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

September 20, 2007/20 septembre 2007

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School. Part 2 of this newsletter is prepared by Professors Pierre Trudel and France Abran of the L.R. Wilson Chair in Information Technology and Electronic Commerce Law, Université de Montréal.

Les auteurs de la première partie 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. Les professeurs Pierre Trudel et France Abran de le Chaire en droit des technologies de l'information et du commerce électronique L.R. Wilson de la Faculté de droit de l'Université de Montréal ont rédigé la seconde partie du présent bulletin.

Part 1

Civil Procedure: Jurisdiction for Defamation on the Internet

The British Columbia Supreme Court has delivered its ruling in *Crookes v. Yahoo*. In this case, the plaintiff sued for defamation arising from certain postings made on the Green Party of Canada Members Yahoo Group (GPC-Group) website. The "Group" is a free service that allows individual internet users to create topic-driven online interactive discussion groups. Postings are normally e-mailed by individual members of the group. In the alternative, postings could be accessed by members of a particular group at its website. In accordance with the Yahoo Group Service, the ownership and control of a group resides in the individual who creates it. Such a person is free, however, to delegate powers of control to a select member(s) of the group (the moderator) even though the owners reserved the prerogative to determine who can be a member of a group or who can have access to its website. Access could be restricted to members only or could be open to the whole world. The GPC-Group is a restricted access group. The majority of its members are full registered users of Yahoo! With Yahoo! ID while the rest are essentially invited members who receive specific postings but do not have access to the website. Yahoo! Inc., a company registered in Delaware with head office in Sunnyvale, California does not prescreen postings on its "Group" websites, but following a complaint, it reviews implicated postings to assess compliance with its terms of service. It pulls down any posting that it adjudges non-compliant. It has no way of knowing whether the offensive posting is later reposted.

In part, the plaintiff's case here is that Yahoo! is the host ISP for the GPC-Group website and that it has control over the content of the website. The plaintiff joined Yahoo! Inc. in this action mainly on the basis that "it provided the means by which the defamatory material was published and that it failed to remove the postings" (¶12) even though it was aware of the alleged defamatory material. In the past, the plaintiff had complained to Yahoo! by e-mail about the offensive publication and after providing necessary details as requested by Yahoo!, the latter pulled down the impugned publication. This was an experience over which the plaintiff expressed satisfaction. However, in the present proceedings, the plaintiff claims that the same material was reposted in the GPC-Group website. Instead of exploring the earlier approach that proved successful, the plaintiff now retained the services of a lawyer who wrote to Yahoo! demanding that the impugned material be pulled down. Proof of the receipt of counsel's letter by Yahoo! was inconclusive and there was no follow-up action on the part of the plaintiff or his counsel before the present action was brought.

The plaintiff's writ of summons and statement of claims were endorsed pursuant to s.10 of BC *Court Jurisdiction and Proceedings Transfer Act*, (CJPTA) 2003 (which came into effect in 2006 and provides for circumstances for service *ex juris* without leave). The plaintiff claims that the BC Supreme Court has territorial competence to hear the case on the basis of a presumed real and substantial connection between BC and the facts of this case. Plaintiff argues that the tort of defamation was committed in BC hence there is no need for leave of court. Under rule 14 of the Rules of Court, a defendant can apply to have the court strike out the plaintiff's claims on jurisdiction in the originating process and other

proceedings or to apply for stay of the proceedings for plaintiff's misleading jurisdictional claims. In such case, the court may require supplemental affidavit from the defendant to debunk the presumption of accuracy of the jurisdictional claims made by the plaintiff to assist it in weighing the claims of both parties.

The court held that the onus is on the plaintiff to establish the right to serve a defendant *ex juris* without leave of court. It noted that "[I]t is when a person downloads the impugned material from the internet that the damage to the reputation may have been done and it is at that time and place that the tort of defamation is committed" (¶26). In this case, the plaintiff has not established that anyone in BC has downloaded the material. Both the publication of the impugned material and the tort of defamation were not established as occurring in BC. The court rejected the plaintiff's reliance on *Burke and Wiebe*. In the first case, the impugned material was in a site accessible to the public and there was evidence of publication in BC. In the second case, the material was under the control of the defendant. Thus, the facts of these two cases do not match up to the present one. Specifically, the court found that "[t]he plaintiffs have not asserted that anyone in British Columbia downloaded or read the alleged libel. The only allegation is that an unnamed friend of Mr. Crookes, at an unknown location, directed Mr. Crookes to the material on the GPC-Members website" (¶22). It also held that neither the individual nor corporate defendants in this case reside in British Columbia. It concluded that the plaintiff had failed to demonstrate that there is a real and substantial connection between the cause of action against Yahoo! and British Columbia.

