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

July 8, 2004/8 juillet 2004

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Anne Uteck and Teresa Scassa 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 Anne Uteck et Teresa Scassa 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

Copyright Law

The long-awaited Supreme Court of Canada decision in the *Tariff-22* case (*SOCAN v. CAIP*) was handed down on June 30, 2004. The case addressed issues of liability for copyright infringement arising from the downloading of music on the Internet.

The Court issued a split decision. Writing for a substantial majority, Binnie J. began by reiterating the "balancing approach" to the interpretation of the *Copyright Act* set out by the Court in *Théberge*. Expressing this approach in Internet terms, Binnie J. wrote: "The capacity of the Internet to disseminate "works of the arts and intellect" is on e of the great innovations of the information age. Its use should be facilitated rather than discouraged, but this should not be done unfairly at the expense of those who created the works of art and intellect in the first place." (at para 40).

One of the most difficult issues before the court related to the problem of locating liability for copyright infringement in a borderless Internet context. The Copyright Board had ruled that for a work to be communicated to the public by telecommunication, it must originate from a host server located in Canada. The majority of the Court overruled this decision, find that the test was "too rigid and mechanical". (at para 44). Instead, the majority opted to use the "real and substantial connection test" developed in the conflict of laws context, and already applied in a number of Internet related cases. The majority took the view that such an approach was consistent with practices in other comparable jurisdictions, such as the European Union, Australia, France and the United States, and was consistent with Canada's obligations under the as yet unratified *WIPO Copyright Treaty*.

It was on this point that LeBel J. dissented. In his view, the real and substantial connection test is more appropriate for use by courts to determine whether they should take jurisdiction over a dispute, and should not be used to determine whether, as a matter of statutory interpretation, a statute applies to a specific fact situation. LeBel J. would have upheld the Board's approach because "it is sound from an operational perspective; it provides the requisite predictability and best accords with the meaning and purpose of the *Act*." (at para 135). In his view, the real question was "whether Parliament did in fact intend that s. 3(1)(*f*) of the *Act* apply extraterritorially." (at para 143) In his view it did not. He was critical of the majority approach on the basis that it could lead to "a layering of royalty obligations between States" (at para 152) and because it might have an adverse impact on the privacy of Internet users by encouraging "the monitoring or collection of personal data gleaned from Internet-related activity within the home." (at para 153).

The Court was unanimous with respect to the other issues on appeal. It is now clear that s. 2.4(1)(*b*) applies to Internet Service Providers (ISPs). Binnie J. rejected a characterization of this provision as an exception from liability that should be construed narrowly. Rather, he framed it as "an important element of the balance struck by the statutory copyright scheme." (at para 89). Binnie J. accepted the main points of the Board's decision with respect to s. 2.4(1)(*b*), and confirmed that "So long as an Internet intermediary does not itself engage in acts that relate to the content of the communication, *i.e.*, whose participation is content neutral, but confines itself to providing "a conduit" for information

communicated by others, then it will fall within s. 2.4(1)(*b*)." (at para 92).

The Court also found that the use of caches by ISPs as a means of improving the performance of their facilities did not give rise to copyright infringement. Binnie J. noted that the "creation of a "cache" copy, after all, is a serendipitous consequence of improvements in Internet technology, is content neutral, and in light of s. 2.4(1)(*b*) of the *Act* ought not to have any legal bearing on the communication between the content provider and the end user." (at para 115).

It had been argued that ISPs could be held liable for authorizing infringement, particularly in a context where they knew how much content was available on the Internet, and how attractive it would be to their customers. Perhaps not surprisingly, giving their recent decision in *CCH Canadian v. Law Society of Upper Canada*, the Court rejected this argument. While accepting that the Internet was a much more complex kind of technology than a photocopier machine, they nonetheless found that, as in *CCH Canadian*, there was a large volume of non-copyright material also available on the Internet, and that "it is not possible to impute to the Internet Service Provider, based solely on the provision of Internet facilities, an authority to download copyrighted material as opposed to non-copyrighted material." (at para 123). The Court did suggest, however, that there might be some circumstances in which an ISP might be found to have authorized a copyright infringement. These circumstances might include ones where the ISP has been given notice that infringing materials are hosted on its system. However, even in such circumstances the Court was wary of suggesting that liability would be a given, and indicated that "[m]uch would depend on the specific circumstances." (at para 127). The Court noted that if "notice and takedown" procedures were desirable, they should be crafted by Parliament, and not left to judicial interpretations of "authorization".

