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

October 9, 2009

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.

Civil Procedure 2.0: Service via Social Media

There have recently been a number of cases, in both Commonwealth and European jurisdictions, where social media have been used as a means of original and substituted service of notices on parties involved in litigation. In an Australian decision rendered in December, 2008 (no report available, affidavits available here), a couple who had defaulted on a $154,000 loan were subjected to a court-ordered service of a default judgment order via their personal Facebook pages, after various attempts to serve them personally had failed. The judge issuing the order was reportedly satisfied by this method service because the defendants had posted their correct e-mail addresses and dates of birth on the site, which also indicated that they were "friends." In March, 2009 the New Zealand High Court in Wellington allowed service of originating documents via e-mail and Facebook on a defendant who was known to be living in an unspecified location in the U.K. The defendant, who had allegedly stolen money from the plaintiff company's bank accounts via the internet, had corresponded with the plaintiff via e-mail and was known to have a Facebook page. The judge accepted the plaintiff's argument that the usual route of newspaper ads would not be sufficient, and cited the earlier Australian decision as a precedent.

In July of 2009, it was reported that BREIN, a Dutch anti-piracy organization, had served the notorious BitTorrent tracker, Pirate Bay, via the latter's Twitter and Facebook accounts, though it was unclear whether the service was court-approved. Finally, in what was apparently the first Canadian case in which social network service was permitted, it has been reported that Master Breitkreuz of the Alberta Court of Queen's Bench issued an unreported order in the case of Knott v. Sutherland permitting substituted service via the defendant's Facebook account as one of several means of completing service.

National "Do-Not-Call" List Violations

The Canadian Radio-television and Telecommunications Commission (CRTC) has handed down several decisions with respect to complaints of violations of the national "Do-Not-Call" list.

A penalty was imposed on each of YYZ Logistics Ltd., McTavish Logistics Ltd. and Best Price Movers for making unsolicited telemarketing calls to numbers which were listed on the national "Do-Not-Call" list; under the Unsolicited Telecommunications Rules (the Rules), this may not be done without the express consent of the customer to be contacted by that telemarketer. In addition YYZ was said to have used an automatic dialing-announcement device to make unsolicited calls on its behalf; the Rules require telemarketers to make all reasonable efforts to avoid contacting a consumer in this fashion without express consent for the use of that method of communication.

All three companies (represented by the same person) made the same argument to the CRTC. They did not, in their replies to the notices of violation, dispute the underlying facts. However, they did make two arguments. First, they claimed that the rules of natural justice should permit them to cross-examine the complainants who had filed affidavits. The CRTC rejected this suggestion. In addition the three companies claimed that the national "Do-Not-Call" list violated their right to freedom of expression in section 2(b) of the *Canadian Charter of Rights and Freedoms*. The CRTC did not engage in an analysis of this claim, contenting itself with rejecting the argument on the basis that:

> The Commission notes that *Charter* rights and freedoms are not absolute and considers that the provisions applicable in this case are justified under section 1 of the *Charter*.

Because the facts underlying the claims had not been contested, the CRTC found the complaints to be justified and imposed penalties of $5,000 on each of YYZ and McTavish, and $2,500 on Best Price.

Mouldaway Canada Inc. was alleged to have initiated nine telemarketing telecommunications to consumers whose numbers were registered on the national "Do Not Call List" and also to have failed to pay the applicable subscription fees. They argued that they were exempt from the Rules on the basis that they did not directly sell products over the phone. Rather, they claimed, they only booked annual furnace inspections. However, the CRTC concluded that this amounted to promoting a service offered by Mouldaway, and therefore constituted telemarketing communications as they were defined in the Rules. "Telemarketing" means the use of telecommunications facilities for the purpose of solicitation, and the definition of "solicitation" includes the selling or promoting of a service. In that event Mouldaway had violated the Rules both by making the calls and by not paying the applicable subscription fees.

Mouldaway argued that a penalty of $4500 would severely affect the financial state of its business. Nonetheless, the CRTC concluded that a penalty of $250 for each infraction was appropriate. Since each of the nine calls constituted two infractions, the CRTC maintained the $4500 penalty.

