

IT.CAN NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors [Teresa Scassa](#), [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 [Teresa Scassa](#), [Chidi Oguamanam](#) et Stephen Coughlan de l'Institut de droit et de technologie de la [Faculté de droit de l'Université de Dalhousie](#). Les professeurs [Pierre Trudel](#) et [France Abran](#) de la 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 Names

In *House of the Blues Brands Corp. v. Artbravo Inc.*, a three member panel considered a dispute over the domain name [houseofblues.ca](#). The complainant owned Canadian registered trademarks for HOUSE OF BLUES, and HOUSE OF BLUES and design. The trademark registrations predated the registration of the domain name in October of 2005. In a rather opaque decision, Panel Chair Rodney Kyle determined that the complainant had rights in these marks, and that the registrant's domain name was confusingly similar.

On the issue of legitimate interest, the complainant had argued that the domain name had been used by the registrant as part of a revenue-generating business involving redirection from the domain name to a third party web site which featured music in exchange for referral fees. After initial contact by the complainant, the registrant's site was changed to resolve to a picture of a painting epitomizing Picasso's blue period. The complainant also alleged that the registrant had no common law or other trademark rights in the name, and that "house of blues" had no generic meaning in Canada.

Kyle determined that since the registrant did not specifically dispute the contention that "house of blues" had no generic meaning and was not used by

the registrant to carry out a non-commercial business or as a place name, these allegations were therefore admitted by the registrant. The panel found that the evidence supported the conclusion that the domain name was used in a revenue-generating business involving redirection to a third party site. The panel also concluded that the domain name was registered in bad faith. The panel accepted that the registrant registered the domain name for the purpose of preventing the complainant from registering it, and that he had engaged in a pattern of similar conduct.

A majority of the panel concluded that the domain name should be transferred to the complainant both because the panel had unanimously found in favour of the complainant and because the complainant satisfied the Canadian presence requirements (CPRs) under the CIRA policy by having four Canadian registered trademarks. However, one panelist held a different view: he held that the domain name should be transferred to the complainant's nominee because the complainant named a nominee, and that nominee satisfied the Canadian presence requirements.

Article 4.3 of the CDRP provides:

4.3 If the Panel decides in favour of the Complainant, the Panel will decide whether the Registration should be cancelled or transferred to the Complainant or in the case where the Complainant does not satisfy the CPR in respect of the domain name that is subject of the Proceeding, a nominee of the Complainant that satisfied the CPR in respect of the domain name that is the subject of the Proceeding (the "Nominee").

The difference of opinion on the panel arose because it is possible to be eligible to bring a complaint under the CDRP without satisfying the CPRs for registration of a domain name. For example, a foreign based company that has a registered trademark in Canada would only be entitled under the CPRs to register a .ca domain name "consisting of or including the exact word component of that registered trade-mark" (art. 2(q) CPR). However,

under the CDRP an eligible complainant is one who satisfies the CPRs “in respect of the domain name that is the subject of the Proceedings”, or who is the owner of a Canadian trademark, and the complaint is in relation to that mark.

The panel was obviously concerned with a situation where a domain name might be transferred to a complainant who had a valid complaint in relation to a Canadian registered trademark, but who would not have been eligible to register that mark in the .ca domain had they applied directly. This situation did not appear to arise on the specific facts of this case, as the Complainant’s mark was HOUSE OF BLUES, and the disputed domain name was houseofblues.ca. However, since the complainant had appointed a nominee in the case, the minority panelist would have ordered the transfer of the domain name to the nominee, and not to the complainant. The majority was of the view that the limitation on registrations contained in CPR 2(q) “does not otherwise qualify the right of a trade-mark owner to both bring a complaint and own a .ca domain name in the trade-mark owner’s own right.” (at p. 24) The panel was unanimous in indicating that “the scope and interaction of instruments that become part of dispute resolution agreements (such as the Policy, the Resolution Rules, and the CPR) could perhaps usefully be clarified by CIRA”. (at p. 28)

[Comment on the issues raised in this item at the IT.Can blog](#) 

Privacy

TREASURY BOARD HAS JUST RELEASED A *FEDERAL Strategy to Address Concerns about the USA Patriot Act*. The document sets out a federal strategy designed around three basic considerations. First, the federal government shares responsibility for personal information protection with provincial governments and the private sector. Second, privacy issues will have to be weighed against other important considerations, including Canada’s international trade obligations, public safety and national security. Finally, the strategy should be built on existing measures such as the *Privacy Act* and *PIPEDA*. In implementing its strategy, the government has raised awareness across all of its institutions of privacy issues raised by the *USA Patriot Act*.

