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

October 18, 2007/18 octobre 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

Domain Name Dispute Resolution Decisions

In *ABELSoft Corp. v. Nissanov*, sole panellist Dennis Magnusson considered a dispute over the domain names abelmed.ca and abeldent.ca. The Complainant, ABELSoft, is a Burlington-based provider of office management computer software for medical professionals, and has a North-America wide market for its products. It has registered the trademarks "ablemed" and "abeldent" in relation to its products, as well as the domain names ablemed.com and abeldent.com. The Registrant was an employee or officer of Toronto-based Antibex Software, which advertised itself as a company that sells software to medical professionals for management of their practices. He had registered the disputed domain names, and each of the corresponding websites resolved to the website of Antibex Software.

The Registrant did not file a Response to the Complaint, and the Panellist found that the Complainant had met its burdens of proof under the CIRA Domain Name Dispute Resolution Policy requirements. The Panellist noted that when considering whether a domain name is "confusingly similar" to a Mark owned by a complainant, the "dot-ca" suffix is ignored. In this case, the domain names and the marks were identical, and thus the domain names were likely to be mistaken for the marks. In assessing whether the domain names had been registered in "bad faith," the Panellist found that the Registrant was clearly a competitor of the Complainant, and that the effect of diverting potential customers to the Registrant's website constituted a purposeful disrupting the business of the Complainant. Indeed, "[t]here being no other apparent explanation for the Registrant's registration of these domain names, the Panel must conclude that the Registrant's primary purpose was to disrupt the business of the Complainant" (p. 4). The Complainant had also easily satisfied the Panel that the Registrant did not have a "legitimate interest" in the domain names. Accordingly, the disputed domain names were ordered transferred to the Complainant.

Informer Privilege and the Open Court Principle

The recent Supreme Court of Canada decision in *Named Person v. Vancouver Sun* raises issues relating to the impact of technology, in particular the internet, and the dissemination of information. It is far from a central issue in the case, but a point of note is raised.

The case concerned an extradition hearing where the named person sought to avoid extradition for reasons which required him to disclose that he was a confidential police informant. This brought into play informer privilege, which is near absolute. On the other hand the open court principle suggests that the public (or more commonly the media) should have access to all court proceedings and be entitled to report them. The bulk of the Court's decision consisted of outlining the independent significance of these two principles, and then laying out a procedure to be used by judges when they come into conflict.

The essence of the procedure is that a claim of informer privilege should be made in camera with only the informer and the Attorney General present.

The judge would also have the discretion to appoint an amicus curiae for this stage of the proceeding, since the informer and the Attorney General will typically be arguing the same side of the issue. At this stage the judge should determine whether the privilege applies.

Having decided there is an informer privilege to be respected, a further proceeding to determine how to proceed in a fashion which still respects the open court principle as much as possible must be held. Other parties than the informer and the Attorney General should be entitled to participate in this portion of the hearing.

It was over this point that the majority of the Supreme Court disagreed with the approach taken by the extradition judge: Justice LeBel in partial dissent, on the other hand, approved of the extradition judge's actions.

At the stage of deciding what type of access to permit and on what conditions, the extradition judge had sent notice of the hearing to "'certain known and respected lawyers for the various media outlets' identified by the amicus" (para 64). The majority held that it was an error to choose "worthy" interveners, and that a broader approach was needed. They held that a judge ought to post notice in a public forum, such as in hard copy at the courthouse and in electronic form over the internet. It might be the media who were primarily interested, but the judge should not select who was notified.

Justice LeBel disagreed on this particular aspect of the decision. First, he held that a judge could and should choose particular interveners, since there might be so many people interested in taking part that it was impractical to allow them all to attend. More interestingly (and in what appears to be the first appearance of the term "blogosphere" in a Supreme Court of Canada judgment) he held that the distinction between "media" and "ordinary citizens" was "becoming increasingly difficult to distinguish… in this age of electronic media" (para 153).

Possession of Child Pornography – Proof of Possession of Computer Images

The Ontario Superior Court of Justice has overturned an accused's acquittal on possession of child pornography charges in *R. v. Panko*. The trial decision acquitting the accused was reported in the IT.Can newsletter of June 15, 2006.

