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

November 27, 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.

Criminal Law: Wiretap Evidence in Bail Hearing

The Ontario Court of Justice has delivered its ruling in *R. v. Pewngam* (currently not available online). This was a judicial interim release (bail) hearing for the accused, an Ontario Canadian with robust record of previous convictions and dealings with the law. The accused goes by several aliases and, in the opinion of the court, seemed to have a weak connection with his professed Ontario community. Except for his ex-wife, other potential sureties presented by the accused appeared to have little knowledge of his means of livelihood and general affairs. With the consent of the defence counsel, the Crown's 54-page synopsis was read into and filed with the court. It was also elaborated and expanded upon in the cross-examination of a police Crown witness who testified at the proceeding. Most of the evidence comprised several intercepted private communications (wiretaps) reports, draft e-mails (that were never sent) and surveillance evidence of the accused with his alleged accomplices in four distinct sets of charges involving exportation of significant qualities of illegal drugs (cocaine, methamphetamine and MDMA) by the accused from Canada to Australia and the United States. The evidence also demonstrated the accused's strong connection with his co-accused and other alleged accomplices in other jurisdictions, including "his frequent contact with them, common knowledge of e-mail accounts and passwords, their reliance on him to pay for their transaction-related flights and other travel costs, including a debriefing on how to improve smuggling across the Canada-United States border" (para 70). In several wiretaps, the accused was heard threatening to abscond and to escape being detained, especially following the arrest of one of his accomplices in Australia.

In its ruling denying the accused bail, the court noted that its discretion to rely on wiretap evidence is based on s. 518(1)(d.1) and (e) of the *Criminal Code*. According to the court, "[t]hese two provisions provide the court holding a bail hearing with the discretion to receive wiretap, email and surveillance evidence, and I am exercising my discretion to do so in the matter before me. While Mr. Pewngam was never found with the drugs himself, other individuals have been apprehended in foreign jurisdictions because they were the ones who received these shipments, and those arrests were made as result of cooperation between law enforcement agencies who shared the results of the wiretap, email and surveillance evidence that is now before this court". (para 69).

Hate Speech on the Internet

The Canadian Human Rights Commission (CHRC) has released publicly a report it had commissioned on the question of whether it should continue to be involved in investigating and trying to eliminate hate speech on the internet. The report, prepared by Richard Moon of the University of Windsor, recommends that censorship by the government should be limited to a narrow range of speech, and accordingly that section 13 of the *Canadian Human Rights Act* (CHRA) should be repealed, with the result that the Commission would no longer deal with hate speech, on the internet or elsewhere.

The essence of Professor Moon's rationale is that hate speech falls approximately into two categories. One consists of less extreme forms of discriminatory expression, the other of extreme expression which threatens, advocates or justifies violence against the members of an identifiable group. The former category, Professor Moon argues, should be addressed and confronted, but censorship of them is not the appropriate response. The more extreme forms of

hate speech which are tied to violence also need to be addressed, and more urgently. However, he argues, the best response to that category is not through human rights law that emphasizes the effect of the action on the victim rather than the intention of the actor and which aims at facilitating a non-adjudicative resolution of the "dispute" between the two. The latter category should be dealt with under the *Criminal Code* rather than the *Canadian Human Rights Act.*

Professor Moon suggested that this approach would largely be in accordance with the actual practice. He notes that "The few section 13 cases that have been sent by the CHRC to the Tribunal and in which the Tribunal has found a breach of the section have almost all involved expression that is so extreme and hateful that it may be seen as advocating or justifying violence against the members of an identifiable group."

The recommendations in the report fell into three groups:

1. Section 13 of the *Canadian Human Rights Act*, which makes it a discriminatory practice to use the internet to expose persons to hatred or contempt on the basis of a prohibited ground of discrimination, should be repealed. Hate speech should continue to be prohibited under the *Criminal Code*, and police and prosecutors should make greater use of section 320.1 of the *Criminal Code*, which gives a judge power to order an Internet service provider (ISP) to remove hate propaganda from its system. In addition it was suggested that each province should establish a "Hate Crime Team" composed of both police and Crown law officers with experience in the area to deal with the investigation and prosecution of hate crime.