Recent Articles:

Heer, Christoper, "The Case Against Copyright Protection of Non-literal Elements of Computer Software", (2004) 18 I.P.J. 1.

Discovery

Recent Articles:

Freedman, Bradley J., "Discover of Electronic Records Under Canadian Law – A Practical Guide", (2004) 18 I.P.J. 31.

Privacy

The Office of the Privacy Commissioner of Canada has released several new Findings under the *Personal Information Protection and Electronic Documents Act (PIPEDA)* including two involving workplace surveillance and one dealing with automated telephone messages.

In Finding #268, three former airline employees complained that the company attempted to collect and use their personal information without their knowledge and consent via a digital recorder taped to the underside of a table in a smoking room accessible to employees and the public. The company argued that it did so in a context that would be permissible under s.7(1)(b) of the *Act* because it had placed the complainants under investigation for malicious gossiping, suspicions of theft, placing liquid Ex-lax in red wine stored in the kitchen refrigerator and mismanagement of the parking gate. While a variety of reasons for suspecting the complainants were provided by the company to the OPC, there was no direct evidence to support the company's suspicions or allegations. However, since the tape had been erased there was no evidence that the complainants' personal information had been collected or used leaving the Assistant Privacy Commissioner to conclude that the company was not in contravention of the *Act* and thus, the complaint was not well-founded. Notwithstanding, Assistant Commissioner Black makes clear that her finding should not be interpreted as an approval of what the company attempted to do. She indicates that had personal information been collected via the digital recorder under these circumstances, she would not have been inclined to allow the company to rely on s.7(1)(b) to justify the collection of personal information. According to Assistant Commissioner Black, placing a tape recorder in a room accessible to many individuals "is a highly indiscriminate means of collecting information" and should only be "the very

last step..if taken at all" and only where a suspected breach of the employment contract is based on substantial evidence and less privacy-invasive measures of obtaining the information are exhausted.

Surveillance of a former employee was also at issue in Finding #269. The complainant alleged that the company had collected his personal information by way of video surveillance and used that information to terminate his employment. The company relied on s.7 to collect and use the complainant's personal information without his knowledge and consent. During the course of the complainant's employment, there were on-going health-related issues and, according to the Assistant Privacy Commissioner, on-going efforts by the company to accommodate the employee and obtain up-to-date medical information without success. The results of an independent assessment "did not refute a growing suspicion on the part of the employer that the complainant was not accurately representing the state of his health." A private investigator was finally hired to conduct video surveillance to determine the validity of the complainant's physical limitations, the results of which were used as evidence that the complainant had misrepresented the state of his health. Because there was no question that the complainant's personal information had been collected and used without his consent, the issue was whether s.7(1)(b) applied. Reiterating earlier Findings, Assistant Commissioner Black noted that in order for a company to successfully rely on s.7(1)(b), a company must have substantial evidence to support their suspicions, that it has exhausted all other means of obtaining the information in less privacy-invasive ways and the collection of personal information is limited, as far as possible, to the purposes for which it is necessary. The Assistant Commissioner was satisfied that the company had met the requirements necessary to rely on s.7 having reasonable and probable grounds to believe the employee was in violation of the employment contract. Thus, the complaint was held to be not well-founded. She did, however, go on to recommend that the company "formalize the steps it took by developing policy and practices" taking into account that video surveillance should only be used as a last resort, the decision to conduct surveillance should be made at a very senior level and private investigators should be instructed to collect personal information in accordance with Principle 4. The company was given 120 days to report back regarding the policy.