All those ordered to pay compensation have the right to apply to the CRTC to have the decision reviewed, varied, or rescinded, and to appeal a final decision to the Federal Court of Appeal.

Privacy and Deep Packet Inspection Technology

The Assistant Privacy Commissioner of Canada has given a decision with regard to Bell Canada's possible non-compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) based on its use of Deep Packet Inspection (DPI) technology. The Commissioner explained the capability of DPI:

> Information is transmitted via the Internet using a protocol that breaks information into packets, routes that information to its destination and reassembles the information in the packets into the original content. The content (or "payload") is the user-generated information (such as e-mail content) that is surrounded by several layers of control information to ensure proper handling and routing.
>
> DPI has the capacity to see through and inspect these many protocol layers. For example, viewing down to the application layer of a packet—the layer directly above the payload—allows an ISP to determine the type of software application that is being used to transmit the packet. Depending on the particular method that an ISP adopts, being able to isolate and identify application information can be useful to the ISP's ability to manage its network traffic and reduce the traffic congestion that its clients can experience on the Internet. Some software applications are heavy users of bandwidth and are designed to use available capacity in the network in order to transmit their information. E-mail is typically a small consumer of bandwidth, while the file sharing and Peer-to-Peer (P2P) applications are large users. Applications that are often used for music and movie file sharing between computers can consume a great deal of capacity and "slow down" other Internet traffic.

The Assistant Privacy Commissioner noted that DPI itself is not new technology, but that the way in which it was being used by Bell and other ISPs was new. Bell's position was that customers using peer-to-peer (P2P) file sharing applications caused undue congestion on its network, which slowed internet service to all users during peak periods. Its solution was to target only P2P file-sharing applications and to decrease their speed during these peak periods. It did this in relation both to Sympatico subscribers and to subscribers for smaller ISPs whose traffic Bell carried on a wholesale basis.

The specific complaints in the investigation were that Bell collected and used personal information from its customers without their consent; that they

collected more personal information than was necessary to fulfill the company's stated purposes of ensuring network integrity and quality of service, and; that Bell did not adequately inform its customers of its practices and policies concerning the collection of their personal information during Internet transmissions.

A large part of the dispute in the complaint arose because of the difference between what DPI *could* be used for and what Bell was actually using it for. Potentially DPI could be used to examine subscriber usage patterns, application usage patterns, or the presence on the internet of competing services. It could even be used to examine the contents of packets sent, including emails, photo images, financial information, and so on. Bell acknowledged that DPI technology could be used to examine content, but insisted that it did not use it for that purpose.

The Assistant Commissioner found that Bell was collecting personal information, since it determined the IP addresses of customers, at least of those who were Bell subscribers. However, this was not done without consent: the internet service agreement stated that both the use and content of the subscriber's usage might be monitored, and so a subscriber would reasonably expect some personal information to be collected. In that event the first complaint, that information was collected without consent, was not well-founded. The information currently in the agreement would not be sufficient to permit an expanded use of DPI, however, and so Bell would be required to inform subscribers further if it engaged in any expanded uses.

The Assistant Commissioner also concluded that the complaint that Bell was collecting more information than necessary was not well-founded. She held that:

> managing network traffic by targeting P2P file-sharing applications in order to ensure adequate bandwidth and quality of Internet service for its customers is an acceptable business purpose for an ISP.

She accepted that this was the only thing that Bell was currently using DPI to do. She did note Bell's assurance that it would respect its privacy obligations if it did begin to use DPI for any additional purposes.

The Assistant Commissioner did find, however, that Bell had not sufficiently complied with its duty of openness under the Act to inform customers of its policies and practices. In large part her recommendations in this connection had to do with making more accessible information in various places on Bell's website and in FAQ files. Bell did disagree with one particular piece of disclosure that the Assistant Commissioner had recommended in her report of investigation: that they disclose that they collect personal information with DPI. Bell had argued that although they used IP addresses for network congestion management purposes, it did not "collect" that information because it was not retained any longer than was necessary to apply the particular traffic management policy. The Assistant Commissioner accepted that the IP addresses were not retained. Nonetheless she concluded that Bell had an obligation to disclose that it collected the personal information:

> The fact that the organization chooses not to retain the information afterwards does not discount the reality of a collection having occurred in the first place.

