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

March 8, 2007

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Teresa Scassa, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School.

Les auteurs du présent bulletin sont les professeurs Teresa Scassa, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie.

Civil Procedure

The Ontario Superior Court has delivered the reasons for its decision in *Directv Inc. v. Gilliott*. In that case, the plaintiff seeks a consolidation of two previous actions involving the defendant and for a court order directing a firm of solicitors to pay some monies it held in trust in the court to the account of the proposed consolidated actions. The defendant is alleged have been in a business that unlawfully sells devices to decrypt Directv broadcast signals in Canada. He is also alleged to be a party to a fraudulent scheme by which Directv subscriptions were sold to Canadian residents. This scheme was hatched in a manner that deceived the plaintiff into believing that it was providing services to US subscribers. The plaintiff's broadcast signal reaches Canada, even though it was not licenced in Canada to provide programming to Canadian residents. In this scheme, the defendant was alleged to have provided the plaintiff with US billing addresses for customers resident in Canada. The allegations against the defendant and a host of other corporate and individual defendants constituted the subject of a separate litigation, the Radio Communications action. In the second litigation, the plaintiff sues the defendant to recover monies associated with the alleged scheme under the first action. The second litigation is the Credit Card action.

In regard to the Credit Card action, it was established that during a nine month period the defendant's credit card with National Bank was charged $369, 473.05, all of which he paid. Of that amount, he paid $361, 931.40 for Directv charges. Directv does not, as a practice, require signatures from customers ordering services from it via telephone or the internet. The defendant deposes that he pays his credit cards on line. He claims to have discovered that he had unknowingly paid over $350,000 on credit card bills as unauthorized purchases from Directv. He alleges that Directv obtained his credit card information unlawfully and without any justification or lawful cause placed the controversial charges thereto. Consequently, in regard to the credit card action, he raised ac counterclaim for $197, 041.18 being sums allegedly improperly charged by the plaintiff. Meanwhile, the defendant executed an anton piller order (pursuant to which it seized plaintiff's Directv receivers and many decryption devices) and an order for interim injunction against the plaintiff. In granting those order the court found that the plaintiff has established "an extremely strong prima facie case of piracy and conspiracy to commit piracy" (¶ 25).

The defendant proceeded against National Bank demanding reimbursement for alleged unauthorized charges to his credit card. Following the bank's hesitation, the defendant sued it a chargeback action. The bank initiated a chargeback procedure under its credit card arrangement. It charged back to the Directv the sum of $172, 432.87 in accordance with an agreement between the later and the bank. Directv did not contest the chargeback. The defendant relies on this to contend that Directv does not have claim to the funds. To successfully oppose the charge back, the plaintiff would have to establish that the defendant did authorize the charges made on his credit card. As noted, the plaintiff did not obtain signatures for subscribers who used the internet or telephone. A summary judgment by consent was entered against National Bank. The judgment allowed Directv time to deliver a motion it may deem appropriate regarding the present action or the chargeback fund. Consequently, Directv commenced the credit card action against the plaintiff alleging that the plaintiff's claims regarding the credit card payments were not credible. It alleges that the plaintiff intentionally used his credit card to subscribe others to Directv and his claim that the

use of the card was unauthorized was false. Directv prayed that the money charged back funds be paid into court pending the determination of the actions.

The court then proceeded to grant the plaintiff's two major prayers. It held that this was a situation where an order of consolidation could be made in respect of the two actions: the Radio Communication and Credit Card actions. The court found that s. 9(1)(c) of the Radiocommunications Act prohibit decryption of encrypted signals emanating from the U.S. and other foreign broadcasts and that the current law in Canada makes unlawful the activities of gray marketers (¶¶38, 39). It also held that the plaintiff request to pay into court the sum of $172, 432.87 which it seeks recover from the defendant pursuant to the Credit Card action (note the balance of $197, 041. 18 was subject of counterclaim by the defendant) was not an attempt to obtain execution of judgment before trial. According to the court, the circumstances of this case satisfy the requirement that there be a specific fund. The court found that "[t]he $172, 432.87 that DIRECTV seeks to be paid into court had been DIRECTV's property. This money (and more) had been paid to it by the National Bank who claimed the money as part of the chargeback procedure. The $172, 432.87 was, in effect, taken away from DIRECTV as a part of its agreement with the National Bank. As it happens, DIRECTV also has proprietary claims and trust claims to this particular money based on unjust enrichment or conversion or perhaps waiver of tort if it is established that Mr. Gillott was a participant in the black market, gray market, or activation fraud schemes" (¶63).