In Finding #270, an individual claimed that her bank improperly disclosed her personal information when it left an automated voice message on her answering machine that automatically broadcasts messages stating that she was behind on making a payment on her credit card. The message indicated who was calling, that the cardholder is behind in making a payment and provides a toll-free number. Because the cardholder's name was not mentioned on the message, the bank argued that it had not disclosed any personal financial information and therefore, there was no contravention of the consent provisions of the *Act*. In the alternative, the bank argued that s.7(3)(b) allows for the disclosure of personal information without consent for the purpose of collecting a debt. With respect to whether the information was personal information as defined under s.2 of the *Act*, the Assistant Commissioner noted that an individual does not have to be named for something to constitute her personal information, but rather, she has to be simply, "identifiable." In this case, although the message did not name the complainant, it was sent to her telephone number which she had provided to the Bank and she was the only credit card holder in the household. Thus, she was identifiable as the individual for whom the message was intended and the information was the complainant's personal information in accordance with s.2. The Assistant Commissioner also determined that the exception to consent under s.7(3)(b) did not apply here. The Bank used the complainant's personal information to collect a debt, but it did not intend to disclose this information to her husband who had heard the message, the overdue payment does reveal sensitive financial information and alerting customers to a problem could be done in a more "privacy-conscious manner." Because the Bank acknowledged this and agreed to review and change its automated messages, the complaint was resolved.

Recent Articles:

Geist, Michael A., "Computer and E-mail Workplace Surveillance in Canada - The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance", (2003) 82 Can. Bar Rev. 151.

2ième partie

Règles d'utilisation des mécanismes de vidéosurveillance – Québec

La Commission d'accès à l'information a publié des règles sur l'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics. Ces règles s'appliquent aux organismes publics qui mettent en place des mécanismes de vidéosurveillance dans des lieux publics. Elles ont valeur de recommandation puisque rien dans la loi ne permet à la Commission de conférer un caractère obligatoire à de telles règles.

La CAI rappelle que dès lors que la vidéosurveillance a pour effet de recueillir sur un support des renseignements personnels sur des individus identifiables, les organismes publics ont le fardeau de s'assurer que cela est nécessaire à l'exercice de ses fonctions ou à la mise en oeuvre d'un programme dont il a la gestion. Dans chaque cas, l'organisme doit être en mesure d'établir que l'objectif poursuivi est suffisamment important pour justifier la cueillette de renseignements personnels. L'objectif doit être sérieux et la CAI recommande de réaliser un rapport des risques concrets et des dangers réels que présente une situation pour laquelle on veut avoir recours à la vidéosurveillance au regard de l'ordre public et de la sécurité des personnes. Les organismes sont aussi invités à documenter leurs analyses au sujet des solutions de rechange moins dommageables pour la vie privée.

L'impact réel de la vidéosurveillance doit être mesuré. Sa finalité ne doit pas pouvoir être détournée et donner lieu par exemple à du profilage, à catégoriser ou hiérarchiser des groupes de personnes ou établir des distinctions selon l'appartenance raciale, religieuse ou politique.

La CAI fait des recommandations sur la collecte et la gestion des renseignements personnels. Elle invite les organismes à se doter de politiques inspirées de ses recommandations en matière de vidéosurveillance de même qu'assurer une révision régulière de leurs pratiques et politiques en ces matières.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, 9 juin 2004.

Rapport sur le gouvernement en ligne – Québec

L'adjoint parlementaire du premier ministre, M. Henri-François Gautrin, a déposé le *Rapport sur le gouvernement en ligne*. Fruit d'une réflexion de près d'un an et de multiples rencontres avec les intervenants du monde gouvernemental, du secteur privé et du milieu de la recherche, le rapport explore en détail les divers éléments de cette priorité gouvernementale, qui a pour principal objectif d'améliorer les services aux citoyens et aux entreprises du Québec. « Le gouvernement en ligne dépasse de loin la simple prestation électronique de services », a rappelé l'auteur du rapport. « Il vise aussi une meilleure transparence de l'administration publique, une participation accrue des citoyens aux processus démocratiques et une économie plus concurrentielle, entre autres grâce à des processus administratifs simplifiés et à une diminution des coûts de gestion, ce qui s'avère essentiel à la compétitivité de nos entreprises, dans un contexte de mondialisation ».

Rapport sur le Gouvernement en ligne : Vers un Québec branché pour ses citoyens, juin 2004.