The accused had taken his laptop in to a computer shop to have it repaired because it would not turn on. Having repaired it the technician notices a large number of picture icons on the desktop and opened a few: they contained images of children involved in sexual activity. The technician reported this discovery to the store owner, who alerted the police. The accused was charged with possession of child pornography and with accessing child pornography. There were a total of 91 picture icons on the desktop, taking up almost the entire screen. At trial the accused admitted that the pictures behind the icons constituted child pornography. He also admitted that the computer belonged to him and that he was the only user of it.

In entering an acquittal the trial judge had excluded various statements made by the accused when he was arrested, both on the basis of a s. 10(b) violation and on the basis that the statements had not been shown to be voluntary. In overturning the acquittal the Ontario Superior Court held that this had been an error of law, and therefore that the statements should have been admitted. These included an admission by the accused, at the time of his arrest, that the police would find child pornography at his home on his computer.

The central basis upon which the trial judge had acquitted, however, was that the Crown had not proven knowledge and control of the images on the part of the accused, as they were required to do to prove possession. With regard to the knowledge component, the trail judge had been invited simply to infer it from the fact that there were 91 icons on the desktop, which the Crown argued should lead irresistibly to the conclusion that the accused knew their contents. The trial judge declined to do so, holding that the icons did not consist of pictures

visible on the screen, that the illegal content only became recognizable once the icon was clicked on, and that active searching of desktop items was not a presumed obligation of a person who had care and control of a computer.

The appeal court held that this analysis had to change once the statements made by the accused at the time of his arrest were taken into account. In particular, the accused had told the arresting officer that child pornography would be found in his home, on his computer. Whether this statement referred to a different computer or to the laptop, in either case it was a relevant circumstance suggesting that the accused collected child pornography.

In addition, the appeal court noted that the trial judge had ignored evidence that the accused had said to the computer technician that he was working on a project that was on his desktop on his computer and that he did not want to lose it. The appeal court noted that this was some evidence that the accused had knowledge of what was on his desktop: that is, there was evidence that this accused did actively search his desktop

Finally, the appeal court noted, the 91 icons were user created and took up virtually the entire screen, and were the vast majority of icons other than a few operating system created icons such as Internet Explorer and Recycle Bin. These facts would have permitted an inference that the accused was aware of what was behind them. Coupled with the failure to consider the other evidence, the finding that knowledge was not proven was an error of law.

The appeal court also found the trial judge's conclusion that control was not established to be in error. The trial judge had concluded that the images could have come to be on the computer either by the accused actively downloading them, by the accused unknowingly receiving or downloading them, or by another person actively downloading them. Since the latter two would constitute innocent explanations and had not been ruled out, the trial judge said, control had not been proven.

The appeal court noted that the evidence of the police expert upon which these conclusions were based was actually elicited by the trial judge in questioning during re-examination. The officer had been tentative in his answers, saying for example that a lot of testing would have to be done to determine whether the computer had been hacked and to say it had occurred that it would be opinion evidence which he could not offer. The appeal court concluded that the trial judge had misapprehended the evidence of the officer in concluding that it was possible that the pornography came from a third party source without the knowledge of the accused: rather, the officer had been asked speculative questions by the trial judge and said he could not answer them.

With regard to the possibility that a third party had downloaded the images, the appeal court noted that the accused had testified that he was the only user of the laptop. It was purely speculative to suggest someone else had used the computer. In particular the appeal court rejected the trial judge's suggestion that in the context of computers a limited physical control cannot lead to any useful inferences of criminal knowledge or control. Rather, the appeal court held, computers should not be any different from other possessions. Quoting *R. v. Missions*, another case involving possession of child pornography, the appeal court held:

> The normal inference that one intends the natural consequences of one's actions is applicable to computer usage just as it is to any other human activity, especially in light of the lack of evidence to rebut the inference.

The appeal court also noted:

> 71 In principle, there is no reason to distinguish a car from a computer. An inference may be drawn that an accused is taken to know the contents of his or her car. The same should be the case for a computer, unless there is an evidentiary basis that raises another possibility that could lead to a reasonable doubt as to knowledge and control.

As a result a new trial was ordered.

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

Privacy: Employee Terminated for Personal Internet Use – Illegal Collection of Information by Employer

In a recent report from the British Columbia Office of the Information and Privacy Commissioner (Order F07-18), Adjudicator Catherine Boies Parker dealt with a complaint by a terminated employee of the University of British Columbia (UBC) that the University's collection of information regarding his personal internet use had been contrary to sections 26 and 27 of the *Freedom of Information and Privacy Act (FIPPA)*. The employee had been terminated in part because of his allegedly excessive personal internet use, information regarding which had been collected by UBC by way of "Log File Reports" (LFRs) and the "Golden Eye Spy Software" (GESS).

