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

April 18, 2012

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Robert Currie and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School, and David Fraser.

Les auteurs du présent bulletin sont les professeurs Robert Currie et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie, et David Fraser.

Technology Tax Law: Exporting VOIP to Non-Resident is Tax-Exempt

In *SWS Communication Inc. v. The Queen*, Justice Robert Hogan of the Tax Court of Canada heard joint appeals of tax assessments on two Montreal companies. The CRA had ruled that each company had failed to collect GST on the supply of telecommunications services to American customers. The two companies, SWS and CMI, were wholesale providers of voice over internet protocol ("VOIP"), purchasing VOIP services from carriers and then reselling them at a mark-up. As the court described SWS's relevant activities, "SWS granted BMT America the right to direct VOIP calls over Internet pathways situated outside Canada for which SWS had arranged transmission rights. These routes were used to transmit VOIP calls originating in the Southwest and Southeast of the United States to termination points outside of Canada and the United States" (para. 10). The equipment used to do the US transmissions were located in that country. There was less evidence about the CMI transactions with its US client, Convergia, though they appeared to be similar.

Under s. 22.1 of the *Excise Tax Act* no GST was levied on telecommunications services which were supplied by a Canadian registrant to a non-resident business. However, s. 132(2) of the Act provides that where a non-resident person has a permanent establishment in Canada, that person is deemed to be resident for the purposes of the business carried on at the permanent establishment. The CRA auditor noted that both of the US customer companies had offices in Montreal, and applied s. 132(2) on that basis, assessing SWS and CMI as being out of compliance with GST collection. Justice Hogan described the auditor's assessment as being based on the "misconception" that s. 132(2) was invoked simply by virtue of the customer having a Canadian-based operation. Noting that the section only applied to business carried on "through" the Canadian establishment, he remarked at para. 19:

> In my opinion, a service is supplied to the Canadian permanent establishment of a non-resident person if it is consumed or used in the activities carried on in Canada through the permanent establishment. In light of the above, it is not sufficient for the Minister to show or assume that the recipient of the supply has a permanent establishment in Canada. The Minister must also show or assume that the supply was consumed in the furtherance of the activities carried on by the permanent establishment. It is clear from the evidence that the respondent's representatives failed to consider whether the services supplied by SWS were made to BMT America's and Convergia's permanent establishments in Canada.

Procedurally, the CRA had actually failed to properly "assume and allege" that the business was done with the customers' Canadian offices, and thus the appellant companies did not bear the burden of proof to show that the transmissions had been made to the US sites. Nonetheless, the appellants had led evidence that supported this fact with regard to both sets of transactions. The appeals were allowed and the assessment remitted to CRA to take into account that no GST was required to be collected.

Emergency Wiretaps and the *Charter*

With *R v Tse* the Supreme Court of Canada has rendered a decision concerning the constitutionality of the emergency wiretap provisions in section 184.4 of the *Criminal Code,* though in the course of doing so it has also clarified the relationship between the

various wiretap provisions. For the most part the emergency power in section 184.4 was found to be acceptable, though the lack of adequate after-the-fact safeguards caused the Court to strike down the legislation as violating section 8 of the *Charter*. The Court suspended that declaration of invalidity for twelve months in order to allow Parliament to draft a new law: in part this approach was taken because the Court had other suggestions as to how the law could be improved, even though these particular points were not necessarily constitutional requirements.

The Court observed that the *Criminal Code* contains a number of provisions permitting wiretaps, which range in terms of how difficult they are to obtain. The "ordinary" wiretap authorizations are found in section 186, require an application in writing to a judge, and require that information concerning various specified areas be provided. As a reflection of the fact that making such an application can be time-consuming, therefore, section 188 provides for emergency authorizations from specially-appointed judges who can issue an authorization for a period not exceeding 36 hours where "the urgency of the situation requires interception to commence before an authorization could, with reasonable diligence, be obtained under section 186." Finally (for current purposes) there is section 184.4, the provision challenged in Tse. That provision allows peace officers to use a wiretap without *any* judicial authorization if three conditions are met:

(a) the peace officer believes on reasonable grounds that the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;