2. If section 13 of the CHRA is not repealed, then it should be amended to apply only to the most extreme instances of discriminatory expression, that threatens, advocates or justifies violence against the members of an identifiable group, should include an intention requirement, and should be dealt with by a different process in which the CHRC would investigate complaints and have carriage of them before the Canadian Human Rights Tribunal (CHRT).

3. Non-state actors also have a role in the prevention of expression that is hateful or discriminatory in character. The report recommends in particular that the major (ISPs) should consider creating a hate speech complaint line and an advisory body to give an opinion as to whether a particular website hosted by an ISP has violated section 13 of the CHRA or the hate propaganda provisions of the *Criminal Code*. If the body concludes a complaint is well-founded, the ISP should shut down the site on the basis of its user agreement with customers.

Insurance Contract and Engineering Law

The Supreme Court of Canada has delivered its decision in *Canadian National Railway Co v. Royal Sun Alliance Insurance Co. of Canada*. The appellant (CNR) engaged in an initiative to design and construct "the largest customized tunnel boring machine (TBM) of its kind in the world for use in the construction of tunnel under a river". It then insured the project pursuant to a builder risk policy. The policy covers all risks of "direct physical loss or damage to real and personal property of every kind and quality including but not limited to the TBM, plus consequent economic loss occasioned by delay in the opening of the tunnel" and excluded "the cost of making good faulty or improper design". CNR selected an experienced manufacturer who then designed, engineered and constructed the TBM under sophisticated expert scrutiny, review and monitoring processes. In the design, the main bearing generates a hydraulic thrust which drives the cutting tool through the earth. To shield that critical bearing from damage was a device comprising "26 independent seals lubricated by constant injection of pressurized grease" which guarded against the escape of excavated material to the main bearing while preventing the grease from leaking out. The design was certified not to occasion excess differential deflection (structural bending of the steel). However, following the completion of 14 percent of the tunnel, contamination was dictated which arose from wearing down and destruction of some seals as a result of excess differential deflection. Consequently, operations were suspended to clean the mainbearing and to make required modifications.

After the adjustments, no more entry of dirt occurred following the completion of the project. Because of the modification, the completion of the project was delayed for 229 days. This resulted in radical cost escalation. In the meantime, it was not clear to the experts why and how dirt penetrated the 26 seals while sparing others.

Relying on the "faulty or improper design" exclusion on their policy, the respondents declined the appellants' claims for insurance coverage. The court found for CNR. According to the Supreme Court (Per McLachlin, CJ and Binnie, LeBel and Abella, JJ) (Deschamp, Charron and Rothstein, J.J. dissenting), in this case where the risk is broadly defined and the design has addressed the risk with the state of the art diligence and expertise, an insurer should not be allowed to rely on the "faulty or improper design" exclusion on the basis that existing engineering knowledge and practice does not seem to properly appreciate the design problem. The required standard is that the design complies with the state of the art. According to the court, failure should not be equated with fault or impropriety. In this case, faulty or improper design exclusion applies to faulty design and not to designer fault; it can only apply where the design is faulty and improper. Note: According to the dissent judgment, the exclusion applies to the thing designed and not to the work of the designers and if the design does not work for the purpose for which it was intended, the issue of its standard is not relevant.

Internet Data Neither Here Nor There

The Federal Court of Appeal has dismissed an appeal by eBay Canada requiring it to hand over to Revenue Canada information identifying "Powersellers" in Canada. Powersellers are clients of eBay who have sold more than a certain volume of items. Revenue Canada wanted the information in order to determine whether those people had correctly reported their income.

The issue in the case was whether the information sought was "foreign-based information". If it was, then Revenue Canada did not have the authority under the *Income Tax Act* to order the production of such information from a third party with regard to unnamed persons. eBay Canada's argument was that the information was stored on servers located in the United States and owned by eBay International. The Canadian corporation was authorized to access and use the data, but did not download it to its own computers in Canada.