These institutions were responsible for reviewing their contracting and outsourcing arrangement to minimize the impact of the *Patriot Act*. The Federal Strategy identifies a series of follow up measures scheduled to take place over the coming year, as well as longer term measures scheduled to occur within one to two years. Treasury Board also released a document entitled *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*. This document “is intended to provide advice to federal government institutions whenever they consider contracting out activities in which personal information about Canadians is handled or accessed by private sector agencies under contract.”

The Privacy Commissioner of Canada has [endorsed](#) the Canadian Government’s strategy. Commissioner Stoddart described the document as a “comprehensive strategy” and a “positive step toward addressing Canadians’ concerns about the flow of their personal information across borders.” She also identified the Guidance Document as a “key document.”

[Comment on the issues raised in this item at the IT.Can blog](#) 

THE ALBERTA INFORMATION AND PRIVACY COMMISSIONER has released a report on an investigation under the province’s *Personal Information Protection Act*. The investigation involved a [complaint against CIR Realtors and PDL Mobility Limited](#). The complainant was a realtor with CIR. He arranged for an ad to be placed in a newspaper. The ad listed his first name alongside the CIR office telephone number. He did not receive any calls in relation to the ad. When he contacted the CIR office, the receptionist (who was a call centre employee) indicated that she had no record of him being a realtor with CIR. In spite of repeated phone calls to the call centre, the omission was not rectified. His employment with CIR was subsequently terminated. At the time of his termination, CIR’s manager played back to him the taped recordings of his conversations with the call centre operators. The complainant had not been aware that the conversations were being taped. The recording of his conversations without his knowledge or consent formed the basis for his complaint to the Alberta Privacy Commissioner.

The Investigator appointed to the file determined that the call centre, PDL, used Voice Logger software to record all calls, and that the calls were used to assist PDL agents to verify information provided by clients, and for PDL to monitor and assess the performance of its staff. CIR provided a script to PDL agents for use on their calls; the script did not contain a notification to clients that calls were being recorded.

The Investigator concluded that because there was a contract between CIR and PDL whereby PDL provided reception services to CIR, CIR was responsible to ensure that PDL complied with *PIPA*. The investigator found that the recorded conversations were “personal information” under the *Act*. As the complainant was an employee of CIR at the time of the calls, an issue also arose as to whether this information was also personal information about an employee, which is a subset of information protected under the *Act*. “employee personal information” can be collected without the consent of the employee in specified circumstances. She further concluded that “As CIR had no business purpose for collecting the information... [it] does not qualify as personal employee information under *PIPA*...” (at para 40). The investigator found that the collection of the complainant’s personal information without consent violated sections 7(1)(a) and (c) and s. 13(1) of *PIPA*. These provisions related to the collection of personal information without consent, and without informing the individual about the purposes for collection. Further, the investigator found that s. 11 of *PIPA* was also violated in that the information was not collected for purposes that were reasonable. There was no intended business purpose for the collection of the information.

The investigator also found that PDL violated the *Act* because it collected personal information through voice recordings for its own business purposes. When it did so without obtaining consent from the complainant or notifying the complainant of the purposes of the collection it violated sections 7(1) and 13(1) of the *Act*.

THE OFFICE OF THE PRIVACY COMMISSIONER OF BRITISH Columbia has released a *Report on the Sale of Tapes of Personal Information*. The report examines and makes recommendations in relation to the ways in which government destroys media containing personal information. Privacy Commissioner Loukidelis found that the mechanisms in place in B.C. were inadequate and, in any event, not followed.

[Comment on the issues raised in this item at the IT.Can blog](#)



[Comment on the issues raised in this item at the IT.Can blog](#)



2^{ème} partie

Frais d'intérêt chargés lors de paiement par Internet – autorisation de recours collectif

La requête en autorisation de recours collectif vise à récupérer les frais d'intérêt qui ont été chargés par la banque. Un représentant de la banque a recommandé à la requérante de payer son compte par Internet de 3 à 5 jours avant la date d'échéance. Cela pose la question de savoir si le délai de 21 jours prévu par la *Loi sur la protection du consommateur* et mentionné au contrat est respecté. Le tribunal estime que la source de la réclamation de chacun des membres du groupe est le mode d'opération similaire de la part de la banque impliquant les mêmes frais d'intérêt. Les conditions pour que le recours collectif soit autorisé sont satisfaites.

Aberback-Patck c. Amex Bank of Canada, 2006 QCCS 1425 (IJCAN), 21 mars 2006.