Criminal Law: Possession and Distribution of Child Pornography

In *R. v. Dabrowski*, the accused had been acquitted at trial of five charges, among which were making, possessing and distributing child pornography, in the form of a videotape, and uttering a threat by telephone. The Crown appealed the acquittals on the two charges of possession and distribution of child pornography. The case arose from the 28-year old accused's relationship with the 14-year old complainant, wherein the two had made video recordings of themselves having sex. The trial judge had ruled that the complainant had consented to the making of the recordings, and that they fell into the exception (laid out by the Supreme Court of Canada in *R. v. Sharpe*, where they interpreted section 163.1 of the *Criminal Code*) which made it lawful to possess pornographic materials which were intended only for private use. The Crown appealed this ruling on the basis, *inter alia*, that "the trial judge did not resolve a crucial factual question, namely, whether the respondent threatened to show the videos to the complainant's family and friends if she did not comply with his rules in certain areas" (para. 11).

MacPherson J.A. for the Court of Appeal reviewed the trial judge's findings, and noted that she had considered evidence from the complainant that the accused made two kinds of threats: (1) that he would have third parties physically injure her if she did not follow his rules about where she could and could not go socially; and (2) that if she did not follow these rules he would "show the videos to her family and friends or put them on a website" (para. 18). Justice MacPherson found that, while the trial judge had ruled that the complainant was not credible regarding the first kind of threats, she had not made a ruling as to whether the second kind of threats had actually been made. He noted that the two kinds of threats were quite different from each other, and further that whether the threats to share the recordings or put them on the Internet had actually been made was an essential factual issue in the case. This was because the "private use" exception from *Sharpe* was not available in any situation where the materials were shown to be held with any intention other than their private use. Therefore, her failure to make a ruling on whether these threats had been made prevented her from properly applying section 163.1.

The Court also commented that the trial judge had been correct to reject a Crown submission that the exception only applied where the accused had maintained exclusive possession over the materials and not shared them with anyone in any way. Justice MacPherson noted that this "would render unlawful such activities as placing these videotapes in a safety deposit box or turning them over to a lawyer or other trusted person for safekeeping" (para. 29). Whether such materials were being held in strict

privacy, and were thus covered by the exception, was a factual question to be determined on the evidence in each case. The Court allowed the appeal and directed a new trial on the two charges of possession and distribution of child pornography.

Privacy: DRM and Consumer Privacy

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) has just released a report entitled *Digital Rights Management and Consumer Privacy: An Assessment of DRM Applications Under Canadian Privacy Law*. The study, which was funded by the Office of the Privacy Commissioner of Canada, concludes that various DRM technologies used in Canada in connection with goods and services (including Apple's iTunes products, CDs from Warner and Sony, and a Disney DVD) actually fail to comply with the basic requirements of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. The personnel conducting the study observed various modes of data collection, as well as tracking of usage and surfing habits, which are not disclosed to the consumers of the products. This stems in part, the report explains, from the position taken by many organizations that IP addresses do not constitute "personal information" under *PIPEDA*. The study explicitly concludes that "DRM is currently being used in the Canadian marketplace in ways that violate Canadian privacy laws" (Executive Summary, p. 10).

Privacy: Street Level and Satellite Photography

The Privacy Commissioner of Canada, Jennifer Stoddart, recently released a statement expressing serious concern about how the use of satellite, aerial and street-level photo images may impact Canadians' privacy. Recent technological developments have seen the increasing availability of high-resolution and detailed satellite photos of all manner of populated areas, from downtown cores and arteries to residential neighbourhoods. In addition, a number of commercial companies are now engaged in street-level photography as a means of gaining content for on-line mapping technology. These techniques can capture extremely detailed views of the areas being surveyed, and can produce images in which individuals are identifiable. The Privacy Commissioner noted as an example that Google Street View has "produced photographs of locations in the United States that include: a young child standing inside a motor vehicle and looking out the half-open driver's window from approximately a one-meter distance; and a child on the front lawn of what appears to be a private dwelling, from approximately three meters' distance."