The Adjudicator was satisfied that the information regarding what websites had been visited by the Complainant's computer was "recorded information … about an identifiable individual" for the purposes of section 1 of *FIPPA*, noting that both the LFRs and GESS did record information, and that UBC itself had linked the information to the Complainant for the purpose of terminating him (paras. 42-51). UBC argued that the collection of the information was authorized by section 26(c) of *FIPPA*, which allows a public body to collect information if it "relates directly to and is necessary for an operating program or activity of the public body." The Adjudicator held that while information about whether the Complainant was engaged in unauthorized internet use was directly related to UBC's management of the Complainant's employment, information that had been collected regarding the Complainant's specific activities (by way of screenshots) was not so related. This was particularly so given that some of the Complainant's internet use had been for personal banking, which was not prohibited by UBC (paras. 62-64). She also found that the collection of the information was not "necessary," given that there were less obtrusive means of addressing the problem (such as discussing it with the Complainant) that were not used, and no evidence that these would not have been effective (paras. 65-90).

The Adjudicator ruled alternatively that section 27(2) of *FIPPA* required that notice be given to the Complainant about the collection of the information, rejecting an argument by UBC that any information collected regarding employee performance is always with an eye to litigation, and thus no notice was required under section 27(1)(c) of *FIPPA* (paras. 95-102). In this case, no notice had been given, and thus section 27(2) had been breached.

The Complainant had requested that all of the information be destroyed as an appropriate remedy. However, the Arbitrator presiding over the Complainant's grievance had ordered production of the records in order to determine their admissibility in that proceeding. While finding that she possessed the authority under *FIPPA* to order destruction of the records (paras. 114-115), in order to avoid creating conflicting orders of two different tribunals she ordered that UBC was prohibited from making any use of the records other than before the labour Arbitrator (para. 128). She also issued an order under section 58(3)(e) of *FIPPA* that UBC "stop collecting information through an examination of log file reports, or the use of spyware, to track its employees' internet use, when there are available to UBC less intrusive steps to address employee internet activity" (paras. 117 & 129).

Privacy: Theft of Laptop Containing Health Records

In a recent report from Ontario's Office of the Information and Privacy Commissioner (IPC) (File No. HR07-36), Investigator Cathy Hamilton dealt with a report from the Privacy Officer of an unnamed "Mental Health Facility" that a staff member's laptop had been stolen from her vehicle. The laptop may have contained health and other personal information of some 560 individuals, consisting of active patients, inactive patients, and referred persons who had not become patients. The laptop was password-protected but was not encrypted. The management of the Facility took various remediating steps, including: disabling the laptop's remote access to the Facility's network; replacing laptops with desktop computers in the satellite offices at which the employee had been working: sending written reminders about computer security to employees; implementing mandatory strong password changes for all computers; providing mandatory "laptop clinics" for all staff using laptops; and purchasing

encryption software. IPC staff worked with the Facility to implement notification of potentially affected persons, noting that such persons were particularly vulnerable and might harm themselves or others if notified in the absence of clinical support. Accordingly, the health care providers of the persons potentially affected were engaged in the notification process. The IPC determined that no further review was necessary and the file was closed.

2ième partie

Publication sur un E-book et piratage : responsabilité de l'exploitant du site

Au cours des années 2004 et 2005, le demandeur a publié des « blogues ». En 2006, il décide de regrouper l'ensemble des « blogues » qu'il a publiés sur le site du « Channel 9 » dans un volume Internet, un E-book. En mars 2006, il obtient un certificat d'enregistrement de droits d'auteur de l'Office de la propriété intellectuelle du Canada pour sa publication intitulée « Beer'28s response posts on the Microsoft Channel 9 website forum ». Ce volume est disponible, selon monsieur Rondot, sur le site BeerCo Software au prix de 49,95 $ US plus taxes. Quelques jours plus tard, il est averti par un internaute que son volume a été piraté sur le site de BeerCo Software et qu'il est disponible sur le serveur de Upload2.net.