Demande de remboursement de sommes perçues lors de la vente de certains iPods – autorisation de recours collectif

La requête vise le remboursement des frais qui avaient été inclus dans le prix de vente de certains appareils iPods découlant d'un tarif de redevances au titre de la copie privée sur des supports audio vierges. Les frais initialement autorisés par la Commission du droit d'auteur ont été contestés avec succès devant la Cour d'appel fédérale. Le recours collectif vise le remboursement de ces sommes. Apple invoque qu'elle a mis en place un programme de remboursement de ces sommes. Mais le tribunal autorise le recours, convenant que le juge qui décidera au mérite pourra évaluer le caractère adéquat du programme de remboursement.

St-Germain c. Apple Canada inc., 2006 QCCS 1282 (IJCAN), 23 février 2006.

Inscription à un tirage par Internet

Le 15 juin 2004, le demandeur a reçu de la SEPAQ une confirmation en bonne et due forme que son inscription au tirage au sort de la chasse au cerf, effectuée par Internet, est gagnante. Le lendemain, il reçoit un courriel l'informant de ne pas tenir compte de ces résultats. La preuve révèle que ces résultats proviennent d'un test de pré-tirage antérieur dont la base de données n'a pas été complètement détruite. Son inscription se révèle finalement non gagnante et il demande que l'on reconnaisse son inscription comme gagnante.

Le tribunal conclut qu'il y a eu faute de la SEPAQ. Quant au dommage, il ne saurait être question de donner au demandeur un gain dont il a pu être privé puisque suivant la preuve, son inscription a été considérée dans le tirage officiel et qu'il n'a pas été privé de quelque chance que ce soit à l'effet que son inscription puisse être gagnante. Le dommage ne s'élève pas à l'équivalent d'une inscription gagnante mais à la déception et à la frustration devant ce revirement de situation.

Tailfer c. Société des établissements de plein air du Québec, 2006 QCCQ 2391 (IICan), 21 mars 2006.

Contrat pour hébergement d'un site web

Le demandeur réclame des dommages reliés au non-respect d'un contrat verbal intervenu avec Oricom pour l'hébergement d'un site web, et plus précisément, de n'avoir pas procédé au renouvellement annuel du nom de domaine Nordikhockey.com. Le tribunal conclut qu'il n'y a pas de preuve prépondérante qu'Oricom avait la responsabilité de procéder au renouvellement du nom de domaine.

Hardy (Nordik Hockey enr.) c. Oricom Internet Inc., 2006 QCCQ 1075 (IJCAN), 28 février 2006.

La biométrie

Au Québec, l'article 44 de la *Loi concernant le cadre juridique des technologies de l'information* balise le recours à des mesures biométriques comme moyen d'identification. Les traits de la personne

peuvent être utilisés dans le cadre du processus d'identification fondé sur la physiologie naturelle d'une personne. On parle alors d'identification biométrique. La biométrie s'appuie sur la prise en compte d'éléments morphologiques uniques et propres des individus, tels que les caractères physiologiques ou les traits comportementaux automatiquement reconnaissables et vérifiables.

Deux catégories de technologies permettent de saisir des caractéristiques ou des mesures biométriques. Il y a d'abord les techniques d'analyse du comportement : la dynamique de la signature (la vitesse de déplacement du stylo, les accélérations, la pression exercée, l'inclinaison...) et la façon d'utiliser un clavier d'ordinateur (la pression exercée, la vitesse de frappe...). Il y a aussi les techniques d'analyse de la morphologie humaine : les empreintes digitales, la forme de la main, les traits du visage, le dessin du réseau veineux de l'œil (l'iris et la rétine), la voix. Par exemple, des dispositifs peuvent effectuer l'appariement entre une carte comportant une empreinte digitale et l'empreinte qui est présentée par le possesseur de la carte.

Le législateur québécois limite le recours à l'identification par la biométrie en imposant des balises. Le consentement de la personne est nécessaire pour vérifier ou confirmer son identité au moyen de mesures biométriques. On ne précise pas la forme que doit prendre ce consentement, mais son importance appelle de consigner ce consentement dans un document explicite.

La prise de mesures ou de caractéristiques doit être minimale. On limite ici la quantité d'informations biométriques recueillies. L'identité ne peut être établie qu'en faisant appel au minimum de caractéristiques ou de mesures requises pour relier un individu à l'action qu'il pose.

Le procédé utilisé doit permettre à la personne de savoir que des mesures portant sur ses caractéristiques biométriques sont prises. Par conséquent, on ne peut capter de telles caractéristiques à l'insu de la personne.