Along with the statement the Privacy Commissioner has published letters which she sent to both Google and Immersive Media Corp. The latter is a company based in Calgary that maintains a "GeoImmersive Database" which, the company's website claims, contains 40,000 miles of photographic images taken throughout North America—including several cities in Canada. GeoImmersive supplies these images to Google for the Google Street View, which as yet has only been launched in the U.S. In her letter to Immersive Ms. Stoddart expressed her concern that the database contained images of Canadians which were taken without their consent, and which were clear enough to constitute "personal information" about those individuals within the meaning of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. *PIPEDA* and provincial counterpart legislation generally require that businesses obtain personal information only by consent, and commercial use or disclosure of the information also requires consent. The letter states: "Your company is now making the images commercially available, presumably to anyone who wishes to enter into a licensing agreement. This would appear to run counter to the basic requirements of knowledge, consent, and limited collection, use and disclosure as set out in *PIPEDA*." She has requested a response from Immersive on the matter.

2ième partie

Obligation de prouver de façon prépondérante que les appels n'émanent pas de la ligne téléphonique de l'abonné

Le demandeur réclame de Bell le paiement de frais d'appels interurbains en Autriche qu'il lui a payés mais qu'il considère lui avoir été facturés de façon erronée car il n'a effectué aucun appel en Autriche. La facture indique que l'appel téléphonique avait été effectué à partir de sa résidence. La défenderesse a invoqué que certains appels interurbains se font à partir de certains pays à partir de numéros de téléphone obtenus licitement de visiteurs de certains sites qui inscrivent leur numéro sur ces sites en vue d'obtenir un accès à des contenus ou activités proposés par ces sites web. Invoquant la décision du CRTC du 9 mars 2005 selon laquelle « les abonnés sont les mieux placés pour contrôler les appels faits à partir de leurs lignes téléphoniques ou qui sont acceptés sur ces lignes », le tribunal estime que, dès lors que Bell a établi que les appels ont été logés à partir de la ligne téléphonique du client, le fardeau de prouver de façon prépondérante que les appels n'émanaient pas de son téléphone revient à l'abonné.

Commentez cet article au Blogue de IT.CAN

- *Rochefort c. Bell Canada*, Cour du Québec, division des petites créances, 2007 QCCQ 9186 (CanLII), 26 juillet 2007.
- Voir également : *Lesage c. Bell Canada*, Cour du Québec, division des petites créances, 2007 QCCQ 9720 (CanLII), 1er août 2007.

Un Livre blanc sur la gestion des noms de domaine

Les noms de domaine sont désormais omniprésents dans le fonctionnement d'Internet : il est devenu impossible à une entité voulant exister sur le Net de se passer de noms de domaine associés à son nom, à ses enseignes ou à ses marques. Publié sous les auspices du Club des noms de domaine (www.club-nd.fr) et de DNS-News.fr, ce Livre blanc sur la gestion des noms de domaine vise à présenter, de façon synthétique, l'essentiel de ce qu'il faut savoir en matière de gestion de noms de domaine. L'ouvrage aide le lecteur à identifier les principales questions à prendre en considération, soit en tant que responsable direct, soit en tant que personne associée à la gestion des noms de domaine d'une entreprise ou d'une collectivité.

La gestion des noms de domaine permet d'assurer au moins trois objectifs stratégiques soit : être présent, s'identifier et exister dans le cyberespace.

Le Livre blanc présente ainsi deux "matrices" fondamentales pour bien visualiser les choses. D'abord, qu'est-ce qu'une stratégie de noms de domaine ? C'est une approche fondée sur l'analyse des besoins de l'entreprise en regard des possibilités offertes par son environnement. Cela suppose que l'entreprise ait fait le point sur ses besoins en matière de présence Internet et qu'elle les tienne à jour. Le deuxième pilier de la stratégie "de base" est la maîtrise des risques, dans une logique d'assurance, avec la mise en place d'outils de surveillance et le traitement rapide des situations litigieuses. Les raisons que l'on peut avoir de déposer des noms de domaine sont aussi examinées. Il peut s'agir de motifs liés à la visibilité qu'on souhaite en retirer ou de la protection que leur enregistrement va apporter à une marque. L'étude de nombreux portefeuilles d'entreprises montre une surpondération des noms déposés pour la protection au détriment de ceux qui ont été déposés pour la visibilité. À budget constant, certains portefeuilles pourraient être plus efficients s'ils étaient réajustés : ils coûteraient moins cher et rapporteraient plus de trafic.