Les 25 et 26 mars 2006, sa publication de 31 pages est téléchargée 119 fois. Le demandeur s'adresse à Microsoft Corporation, le 25 mars 2006, afin de l'avertir des événements. Il demande que Microsoft bloque l'accès aux internautes afin qu'ils ne puissent plus télécharger « illégalement » sa publication. À partir de la mi-avril, l'accès à Upload2.net n'a plus été disponible pour obtenir la publication en question. Le demandeur réclame 7 000 $ des défenderesses, soit 116 fois 49,95 $ US, ce qui représente, au moment de la réclamation, 6 761,60 $ Can pour la publication téléchargée « illégalement » les 25 et 26 mars 2006.

Microsoft Corporation soumet que le demandeur devait tenir compte des conditions d'utilisation du site « Channel 9 ». Ces conditions, accessibles sur le site, prévoient que ceux qui affichent des documents sur le site accordent une licence permettant leur téléchargement par les tiers qui visiteront le site.

Le tribunal conclut que la balance des probabilités est à l'effet que les employés de Microsoft Corporation n'ont pas pris connaissance des courriels du demandeur en mars 2006. Ils n'ont pu en conséquence poser, s'il y avait lieu de le faire, les gestes requis pour empêcher le téléchargement de la publication du demandeur à l'égard de laquelle il affirme détenir des droits d'auteur. Près de 70 % du contenu de la publication du demandeur contient des textes déjà publiés sur le site de « Channel 9 », lesquels peuvent être accessibles par les internautes sans qu'il y ait lieu de rémunérer le demandeur. Le Tribunal statue que ce dernier n'a pas démontré de faute de la part de Microsoft Corporation ou de ses employés.

- *Rondot (Beerco Software) c. Microsoft Corporation*, 2007 QCCQ 10396, 7 septembre 2007.

Biométrie

L'édition de septembre 2007 du *Bulletin e-Veille* est consacrée à la biométrie. On y apprend que le marché de la biométrie connaît une croissance fulgurante. Selon les prévisions de l'International Biometric Group, après avoir généré 1,2 milliard $ US en 2004, il devrait permettre d'atteindre des revenus globaux de 3,01 milliards $ US en 2007, puis d'environ 7,41 milliards $ US en 2012. L'on prévoît que les administrations publiques et les entreprises privées seront de plus en plus friandes de ces technologies. Dans une revue des avancés récents, on peut lire qu'il y a des développements majeurs au niveau des technologies biométriques imbriquées : s'identifier en présentant son iris, son doigt ou son visage à son cellulaire fait maintenant partie des utilisations émergentes de la biométrie. On signale des progrès dans la reconnaissance faciale, la reconnaissance des circuits vasculaires, la reconnaissance vocale et celle de l'iris. Il est même question de reconnaissance des signaux électrophysiologiques, c 'est-à-dire les circuits électriques du fonctionnement du corps : nos organes émettent des signaux que peuvent capter certains appareils.

Un article fait état des développements européens. On y indique que le développement des technologiques biométriques a pour objectif de centraliser plusieurs mécanismes d'identification dans un outil unique. Enfin, les avantages liés à l'introduction de la biométrie se recoupent d'un projet à l'autre. Principalement, les outils technologiques biométriques ont pour objectif de rechercher un équilibre entre la sécurité et le respect de la vie privée tout en réduisant les transactions économiques frauduleuses, l'utilisation de fausses

identités et les menaces terroristes. Ces avantages que procure le recours à la biométrie valent autant pour les citoyens que pour les administrations publiques et les entreprises. Bref, la biométrie n'est pas une panacée ni une fin en soi, mais elle s'avère un moyen efficace pour atteindre les objectifs de sécurité que se sont donnés les États européens.

Les Administrations européennes ne sont pas les seules à adhérer à la biométrie. En Amérique du Nord comme en Asie, l'attestation de l'identité des individus à l'aide de mesures biométriques est utilisée à diverses fins. Que ce soit pour contrôler l'accès à des lieux ou à des documents, ou encore pour sécuriser une carte d'identité nationale, une carte d'accès à des services publics, un passeport ou des documents de voyage, divers pays font un usage novateur de cette technologie.

Enfin, l'on passe en revue les applications actuelles de la biométrie pour le contrôle aux frontières et perceptions des citoyens au nord de l'Amérique.

Commentez cet article au Blogue de IT.CAN

- *Bulletin e-Veille*, septembre 2007.