Collection of Personal Information for Domain Name Registration

The Privacy Commissioner has rejected a complaint suggesting that a domain name registration company was collecting more information than required in order to make changes to web site registration information. The complaint was made by a person who operated a website in connection with an organization he ran, and who wanted to change the administration email address for the web site domain name. The web site had been suspended nearly a year after first being registered: the domain name registrar had received no replies to the renewal notices it had sent out, and so the site had been automatically suspended. The complainant claimed that the registration company had made a mistake in recording the email address through which communication with him should take place. When he attempted to have a different email address substituted, the domain name registrar sought photo identification. The complainant objected to supplying either his driver's license or passport to them, and complained that in requesting photo identification the registration company was unnecessarily gathering personal information.

The Privacy Commissioner rejected the complaint in large part because the complainant had not actually provided the requested information. In that event, there had not in fact been any gathering of personal information. However, the report also noted that the complainant had not actually been the registrant for his web site, since that process had been undertaken by his lawyer. Renewal notices had been sent to the email address provided by the lawyer. Since the complainant now wanted to change that email address, the Commissioner held, the domain name registrar needed to be certain that the complainant had the authority to make the proposed changes. Domain name hijacking is a legitimate concern, and it was reasonable for the domain name registrar to take steps to prevent it.

Requesting a driver's license or passport as identification before making a change to the administrative email address for a domain name was a reasonable requirement in order to prevent domain names from being hijacked. The request was in line with ICANN standards, to which organization the domain name registrar was accountable, and was not an excessive amount of personal information to seek. The domain name registrar's practices at the time had not made sufficiently clear the reason for the requests, but that deficiency had since been remedied.

Criminal Law – Electronic Disclosure

Conditions attached to disclosure by electronic means have arisen in *R. v. Mohammed*, [2007] O.J. No. 700 (no hyperlink available), a case concerning

one of several accused charged with terrorist offences in the Greater Toronto area. Disclosure in the case is expected to be on an enormous scale, with the Crown estimating that in printed form the material would comprise over one million pages. Further, much of the evidence was already in electronic or digital form when the police seized it from various computers, memory sticks and flash drives, and there were many thousands of intercepted private communications stored digitally or on video. Given the nature and volume of the material, disclosure in the case is being made in electronic form. Counsel for each accused is being provided with an external hard drive that can be plugged into the data port of a computer, and the disclosure is being provided in installments. At certain specified times defence counsel will return the hard drives to the prosecution, and more Crown disclosure will be added to the hard drives before they are given back to defence counsel. Lap top computers have been provided to the accused who remain in custody so that they too can review the material. In addition, defence counsel are being provided with training in the use of the software program through which the material is searchable.

The issue in this pretrial motion was not disclosure in an electronic format per se, which was preferred by all the parties. However, the Crown had prepared an undertaking for defence counsel and was refusing to make the described disclosure unless defence counsel signed it. It was the existence of some of the conditions in the undertaking which formed the substance of the dispute: in particular

2. I undertake that I will maintain custody and control over the hard drive and all disclosure material (and copies thereof) and will ensure that they are not disseminated or used for any purpose other than for the defence of this prosecution.

3. I further undertake that no one will be permitted to view the disclosure except the accused, myself, any expert hired by me, and other persons acting under my supervision.

4. I further undertake that the disclosure will not be allowed to leave my office in the possession of anyone other than myself or a member of my firm, except with the written permission of the Crown prosecutor.

5. I further undertake that to avoid the risk posed by internet hackers, the portable hard drive which has been provided to me today, will not be connected to any computer (stationary or portable) while that computer is connected to the internet.