Face à un environnement complexe et mouvant, l'entreprise doit chercher à se doter d'outils qui lui permettront d'anticiper d'éventuelles opportunités comme d'éventuelles menaces. Pour ce faire, la définition d'une stratégie de nommage assortie d'une charte, l'organisation des interactions entre les différents intervenants concernés par le dossier, ainsi que la mise en place d'outils de veille performants sont des atouts indispensables pour toute structure désireuse de se construire une présence sur Internet solide et efficiente.

- Loïc DAMILAVILLE, *Livre blanc sur la gestion des noms de domaine*, édition 2007.

Les pratiques du commerce électronique

« Le mythe du 'vide juridique' à propos d'Internet a fait long feu » constate la préface de cet ouvrage faisant le point sur le cadre juridique et les pratiques de certaines des activités les plus importantes se déroulant dans le cyberespace. Les technologies de l'information constituent pour le législateur un défi permanent. Le cadre juridique et les pratiques du commerce connaissent des ajustements continus pour tenir compte des spécificités du commerce électronique. Le cadre juridique est sans cesse tiraillé par l'apparition de nouvelles pratiques sur les réseaux numériques. La publicité en ligne prend des formes plus variées et plus originales que jamais ; les ventes aux enchères ont trouvé sur Internet une nouvelle jeunesse ; les jeux, concours, loteries et paris en ligne connaissent un succès grandissant ; les plates-formes se multiplient pour favoriser la vente de particulier à particulier ; les mineurs deviennent sur Internet des consommateurs particulièrement actifs qu'il faut séduire à tout prix ; les protections et règles de forme prévues par la loi sont habilement contournées… Comment la loi sur les pratiques du commerce résiste-t-elle à ce mouvement perpétuel ? Des adaptations sont-elles toujours nécessaires ? La directive européenne sur les pratiques commerciales déloyales à l'égard des consommateurs va-t-elle apporter des changements majeurs dans le secteur ? Autant de problèmes que ce livre se propose d'examiner.

Dans un chapitre consacré à la publicité sur Internet, Étienne Montero passe en revue les principes généraux applicables sur le net et aborde les problèmes, parfois les fléaux, associés à l'activité publicitaire comme les pop-ups, le référencement, le splog, le marketing viral, le spin et le split. Dans un texte sur les contrats conclus par les mineurs sur Internet, Marie Demoulin examine les échappatoires de la loi belge sur les pratiques du commerce à l'égard des transactions en ligne impliquant des personnes mineures. Thibault Verbiest présente une revue du droit belge applicable aux jeux et paris sur Internet. Ce chapitre aborde le phénomène en tenant compte des principes du droit communautaire. Deux chapitres traitent de la vente aux enchères en ligne. Le droit est envisagé du point de vue du consommateur dans un chapitre rédigé par Marc Vandercammen tandis que Tanja De Coster présente une analyse du cadre juridique du site e-Bay. L'ouvrage est complété par une étude de Hervé Jacquemin sur les formes applicables à certains contrats conclus par voie électronique.

- CENTRE DE RECHERCHES INFORMATIQUE ET DROIT, *Les pratique du commerce électronique*, Cahiers du Crid no. 30, Bruxelles, Facultés universitaires Notre-Dame de la Paix de Namur, Bruylant, 2007, 191 p.

À signaler :

- Sulliman OMARJEE, « Streaming : Dailymotion et Myspace sont responsables ! », *Droit et technologies*, 13 septembre 2007.

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 if they relate to Part 1 or Pierre Trudel at pierre.trudel@umontreal.ca if they relate to Part 2.

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 la première partie du présent bulletin, veuillez contacter les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan à l'adresse électronique it.law@dal.ca ou en ce qui concerne la deuxième partie, veuillez contacter Pierre Trudel à pierre.trudel@umontreal.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.