Accordingly Bell was expected to amend its information to subscribers in this regard.

Privacy: Monitoring Employee Calls (at a Call Centre)

In *Halifax (Regional Municipality) v. Nova Scotia Union of Public and Private Employees, Local 13*, Justice Robert Wright of the Nova Scotia Supreme Court conducted a judicial review of the decision of a labour arbitrator. The case concerned the call centre which is operated by the Municipality (HRM) and is staffed by approximately 25 members of the Union. The call centre handles general inquiries from members of the public about municipal services, taxes, by-laws, etc., and operates two separate phone lines: the "Primary Line" is used to handle incoming calls from the public exclusively, while the "Secondary Line" allows for internal calls elsewhere in the city, in order to allow customer service representatives to respond to calls on the Primary Line. Employees also used the Secondary Line on occasion to make personal calls.

In January 2007 HRM advised the Union that it had purchased and would be implementing a Call Recording technology that would record all incoming

calls in order to allow for training, quality control, monitoring of disputes, and so on. It initially planned to apply the technology to both Lines, but decided to limit it to the Primary Line because of the employees' personal calls on the Secondary Line, even though some customer calls were made on the Secondary Line. It further decided that the recordings would be stored for one year and then destroyed. The Union nonetheless grieved the plan on two bases: first, that it constituted an unreasonable use of management authority under the Collective Agreement; and second that it infringed the employees' reasonable expectation of privacy in the workplace and thus violated the privacy provisions of the Nova Scotia *Municipal Government Act* (the "privacy provisions"). The arbitrator had found for the Union on both points.

Justice Wright began by reviewing the privacy provisions, noting that one of the stated objectives of this part of the legislation was to prevent the unauthorized collection, use or disclosure of personal information by municipalities, and that "personal information" was broadly defined. He disagreed with the arbitrator's finding that "personal information" could be construed so broadly as to include "the spoken word product of HRM call centre agents in the performance of their duties to receive incoming calls from the public about municipal services" (para. 31). He specifically disagreed with the arbitrator's conclusion that, in the specific context of a call centre, a recording of an individual's voice is a source of information about a person. Such a recording, he reasoned, had no personal information component, since the calls themselves were of a non-personal nature and contained only business-oriented content. Given that both live and recorded monitoring of employee telephone calls was widespread in both the public and private sectors, His Lordship held that it would be inconceivable that the Legislature could have intended such a recording to be considered "personal information" for protection of privacy purposes. Additionally, "[n]either would it make sense for the legislation to carve out the spoken work product of call centre agents for protection under the privacy legislation from those same employees' written work product (such as e-mails, correspondence and memos) which are available for supervisors to review" (para. 45). Accordingly, he set aside this finding of the arbitrator.

Turning to whether the Call Recording technology violated the Collective Agreement, Justice Wright upheld the arbitrator's finding that the dispute was arbitrable. Rejecting an argument to the contrary by HRM, he agreed with the arbitrator that installing the technology fell within the "functions of the employer within the scope of the agreement," and thus triggered the employer's duty to "act in a fair and reasonable manner." This was because the use of the technology both created a "working condition" and constituted a "unilaterally promulgated employer rule," each of which were well within the jurisdiction of the arbitrator (paras. 52-55). On the substantive question, he upheld (on a standard of review of reasonableness) the arbitrator's findings that the employees' reasonable expectation of privacy under the Collective Agreement had been violated, because: the technology was a well-motivated but "disproportionate intrusion on the privacy interests of the call centre agents" (para. 67); and the "surveillance" was "permanent, mandatory and intrusive in the extreme," and thus was not "fair and reasonable" in keeping with the collective agreement (paras. 78-79). Wright J. noted that he was not in agreement with the arbitrator's decision on this point, but that it survived the reasonableness standard of review because it was "intelligible and transparent and [fell] within the range of the possible legal outcomes available" (para. 81).

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.