer to use his computer when she was at his home, and that she helped him to type e-mails from time to time, including these particular e-mails. Ms. Saffer also said that the husband left printed e-mails around his home. Saffer did not explain directly how she came to have copies of the emails.

The husband testified that the emails had been sent and received from his private, password-protected Yahoo account. He agreed that Saffer had access to his computer, but not to his Yahoo account unless he was standing by her side. He acknowledged that he often had difficulty printing and sometimes asked her for help printing documents after he had opened them. However, he denied that she had typed the emails in question for him. He also testified that any printed e-mails were either in files in a cabinet in his bedroom or a filing cabinet in his home office. He indicated that he never provided Ms. Saffer with his Yahoo password, never showed Ms. Saffer any e-mails between him and his lawyer, and kept those e-mails in a separate folder in his e-mail account, as a further layer of protection.

The wife attached those communications to an affidavit she presented to the court: she suggested that they went to his credibility in claims he was making about family finances. The issue was whether those emails were protected by solicitor-client privilege, or whether they were subject to some exception to that rule. Two exceptions were discussed: the "criminal intent" exception and the "loss of privilege by disclosure to a third party" exception.

The judge readily concluded that the criminal intent exception did not apply. Although there was discussion in the emails of what might be characterized as aggressive pursuit of litigation strategies, it did not disclose an intent to file a false affidavit with the court. Further, nothing in the emails showed that the husband had sought advice on how to act illegally, and the lawyer had shortly afterward sent a further email retracting his advice, since it had been given based on a misunderstanding.

The more difficult question was the loss of privilege through disclosure issue. However, the judge held that is could be settled without having to decide exactly how Saffer came to have copies of the emails. Solicitor-client privilege was not lost solely because a third party had seen the material in question. A court was also required to determine whether the information was so important to the outcome of the case that it should be admitted despite the existence of the privilege. This inquiry includes consideration of whether the information was obtained through improper means. In this case, whether the husband's explanation or Saffer's explanation was accepted, the privilege should not be seen as lost. The judge held:

> 38 If Ms. Saffer is correct that Mr. Eizenshtein let her see the e-mails, that might be characterized as "advertent" disclosure.

However, I find, even if this happened, Mr. Eizenshtein reasonably assumed the e-mails would go no further. In assessing whether the documents can be disclosed to the court, the distinction between advertent and inadvertent disclosure is less important than Mr. Eizenshtein's intention when he allowed Ms. Saffer to see them.

39 Asking an intimate friend or family member for assistance in printing or typing a document is the technological equivalent of an illiterate person asking for help to read a legal document. I find that this does not result in a loss of privilege. I also find that leaving correspondence in a file in the privacy of one's own home is not sufficiently reckless to warrant a waiver of privilege.

The trial judge also noted that solicitor-client privilege had to be understood and protected in light of the new threats to it found because of new technology:

41 We live in an interesting time. The electronic age creates communication problems never contemplated when the law of solicitor-client privilege was first developed. Identity theft, electronic fraud and computer "hacking" are ever-present concerns. More and more information is prepared and communicated electronically, often with no security protection, sometimes only with the protection of an often used or easily guessed password. Information from one computer can be accessed from computers at another location, even on the other side of the world. Much of a person's private information is now stored on a computer, often with a right of access to the computer by other members of the person's household or business, who also have need to use the same machine.

42 The law must evolve to protect solicitor-client communication in an electronic world. It is important to take a firm stand on this issue. Solicitor-client privilege is important to our justice system.

43 It is also important to respect family relationships and other relationships of trust. To allow the admission of evidence, even if disclosed to others with whom a person has a close business, family or intimate relationship, would encourage troubling scenarios, such as was suspected initially in this case, when the child of the marriage was considered the "prime suspect" for the leak. The message would be "if you can get your hands on it, we'll take a look at it". That is not what our courts should be saying about solicitor-client communications. Instead, the message should be "Hands off – it's private!"

Defamation by Domain Name Misdirection

The Alberta Court of Queen's Bench considered the tort impact of registering a misleading domain name and directing a company's business first to a competitor and then to a pornographic website in *Inform Cycle Ltd. v. Draper*. Inform Cycle was a high-end bicycle business which had registered the website InformCycle.ca. Draper had previously worked for the owners of the business, but at the relevant time worked for Rebound, a different bicycle business. He registered the domain name InformCycle.com and directed its traffic to Rebound for a period of about three weeks. At that stage, immediately before leaving on vacation, Draper redirected the InformCycle.com site to a pornographic website. It remained directed in that fashion for a little more than two weeks. Inform Cycle was eventually able to shut down the forwarding, and commenced an action against Draper.

In an earlier proceeding Inform Cycle had received summary judgment against Draper for passing off, for having directed the InformCycle.com traffic to a competitor; defamation, for having directed the InformCycle.com traffic to a pornographic website, and; the intentional tort of "knowingly and deliberately undertaking the registration and forwarding of the Misleading Domain Name". These proceedings dealt with the issues of damages for each.