Critères de la diffamation lors d'un débat public – Québec

Dans cette décision, le défendeur Gervais a participé à une émission télévisée d'affaires publiques pour critiquer l'hôpital, où il oeuvrait à titre de bénévole, et la façon dont il a été congédié. À cette occasion, le directeur de l'hôpital déclare en ondes que le bénévole est un « impulsif compulsif » et souligne que de nombreuses plaintes ont été portées contre celui-ci. L'action fondée sur la diffamation et l'abus de droit a été accueillie en partie en première instance.

La cour d'appel infirme la décision. Elle considère que lorsqu'un commentaire est prononcé dans le cadre d'un débat public, il importe de considérer le contexte du débat dans lequel s'inscrit la déclaration. En allant étaler ses reproches à l'endroit de l'hôpital à la télévision, Gervais devait s'attendre à ce que la

parole soit donnée aux représentants de l'hôpital et à ce que ceux-ci répondent à ses accusations. L'expression « impulsif compulsif », en plus de ne pas répondre aux critères de l'injure, est une opinion du directeur sur un comportement constaté dans son établissement et ne constituait pas une attaque en règle. Dans les circonstances, l'opinion se situait à l'intérieur du seuil permis dans notre société en termes de liberté d'expression.

Bouffard c. Gervais, Cour d'appel, 500-09-010807-014, 2 juin 2004.

Propriété de la ligne téléphonique et vie privée – Québec

Dans *Courtemanche c. Poisson*, le défendeur veut mettre en preuve une conversation téléphonique entre son amie et le demandeur afin de prouver que ce dernier est auteur de vandalisme commis sur ses biens. Il y a objection à l'admissibilité en preuve des propos tenus lors de la conversation téléphonique au motif que la preuve aurait été obtenue en violation du droit à la vie privée des deux personnes participants à la conversation. Le défendeur soutient, quant à lui, que l'interception est légitime puisqu'il s'agit de sa ligne téléphonique.

La cour rappelle que la question doit être décidée non pas en fonction de la propriété du téléphone, mais bien en fonction de la conversation elle-même. L'amie du défendeur était en droit de s'attendre à pouvoir communiquer de manière privée au téléphone avec le demandeur, même si elle utilisait la ligne téléphonique du défendeur. La conversation était de nature privée.

Courtemanche c. Poisson, Cour supérieure, 505-05-004550-981, 8 janvier 2004.

Utilisation de l'adresse électronique de l'employeur à des fins autres – Québec

Le défendeur, cadre haut placé dans la compagnie demanderesse, a publié un texte litigieux sur un forum de discussion et signé de l'adresse de courriel fournie par son employeur et réservée exclusivement aux employés de la compagnie. L'employeur réclame des dommages-intérêts suite à la parution de l'article étant donné qu'il a eu des problèmes d'obtention de financement.

Le tribunal estime que l'adresse internet fournie par l'employeur à ses employés lui appartient et qu'elle est mise à leur disposition que pour les fins de leur travail. L'utilisation sans permission du nom de la demanderesse constitue une atteinte à la vie privée. Le défendeur a également enfreint son devoir de loyauté. Étant donné sa position dans l'entreprise, il aurait dû savoir que l'utilisation de l'adresse internet fournie par l'employeur pourrait causer des dommages à ce dernier, surtout si telle utilisation était douteuse.

Arpin c. Grenier, Cour du Québec, Division des petites créances, 700-32-011739-032, 7 mai 2004.

Responsabilité pour des frais d'interurbains résultant de fraude sur Internet – Québec

Le demandeur a visité un site qualifié d'« attrape touriste ». Suite à l'utilisation de ce site, il a été facturé par Primus Canada de nombreux frais d'appels interurbains logés à son insu à Saotomprin en Nouvelle-Guinée. La Cour rejette les prétentions de la société de télécommunications selon lesquelles elle ne peut, sans violer la vie privée, s'immiscer dans les communications que les clients effectuent sur Internet. La responsabilité est imputée à part égale au client et à la société exploitante de télécommunications. Cette dernière est bénéficiaire des frais d'interurbains et doit supporter une part de responsabilité quant à la protection des intérêts de ses clients. Quant au client, il doit demeurer vigilant quant au choix des sites qu'il visite.

Sans c. 3362426 Canada Inc. Cour du Québec, Division des petites créances, 500-32-075612-038, 27 mai 2004.