6. I further undertake that to avoid the risk posed by internet hackers, none of the disclosure material contained on the portable hard drive will be downloaded onto any computer that is or will be connected to the internet.

7. In the event my client retains new counsel, I further undertake that I will not transfer the hard drive to other counsel but rather return the hard drive to the Crown

Some issues were not seriously in dispute. The judge accepted that it was reasonable for the Crown to impose some conditions in the context of the particular prosecutions. Further, the disposition regarding some conditions was essentially agreed at the hearing. The Crown conceded that it did not require defence counsel to maintain "custody and control" of the hard drive as condition 2 specified, and that "custody or control" would be sufficient. The Crown also agreed that the disclosure material could be shown to witnesses or potential witnesses, though condition 3 might have seemed to forbid this. The material could also be shown to outside counsel retained by defence counsel (even though condition 4 limited the material to people within counsel's firm) provided outside counsel signed similar undertakings.

The judge found that conditions 3 and 4 were too restrictive in their impact on expert witnesses who might be retained by defence counsel. Such witnesses might reasonably need to take some of the material disclosed into the field. Other expert witnesses might not be in the same city or country as defence counsel, so that viewing the material in defence counsel's office would be impractical. In these cases, though, the conditions would prevent the material leaving defence counsel's office unless prior permission was obtained from the Crown. The applicant objected that he should not be required to disclose to the Crown confidential aspects of preparation, such as which expert witnesses had been retained. The judge accepted this argument and modified condition 4. Instead, defence counsel were

required to make the expert witness aware of the undertaking, to give the expert specific instructions on the use that could be made of the information, and in particular not to disseminate it. The modified condition also specified that the material must be sent in a secure fashion: in particular it specified that the material could not be provided to the expert over the internet.

The concern over material being hacked also underlay conditions 5 and 6 about not allowing the hard drives to be connected to the internet, though in addition other concerns were reflected in those conditions. The Crown raised the concern that cookies might be surreptitiously placed into the disclosure if the computer were connected to the internet. Further, they suggested that cookies which already existed in the electronic material seized during the investigation might cause the computer to initiate communication and an unauthorized exchange of data over the internet. The judge concluded that these were legitimate concerns and that the conditions could reasonably be imposed.

Defence counsel's objection was not that it was unreasonable not to connect the hard drive to the internet, but that it unreasonably interfered with his working methods. He argued that he found it convenient to be able to move back and forth from the disclosure materials to online databases, which was not possible if the hard drive could not be connected to the internet. He suggested that it the conditions were to be imposed the Crown should provide him with a dedicated computer to use with the hard drive. The trial judge was unpersuaded, holding that the minor inconvenience to counsel's idiosyncratic work habits was not a violation of the right to full answer and defence. He also held that having a computer to view disclosure was part of the ordinary overhead in a case with many documents and that it was not the Crown's responsibility to provide an extra computer.

The rationale for condition 7, that in the event of a change in counsel the former lawyer would return the hard drive to the Crown rather than give it directly to the new lawyer, was found to be reasonable. This approach would allow the Crown to keep track of what disclosure it had made in the even of a change in counsel, which would not be unusual in a trial of this magnitude. The applicant's objection to it had been based on the belief that work done with the disclosure material would be recorded on the hard drive, and therefore available to the Crown if it were returned. The evidence led, though, was that any work performed by counsel would be recorded on the computer used to view the disclosure material, and that it would not be possible to write to the external hard drive. Consequently, the judge upheld condition 7.