La confiance et le commerce électronique

L'encadrement des activités effectuées via les environnements électroniques doit désormais s'envisager non plus au regard du seul droit positif mais aussi de l'ensemble des mécanismes développés par les acteurs pour faire face à la lenteur et à la complexité des rouages parlementaires. Une kyrielle d'instruments s'est développée pour accompagner l'implantation du paiement en ligne, des prestations électroniques de service, de l'informatisation du secteur de la santé et des services sociaux, des modes alternatifs de règlement des conflits, du vote électronique, du transfert de renseignements personnels aussi bien à des fins commerciales que de sécurité des frontières. Parmi ces instruments, on fait référence aux codes de conduite, à la certification, aux labels de qualité, aux guides ou modèles de pratique, aux politiques de confidentialité, à la régulation par l'architecture, aux best practices et autres contrats. Ces mécanismes ont pour objectif, en plus de prescrire les droits et obligations de chacun, d'établir un lien de confiance entre l'administration et le citoyen, entre le commerçant électronique et l'internaute, entre deux entités juridiques.

Dans un environnement où les acteurs ne sont pas en présence l'un de l'autre, la confiance joue ainsi un rôle important. L'auteure dresse un portrait de la notion de confiance (ses fondements, ses caractéristiques et ses diverses matérialisations) afin de démontrer qu'elle est un instrument de régulation des environnements électroniques.

- Cynthia CHASSIGNEUX, « La confiance, instrument de régulation des environnements électroniques », (2007) 37 *R.D.U.S* 441.

Droit de la consommation appliqué au commerce électronique

Dans le but de renforcer la confiance et assurer le développement du commerce électronique dans le respect des droits de tous, le Forum des droits sur l'Internet a publié une Recommandation sur l'application du droit de la consommation au commerce électronique. Cette Recommandation témoigne d'un consensus des acteurs autour d'une plate-forme commune de plus de 100 propositions. Quatre idées principales inspirent cette plate-forme : harmoniser les différents canaux de distribution, donner aux acteurs français des armes face à la concurrence internationale, améliorer l'information du consommateur et moraliser certaines pratiques liées à la commande. Ces propositions tendent à assurer une adaptation du droit de la vente à distance aux spécificités d'Internet et incluent des « bonnes pratiques » qui fournissent aux consommateurs et aux professionnels des illustrations des best practices.

Commentez cet article au Blogue de IT.CAN

- *Recommandation du Forum des droits sur l'internet « Droit de la consommation appliqué au commerce électronique »*, 26 septembre 2007.

Regard critique sur l'orientation de la jurisprudence française relative au web 2.0

Dans cet article, l'auteur relève que plusieurs décisions rendues par des juridictions parisiennes remettent clairement en cause la possibilité de faire bénéficier les fournisseurs de services associés au web 2.0 du régime de responsabilité aménagé des hébergeurs prévu par la loi sur la confiance dans l'économie numérique. Il est à craindre que l'orientation actuelle de la jurisprudence en vienne à mettre en péril l'équilibre mis en place par la législation française en stigmatisant le rôle des intermédiaires, notamment, en leur faisant porter une responsabilité du fait des contenus mis en ligne à l'initiative des usagers de leurs services.

Ainsi, l'auteur critique l'appréciation exagérément restrictive du champ d'application du régime de responsabilité des prestataires d'hébergement. La Cour d'appel de Paris, pour paralyser l'application du régime des prestataires d'hébergement, a considéré que l'intervention des sociétés Tiscali et MySpace ne saurait se limiter à la simple fonction technique d'hébergement, mais que ces sociétés devaient aussi être envisagées comme ayant la qualité d'éditeur. L'auteur fait remarquer que dans l'environnement des services web 2.0., il est fréquent que, sur une même page-écran, se côtoient des informations éditées ou crées par le prestataire du service et d'autres qui sont fournies par les utilisateurs. Certains sites ont une nature composite et il serait arbitraire de vouloir les réduire à une qualification unique.

Commentez cet article au Blogue de IT.CAN

- Sébastien PROUST, « Propos critiques à l'encontre de l'orientation actuelle de la jurisprudence face au développement du web 2.0 », *Revue Lamy Droit de l'immatériel,* août/septembre 2007, pp. 29-34.

À signaler

- Julien LE CLAINCHE, « Liste noire de notaires : dernier acte ? », *Revue Lamy Droit de l'immatériel*, août/septembre 2007, pp. 35-39.
- Claudine GUERRIER, « La vidéosurveillance est-elle conciliable avec la liberté de circulation? », 21 septembre 2007, *Juriscom.net*.
- Xavier JORELLE, « Quelle responsabilité pour les plateformes de commerce électronique 2.0? », 19 septembre 2007, *Juriscom.net*.