With regard to the passing off, Brooker J. awarded $5,000, noting that there was no evidence as to whether Inform Cycle actually lost sales as a result of Draper's actions, but that there was a presumption of damages. With regard to the defamation, Brooker J. noted that the fact that the publication was on

the internet, and therefore published to the world at large, was relevant. [On that point see as well the recent decision in *Griffin v. Sullivan*, 2008 BCSC 827] In addition, though, the nature of the defamation also needed to be taken into account. The defamation did not consist of a statement which could be replicated and forwarded endlessly: it was a referral to a porn site which lasted for a limited period of time. There was no evidence of how many people were misdirected, nor whether they thought the direction was intentional on the part of Inform Cycle or a computer glitch. The judge awarded another $5,000 for this ground.

With regard to the third ground, the judge awarded no damages, holding that he did not understand or recognize the tort for which summary judgment had been granted. He held that there was nothing objectionable in simply registering a domain name, and that any misuse of the registered name would be subsumed into the passing off and defamation torts. He did, however, order an additional $5,000 in punitive damages.

Non-disclosure of Encrypted Data

The Ontario Superior Court of Justice recently, in *R. v. Beauchamp*, dealt with the issue of Crown disclosure where the information in question consists of encrypted data obtained under a search warrant, which the Crown has not been able to de-encrypt. The several accused in the case were charged with 33 offences relating to forgery and credit cards, and the police had seized a computer hard drive which contained a variety of encrypted files. The Crown had been unable to de-encrypt the files and so had no knowledge of their content. However, the Crown and the accused agreed that the encrypted information was relevant and was both potentially inculpatory and potentially exculpatory for all the accused. The accused argued that as the information in the encrypted files was relevant, it met the standards from *R. v. Stinchcombe* and therefore that the Crown was required to disclose it. The Crown refused, arguing that as it had not been able to de-encrypt the information, it was not in the Crown's possession or control. They also argued that there were further grounds than those specifically listed in Stinchcombe which could justify non-disclosure.

The application judge accepted the Crown's position that the information did not need to be disclosed. He did not accept that the issue could be settled straightforwardly on the basis that the Crown did not have possession or control of the information since it was unable to de-encrypt it. The Crown did have partial possession, and so further analysis was necessary. However, Smith J. concluded that looking at the fundamental principles underlying disclosure, the right conclusion was that the Crown was not obliged to disclose in these circumstances.

Several considerations were relevant. First, the information would not be part of the case to meet, since the Crown did not know what it was. Further, there was no evidence from any accused as to how it might be relevant to an issue related to the defence. Second, the Crown was expected to exercise its discretion over disclosure in order to, for example, not release irrelevant or privileged information. In the circumstances here, the Crown was unable to exercise its discretion. However, there was a reasonable possibility that private information, such as credit or debit card information or the identities of members of the public would be among the encrypted files. Disclosure of the material would therefore potentially permit the commission of further offences, and the Crown would be unable to exercise its discretion to guard against this possibility. Further, if the information remained encrypted, a court would not be able to review the Crown's exercise of discretion. In addition, it appeared that some accused would be able to de-encrypt the information but others would not, which would create disparity.

There was some discussion of resolving the issue through disclosure to defence counsel with appropriate undertakings. However, some accused were not represented by counsel, and there was no evidence that defence counsel had access to the password necessary to access the data. The application for disclosure was therefore rejected, subject to a right to re-apply upon showing how the information sought would be probative to an issue involved in their defence. In addition the accused were entitled to, at their option, obtain disclosure by providing the Crown with the password or key so that the Crown could exercise its discretion with regard to the material.

Permanent Injunction Against File Sharing Site

ADISQ, the association which represents Quebec's recording industry, has obtained a permanent injunction against QuebecTorrent.com, a peer-to-peer file sharing site based in Quebec and specializing in Quebec content. The site had about 85,000 users and had been operating for approximately two years, sharing files containing music, television clips and movies. ADISQ had launched the action seeking $200,000 in damages, claiming that file sharing sites had cut deeply into CD sales in the province. The defendant agreed to the injunction in order to avoid litigation, and the plaintiffs dropped the damage claim. The consent order is not available online, but see media coverage of the result here.

Use of Non-identifying Data in Google/Viacom Disclosure

Viacom and Google (the owner of YouTube) have reached an agreement allowing Google to anonymize data before handing it over to Viacom. Viacom had brought a copyright infringement suit in the United States against YouTube, and had obtained an order obliging YouTube to disclose information which included individual users' IP addresses and user IDs. This information would have made it possible to identify individual users. The parties have now signed an agreement, however, permitting Google to include unique identifiers in the data instead. This will mean that the separate activities of individual users will still be linkable to one another, but the information could not be used to determine the identity of the user. The text of the agreement can be found here.

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