The Court of Appeal upheld the lower court ruling that on these facts the data was not foreign-based information. Although the information was located on servers outside the country, its ready accessibility in Canada meant that it was also located here. The Court of Appeal reasoned that the statutory limitation on obtaining foreign-based information had been created in the context of written documents. The scheme contained limits which were meant to reflect the difficulty which might be posed for those in Canada ordered to produce documents which were not themselves located in Canada and which were in the possession of another person. Those considerations, however, did not apply to electronic data because "with the click of a mouse, the appellants make the information appear on the screens on their desks in Toronto or Vancouver, or anywhere else in Canada. It is as easily accessible as documents in their filing cabinets in their Canadian offices" (para 48). The court described it as "formalistic in the extreme" to argue that the information would only be located in Canada if it were actually downloaded to a Canadian computer.

In that event the information existed in more than one place and it could be subject to an order. Since the lower court judge had not erred in applying the law to the particular facts, the appeal from that decision was dismissed.

Traffic Shaping Complaint Dismissed

The Canadian Radio and Telecommunications Commission (CRTC) has rejected a complaint brought against Bell Canada by the Canadian Association of Internet Providers (CAIP) objecting to Bell's policy of traffic shaping. Bell acknowledged that it engaged in traffic shaping on its network (and, in particular, on Gateway Access Service (GAS), used by Internet service providers (ISPs) use to provide retail Internet services) by slowing down the transfer rates of all peer-to-peer (P2P) file-sharing applications between 4:30 p.m. and 2:00 a.m. daily. Bell argued that traffic shaping was the best

practical approach to address network congestion. CAIP argued that Bell's traffic shaping violated the *Telecommunications Act* and was contrary to its privacy objectives.

The Commission concluded that Bell was responsible for ensuring that its network operated effectively and efficiently, and that it was entitled to take measures to ensure that result. The Commission also concluded that Bell Canada had established that there was congestion in its network during peak periods. The Commission accepted Bell's submission that the intensive use of P2P file-sharing applications during periods of high internet traffic could result in network congestion and degrade the service for other end-users. The Commission therefore concluded that Bell had established that some measures were required to prevent its customers from using, or permitting to be used, P2P file-sharing applications so as to prevent fair and proportionate use by others of its network. The Commission also noted Bell's submission that the only technologically and economically practical solution was traffic-shaping, and that there was no evidence establishing the availability, feasibility, or utility of any alternative solution.

The Commission also noted that the traffic-shaping measures adopted by Bell gave equivalent treatment to both its own retail internet service end-users and the GAS ISPs' end-users. CAIP had alleged that Bell was using the traffic-shaping to secure sufficient bandwidth for its own services and to prevent ISPs from competing against Bell. The Commission concluded, however, that there was no basis on the record to reach that conclusion.

CAIP had also argued that Bell's traffic-shaping measures required them to examine packet headers and packet content without prior knowledge or consent of the users, which they suggested violated privacy guarantees. The Commission noted, though, that there was no evidence that any of the examined header information was collected or disclosed by Bell or used by Bell for any purpose other than traffic-shaping, and no-one claimed that Bell had collected, retained, or disclosed customer information in its ongoing application of its traffic-shaping measures.

In the circumstances, therefore, Bell was not in violation of the *Act* through its traffic-shaping practice and CAIP's application was denied.

However, the Commission did note that broader issues were raised. First, there was the issue of the resolution of complaints. The Commission observed that it expected Bell to develop solutions for complaints on a timely basis and directed them to file a report on the resolution of complaints related to affected non-P2P file-sharing applications by **9 January 9, 2009**. In addition the Commission noted that the issues raised in the complaint raised concerns that went beyond the scope of the particular proceeding. Accordingly they concluded:

> In light of the importance of these concerns, in a Public Notice issued today, the Commission initiates a proceeding to review the current and potential Internet traffic management practices of ISPs with respect to both retail and wholesale services. The Commission will consider whether such practices are consistent with the *Act* and whether any measures are required to ensure this. The process for this further proceeding, which will include an oral public hearing, is outlined in Telecom Public Notice 2008-19.

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.