(b) the peace officer believes on reasonable grounds that such an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and

(c) either the originator of the private communication or the person intended by the originator to receive it is the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

The accused argued that section 184.4 violated the *Charter* in a number of ways: the Court rejected most of those arguments, but did ultimately find a section 8 violation. The Court rejected the arguments that section 184.4 was vague or overbroad. The accused had argued that the terms "the urgency of the situation", "reasonable diligence", "unlawful act" and "serious harm" were unclear and would permit the section to be used in too many circumstances. The Court found none of the terms to raise *Charter* issues, though in the course of reaching that conclusion they did give guidance as to the way in which the provision should be understood. Specifically, section 184.4 was aimed at exigent circumstances and should be limited in its use to those situations. The requirement that an authorization could not be obtained with reasonable diligence, for example, in most circumstances would have the practical effect of requiring the police to begin such an application. This might not always be the case (due to a shortage of personnel or unavailability of judges, for example) but in general the reasonable diligence requirement would call on police to actually commence the application process.

Further, the Court noted that part of this reasonable diligence requirement would include making an application under section 188 for an emergency authorization pending the full application. In that regard, therefore, they clarified that applications under section 188 did not have to be in writing, and could if necessary be made by telephone. These conclusions make section 188 authorizations that much easier to obtain, and thereby reduce the period of time in which a section 184.4 interception could be justified. The Court noted that no absolute time period was imposed on section 184.4 interceptions (unlike the 36 hours in section 188) but that nonetheless the other requirements acted to keep them within strict temporal limits.

The Court also observed some differences between section 184.4 interceptions and the others in question. First, authorizations for an interception are only available (under section 183) for particular listed offences. It had been argued that section 184.4 should also therefore be limited to those offences: that one could not impose a requirement on the police to be reasonably diligent about seeking an authorization if the circumstances

were such that one would be impossible to obtain. The Court rejected that argument, however, holding that section 184 imposed its own limits: an unlawful act that would cause serious harm to any person or to property. Second, interceptions under section 184.4 need not be a near-last resort in the way that is required for section 186. Section 186 limits wiretap authorizations to cases where there is "no other reasonable alternative method of investigation": section 184.4, on the other hand, says that the interception is "immediately necessary". This phrase requires that the police be faced with an emergency, but does not also require that the police have exhausted all other investigative techniques before using a wiretap. This is a reflection of a third difference the Court noted: sections 186 and 188 are provisions aimed at evidence-gathering, while section 184.4 is meant to be a way of *preventing* serious harm. This meant, they also observed, that there could be rare circumstances in which no offence has yet been committed, and therefore sections 186 and 188 would not be available: that should not preclude the use of section 184.4 if its conditions were met.

In addition the Court observed other inherent limits in the provision. For example, the requirement of "serious" harm to property meant not only that the harm had to be significant but that the property itself also had to be significant, such as a bridge, a building, or a home. Similarly, they concluded that "victim" in section 184.4(c) had to be construed narrowly, thus limiting the circumstances in which the power could be used. Overall, the Court found that the provision was not overbroad and that there was a place for it.

However, the Court found that there were concerns with the exact incarnation of the wiretap power in section 184.4. It was, they noted, the only wiretapping power in Part VI that did not require either consent of one of the parties to the communication or judicial pre-authorization. Since those safeguards were not in place, particularly the judicial pre-authorization, it became that much more important that other protections be included. In particular the Court found that there was a section 8 violation because the provision had no requirement that a person whose communications had been intercepted would be notified after the fact of that interception. In other situations where an emergency power without pre-authorization had been found to be constitutional, there was no need for such notice: the Court adopted the words of the trial judge who had found that

> The interception of private communications in exigent circumstances is not like situations of hot pursuit, entry into a dwelling place to respond to a 9-1-1 call, or searches incidental to arrest when [public] safety is engaged. In those circumstances, the person who has been the subject of a search will immediately be aware of both the circumstances and consequences of police action. The invasion of privacy by interception of private communications will, however, be undetectable, unknown and undiscoverable by those targeted unless the state seeks to rely on the results of its intentionally secretive activities in a subsequent prosecution.