Criminal Law and Sentencing

The Manitoba Provincial Court has delivered its sentence in the case of *R v. Kozun*. In this case, the accused is a 25 year old man who pleaded guilty of distributing child pornography internationally. His method of distribution involved the use of his own personal computer which he converted to a server for the purposes of electronically retaining, receiving and transmitting pictures and videos via the internet. Essentially, this style of distribution thrived on a barter system whereof participants are required to give images or videos in exchange for other images or videos. The internet was the main exchange medium used in this process. The accused's activity was uncovered by the German police authorities after they obtained passwords and downloaded 8 images from Mr. Kozun's computer. The Germans then contacted the Winnipeg Police Integrated Child Exploitation Unit regarding the activity now traced to a Winnipeg based computer. Further investigation showed that "the accused's computer was placing rotating advertisements in internet chat rooms. The advertisements offered child pornography computer files in exchange for other child pornography computer files" (¶16). In all, it was found that the accused's computer contained 3522 commercial child porn files of graphic, disturbing and escalating detail out of which 3368 were pictures and 154 were movies. The age range of the children was 8 months to 14 years.

According to the court, the major issue between the Crown and defence counsel deliberation was the availability and imposition or otherwise of a conditional sentence of imprisonment. After a review of the sentencing provisions of the Criminal Code (ss. 718, 718.1, 718.2) in regard to child pornography, the court highlights the central objectives of deterrence and denunciation. It also juxtaposes the aggravating and mitigating features of this particular case. In regard to the former, it notes inter alia that

Mr. Kozun had been involved in child porn at the age of 15. As to the latter, the court notes inter alia that his overall risk of re-offending as described by three clinical psychologists who provided services to him is variously described as low. In addition, the court found his personal presentation before the court as sincere, noting that he took personal responsibility for his conduct and pleaded guilty. The court then embarked on a two-way lengthy review of authorities in which real jail terms and conditional sentences were imposed. The court held that "absent exceptional circumstances, this type of offence must attract a term of real jail" (¶98). It, however, found that this case can be really distinguished from previous decisions that have imposed real jail terms notably, the recent Ontario Superior Court of Justice decision in *R v. Kwok*. In this case, the accused had the benefit of favourable opinion from clinical psychologists with whom he had consulted extensively. According to the court "the temporal range and depth of the rehabilitative process that Kozun has engaged is impressive and unprecedented in comparison to the case law I have reviewed". Also, unlike Kwok, Kozun pleased guilty before trial.

In sentencing Mr. Kozun to 18 months conditional sentence to be served in the community, the court notes "that a conditional sentence is a serious consequence, it has deterrent value and can be considered harsher than real jail term for various reasons" (¶78). Even though the judges are not trained to determine who is or is not a danger to the society, their decision to impose conditional sentences (as in this case) is informed by a wealth of written or oral material on each individual. Continuing, the court asserts that "[t]he conditional sentence is, in its entirety and in its philosophical thrust, an eminently reasonable and workable alternative to bricks and mortar jailhouses" (¶79). In the courts opinion, the erosion of public confidence in conditional sentence arises as a result of an inefficient correctional system. Public criticisms of conditional sentence are uninformed, the court held. Such criticisms and ridicule do not apply to "the actual law, but [to] the perceived enforcement of the law applicable to such sentenced individuals. The distinction is either easily lost or easily ignored" (¶89).

Comment on the issues raises in this case at IT.Can blog

Media Access to Surveillance Videotape

In *Re: CanWest Media Works Inc. and CTV Television Inc.* the court has allowed post-trial release of a security camera videotape of a robbery in which a person was killed. The Crown (and the convicted accused) had argued against release of the tape to the media, based on the privacy concerns of the victim's family. In particular the Crown argued that if the tape, which showed the victim being fatally shot, were released to the media it would not only be shown on national and international television but might also end up on internet sites such as YouTube.com or MySpace.com. The applicants argued that they were content to receive an edited version of the tape, even though the entire tape had been shown in open court. They only wished to broadcast the portion of the tape showing the events earlier in the robbery, based on which the accused had pleaded self-defence. The actual shooting would not be broadcast, and the victim's face would not be shown.

The Queen's Bench judge concluded that in this case the free press interest in broadcasting an exhibit filed in the course of a judicial proceeding was not outweighed by the privacy rights of the victim's family, at least in the case of an edited tape. Further, the edited tape would not distort the public's understanding, since it would still be possible to assess the self-defence claim from the proposed edited version. Accordingly the tape was ordered released.

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 Teresa Scassa, 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 Teresa Scassa, 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.