Tout autre renseignement concernant la personne et obtenu suite à la saisie des mesures ne peut être utilisé à aucune autre fin que l'identification de cette personne. Cette interdiction a pour but de protéger la personne contre l'utilisation de renseignements

secondaires qui pourraient émaner de la saisie de mesures biométriques. Par exemple, la cueillette d'une image de la rétine d'un individu dans le cadre d'un système de sécurité pourrait en certains cas déceler une maladie de l'œil. Cette information secondaire, en vertu du deuxième alinéa de l'article 44, ne pourrait être utilisée par l'employeur pour justifier une décision à son égard. De plus, cette information ne pourrait être dévoilée qu'au principal intéressé, et à sa demande s'il a connaissance qu'elle a été recueillie.

Les informations sur les caractéristiques biométriques doivent être détruites lorsque l'objet fondant la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus. On confirme ici la règle du respect de la finalité pour laquelle les informations ont été recueillies ou conservées. Cet alinéa vise à empêcher que des dossiers biométriques soient conservés sans motif valable.

La Loi attribue d'importants pouvoirs à la Commission d'accès à l'information pour réguler le recours à la biométrie. Ainsi, l'existence d'une banque de caractéristiques ou de mesures biométriques doit lui être préalablement divulguée. La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne. Elle peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction.

En droit français, voir :

Pierre LECLERCQ, « À propos de la biométrie, » *Communication-commerce électronique*, mars 2006, p. 14 à 18.

Sur la biométrie : autour d'une exposition intitulée « [Biométrie, le corps identité](#) » à la Cité des sciences.

Confection de listes d'adresses de courriel par « aspiration » d'adresses sur le web – France

Dans un arrêt du 14 mars 2006, la Cour de cassation a confirmé une décision de la Cour d'appel de Paris condamnant le responsable d'une entreprise ayant

recueilli, à l'insu des personnes concernées, des adresses de courriel en faisant usage de logiciels permettant « d'aspirer » sur Internet des adresses de courriel de personnes physiques. Sans stocker ces adresses, elle a transmis des messages non sollicités à ces adresses. La Cour estime que ce genre de procédé constitue une utilisation d'informations nominatives, même sans stockage mais utilisées sans rapport avec l'objet de leur mise en ligne, et est une violation des dispositions de la Loi informatique et libertés.

Fabrice X c. Ministère public, Cour de cassation, ch. criminelle, 14 mars 2006, sur Juriscom.net.

Responsabilité de l'employeur pour les activités personnelles de ses salariés sur Internet – France

Depuis son lieu de travail, un salarié a créé un site dénigrant une société commerciale. Celle-ci a poursuivi l'employeur. L'employé a admis avoir créé le site dénigrant. La responsabilité de l'employeur est retenue car il avait permis aux salariés par une note de service d'utiliser les équipements informatiques

mis à leur disposition pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité. L'entreprise oeuvre dans le domaine de la construction d'équipements et de systèmes de télécommunications et les tâches du salarié implique un usage quotidien d'un ordinateur. De cela, la Cour d'appel d'Aix-en-Provence déduit qu'en l'espèce, l'employé agissait dans le cadre de ses fonctions et avec l'autorisation de son employeur.

SA Lucent Technologies c. SA Escota, SA Lycos, Monsieur Nicolas B., CA Aix-en-Provence, 2e ch. 13 mars 2006, Juriscom.net.

Valérie SÉDALLIAN, *La responsabilité de l'employeur du fait des activités personnelles de ses salariés sur internet*, Juriscom.net, 31 mars 2006.

À signaler

Cédric MANARA, *Du commerce amoureux au commerce électronique*, Juriscom.net. Cet article examine la responsabilité des sites commerciaux proposant des rencontres.

This newsletter is intended to keep members of IT.Can informed about Canadian legal developments as well as about international developments that may have an impact on Canada. It will also be a vehicle for the Executive and Board of Directors of the Association to keep you informed of Association news such as upcoming conferences.

If you have comments or suggestions about this newsletter, please contact Professors Teresa Scassa, Chidi Oguamanam and Stephen Coughlan at it.law@dal.ca 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.

Copyright 2006 by Teresa Scassa, Chidi Oguamanam, Stephen Coughlan, Pierre Trudel and France Abran. Members of IT.Can may circulate this newsletter within their organizations. All other copying, reposting or republishing of this newsletter, in whole or in part, electronically or in print, is prohibited without express written permission.

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 Teresa Scassa, 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.

© Teresa Scassa, Chidi Oguamanam, Stephen Coughlan, Pierre Trudel et France Abran 2006. Les membres d'IT.Can ont l'autorisation de distribuer ce bulletin au sein de leur organisation. Il est autrement interdit de le copier ou de l'afficher ou de le publier de nouveau, en tout ou en partie, en format électronique ou papier, sans en avoir obtenu par écrit l'autorisation expresse.