The absence of any notice requirement, the Court therefore held, meant that section 184.4 violated section 8 of the *Charter*.

The Court also considered a number of other objections to the scheme: the lack of a requirement to report to Parliament how frequently the provision was used, the lack of a record-keeping requirement, the lack of any restriction on the use that can be made of the interceptions, and the fact that the power was available to "peace officers", a term which included sheriffs enforcing civil judgements, the mayor of a city, and so on. With regard to the last, the Court held that there might well be a *Charter* problem there, but that without an evidentiary record they would not address the issue. With regard to the others, the Court found that such requirements might well be sensible and suitable, but were not constitutional requirements. The Court suspended its declaration of invalidity for twelve months to allow Parliament to draft a new law, clearly anticipating that their comments would be taken into consideration.

Privacy: Don't Just Lock Up That Flash Drive—Encrypt It

The Information and Privacy Commissioner for British Columbia recently released an investigation report regarding a data breach at the University of Victoria. On the night of 7 January 2012, thieves broke into the Administrative Services Building at

the University. They stole laptop computers and other mobile storage devices, none of which had any personal information on them. The thieves also removed a wood panel at a work station, behind which was a small commercial safe which was secured to the concrete floor. They dislodged the safe from the floor and made off with it. Inside the safe was a mobile flash drive containing the personal information of some 12,000 past and present employees of the university, including names, SINs, banking information and payroll data. The drive was intended as a "failsafe" backup for the main server used for payroll purposes. It was not encrypted. At the time of the report's issue, the drive had not been recovered. The University notified the police and also reported the incident to the Office of the Information and Privacy Commissioner, which assisted the university in notifying people potentially affected by the breach.

The Commissioner noted that, under the BC *Freedom of Information and Protection of Privacy Act*, public bodies such as the university must make "reasonable security arrangements" against the risk of breach or disclosure. Whether a particular arrangement was "reasonable" depended on a number of factors, including the nature of the device or storage medium. The university's security procedures provided that confidential information should be "stored within a controlled-access system," such as a locked cabinet. This policy, the Commissioner felt, did not "recognize the risks involved with personal information contained on laptops and other portable devices. It does not provide specific guidance on how to reduce or eliminate the risk by ensuring the security of personal information, and it does not reference the need for encryption of sensitive data" (p. 11–12). Because of the portability of the device, locking up or even password protection was not sufficient, and encryption should be the default. Indeed, "there is simply no rationale for failing to encrypt this information" (p. 16).

Moreover, the university did not have sufficient reviews in place as to whether the information stored on the device was actually needed—particularly given the sensitivity of the data—and this particular device had an unnecessary amount of data stored on it.

The Commissioner also found that the physical safeguards in place did not meet the reasonableness standard, as the safe was too easily dislodged and the area in which it was located was not alarmed. The particular care which was required to meet the reasonableness standard was heightened in this instance, due both to the nature of the information, which would make it greatly desirable to criminals, and to the fact that it was information that employees were required to provide as part of the employment relationship. The university was, however, found to have appropriately contained the breach, engaged in appropriate risk evaluation and notification, and adopted reasonable prevention strategies. The Commissioner concluded:

> In the end, a relatively simple but preventable error has resulted in a significant privacy breach and enormous costs in time and money for the University and past and present employees. The critical message arising from this incident is that, when dealing with highly sensitive personal information, public bodies and organizations must ensure that they have carefully assessed the privacy and security risks associated with the information and employ all reasonable methods to protect it (p. 24).

Internet Defamation: SCC Dismisses Appeal in *Breeden v. Black*

Just as this newsletter was going to print (so to speak), the Supreme Court of Canada released its long-awaited decision in *Breeden v. Black*, dismissing the defendants' appeal from the Ontario Court of Appeal's 2010 decision (reported in a previous issue of this newsletter). The case involves the assumption of jurisdiction in internet-based defamation cases, and relies on the Court's revamping of the criteria for assumed jurisdiction in the concurrently-released *Van Breda* decision. Black will be reported upon more thoroughly next issue.

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 Professor Robert Currie, Director of the Law & Technology Institute, at robert.currie@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 le professeur Robert Currie à l'adresse suivante : robert.currie@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.