Norme internationale de qualité pour les radiodiffuseurs

La Fondation Média & Société de Genève a rédigé une norme internationale de qualité pour les entreprises de radiodiffusion. La norme ISAS BC 9001 est destinée aux radios, télévisions et producteurs

de contenus sur Internet. Il s'agit d'une adaptation de la norme ISO 9001 pour les entreprises de radiodiffusion et les producteurs de contenus sur Internet. La norme a été réalisée par un comité d'experts internationaux. Elle vise à assurer la qualité des prestations des diffuseurs aussi bien du point de vue des gestionnaires, des annonceurs que du public en général.

ISAS, Norme internationale, Systèmes de management de la qualité, exigences pour les radiodiffuseurs (radio, TV et sites internet associés).

Le réseautage de l'information en santé – Québec

Rédigé par une équipe multidisciplinaire de spécialistes en éthique, philosophie, droit, sociologie, science politique et évaluation sociale des technologies, ce manuel vise à promouvoir l'identification, l'évaluation et la gestion des questions éthiques et sociales du réseautage de l'information de santé.

Diane L. DEMERS, François FOURNIER, Marc LEMIRE, Pierrot PÉLADEAU, Marie-Claude PRÉMONT et David J. ROY, *Le réseautage de l'information de santé : Manuel pour la gestion des questions éthiques et sociales*, Montréal, Centre de bioéthique de l'Institut de recherches cliniques de Montréal, 2004, 268 pages.

Comment lutter contre le racisme sur Internet? – Forum

Dans le prolongement de la réunion de Paris de l'OSCE (Organisation pour la Sécurité et la Coopération européenne), le Forum des droits sur l'internet tient du 18 juin au 18 octobre 2004 un forum de discussion sur les moyens de lutter contre le racisme, l'antisémitisme, la xénophobie sur l'internet. Les contributions feront l'objet d'une synthèse, qui sera remise au secrétaire d'État aux Affaires étrangères de France en vue des prochaines conférences de l'OSCE sur la tolérance et la lutte contre le racisme de Bruxelles (septembre 2004) et de Sofia (décembre 2004). Un dossier est proposé sur le thème et les internautes sont invités à faire connaître leurs points de vue en participant au forum.

Forum des droits sur l'internet, *Forum racisme, xénophobie et antisémitisme sur internet : que faire?*.

Le Conseil constitutionnel censure des articles de la loi pour la confiance dans l'économie numérique – France

La *Loi pour la confiance dans l'économie numérique* a été publiée au Journal officiel le 22 juin 2004 (disponible à http://www.droit-technologie.org/3_1.asp?legislation_id=189). Ce texte intègre les modifications imposées par le Conseil constitutionnel dans sa décision du 15 juin dernier. Ces modifications portent principalement sur le droit de réponse et la prescription en ligne.

CONSEIL CONSTITUTIONNEL, Décision no 2004-496 DC – 10 juin 2004.

Voir également :

Benoît TABAKA, *Le Conseil constitutionnel rase une partie de la LEN*, Juriscom.net, 15 juin 1004.

À signaler

La professeur Sylvette Guillemard de la Faculté de droit de l'Université Laval a remporté le Prix du concours d'essai juridique de l'Association canadienne des professeurs de droits pour l'article intitulé *Le "cyberconsommateur" est mort*, vive l'adhérent, (2004) 131 *Journal du droit international*, 7-61.

Le 22 juin 2004, le sénat français a voté une proposition de loi visant à protéger les noms des collectivités locales et des élus sur internet. *Proposition de loi tendant à protéger le nom des collectivités territoriales et des fonctions électives sur internet*.

En France, un projet de loi relatif à la garantie de la conformité du bien au contrat due par le vendeur au consommateur et à la responsabilité du fait des produits défectueux vise à établir un nouveau régime de responsabilité en matière de droit de la consommation, http://www.foruminternet.org/actualites/lire.phtml?id=738.

Sandrine ROUJAT, *Première loi "anti-spyware", source de nombreux conflits d'intérêts*, Juriscom.net, 10 juin 2004.

Sandrine ROUJAT, *SPAM : entreprises, internautes, défendez-vous*, Juriscom.net, 24 juin 2004.