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

October 16, 2008/16 octobre 2008

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

Conflicting Authorities over Approved Screening Devices

The issue of whether the Crown is required to prove that a screening device is an approved one as part of establishing compliance with the statutory requirements for making a breathalyzer demand was before the Ontario Superior Court of Justice in *R. v. Leggett*. The accused was charged with having charge of a motor vehicle with an alcohol concentration in his blood of over .08. At trial, the officer who had made the breathalyzer demand testified that he had requested a sample of breath from the accused into an approved screening device. The accused failed the approved screening device test, which formed the reasonable grounds for the officer to make a breathalyzer demand. In his direct testimony, the officer described the screening device as a Drager Alcotest 7410 and gave its serial number. In cross-examination the officer confirmed the serial number he had given, which differed by one letter from his notes, and acknowledged that the word "Drager" did not appear in his notes. He was not otherwise challenged on his description of the device as an approved screening device, though defence counsel did ask the trial judge to note the issue. After the Crown closed its case, the accused argued that the Crown had not proven that the initial demand for a breath sample was made using an approved screening device. In particular, although the officer had described it as an approved device, he had identified it as a Drager Alcotest 7410, which does not appear in the regulations in the list of approved devices. The regulations did include an Alcotest 7410 GLC, but the accused argued that the officer's different identification of the device he used contradicted the claim that an approved device was used. In that event, the accused argued, there was no proof that an approved device was used and therefore the statutory requirements for having reasonable grounds to make the breathalyzer demand were not met. In that event, the accused argued, the objective component of the section 254(3) demand was not met and the breathalyzer evidence was not admissible. The trial judge accepted the accused's argument and acquitted the accused.

The Crown appealed and Gautier J. granted the appeal. Properly, he held, the accused should have raised the issue as a *Charter* motion, arguing that there was a violation of section 8 of the *Charter*. The accused did not do this, nor even raise centrally with the officer the question of whether the screening device used was an approved one. Further, if a *Charter* violation had been shown, the trial judge would have been required to consider section 24(2) in order to decide whether the evidence should have been excluded. On that basis, Gautier held that he would have granted the Crown appeal if the matter were considered on *Charter* grounds.

In fact, though, the central issue in dispute in the case was whether the breathalyzer evidence was inadmissible simply on the basis that the statutory preconditions for using it had not been complied with. Specifically, the case had been argued at trial on the basis that the Crown had failed to prove that the screening device was an approved screening device, and therefore had failed to prove that there were reasonable grounds for the officer's belief under s. 254(3). In that event, it had been argued, the officer had no authority to make the breathalyser demand, and so the Crown could not rely on the presumption of identity in section 258(1)(c). On appeal, Gautier

rejected the view that this was a correct analysis, holding instead that the issue needed to be framed as a *Charter* claim.

The confusion arose because a pre-*Charter* Supreme Court of Canada case, *R. v. Rilling*, had held that the absence of reasonable and probable grounds did not render certificate evidence inadmissible: that is, it had rejected the position put forward by the accused at trial here. However, the much more recent decision in *R. v. Woods* had stated:

> Accordingly, the only issue in this case is whether the *ASD breath sample was legally obtained*. If it was, the breathalyser evidence was properly admitted and the respondent's conviction was sound. If not, the conviction cannot stand (emphasis in original). (para 8)

Some courts had taken this passage to overrule *Rilling*. Gautier J. considered the conflicting authorities, noting that the New Brunswick Court of Appeal had taken *Rilling* to no longer be good law in R. v. Searle. However, he held that he accepted the arguments to the contrary in other cases, and in particular in the very brief Ontario Court of Appeal decision in *R. v. Anderson*, which affirmed that *Rilling* was still correct on the non-*Charter* argument.

Gautier J. noted that the real issue was whether the officer had reasonable grounds for making the breathalyzer demand. He had testified that he did, and that he had used an approved screening device. Although he had been asked to identify the type of approved screening device, there was no requirement on the Crown to prove this fact, and "it was probably unwise to do so" (para 66). Nothing in cross-examination or the evidence of the accused challenged that the officer had used an approved screening device, and so the reasonable belief of the officer was sufficiently established.

Criminal Law: DNA Order & Informational Privacy

The Ontario Superior Court of Justice has released it decision in *R v. Gasparetto*. In that case, after pleading guilty, the accused was convicted for fraud. She admitted to obtaining monies in excess of $5,000 by deceit, falsehood and other fraudulent means. Essentially, she had represented her intention to set up an exclusive women's fitness outfit and solicited the support of the first complainant, her former business associate, and potential investor in the new venture. She purported to prepare and defend a business proposal in respect of the outfit before her father, a wealthy businessman and a potential financier. On the basis of her representation, the first complainant not only advanced monies to her, she also introduced the accused to a third party, the second complainant, from whom the accused obtained significant amounts of money. The accused father denied involvement in her schemes. According to the court, there was no doubt that her purported investment opportunity or business proposal "was completely without substance or merit" (para 7). The accused admitted to, among others, having gambling addiction and that she suffered from psychiatric conditions. Her counsel requested, with her consent, that the accused be ordered to attend psychiatric assessment. Following the result of the psychiatric assessment, at the sentencing hearing, the Crown asked for the accused to be sentenced to "six months in custody and three years probation … as well as a freestanding restitution order in favour of both complainants for the full amount of the fraud and a DNA order" (para 19).

In rejecting the Crown's request for a DNA order, the court held that "[f]raud is a secondary designated offence and, [that] pursuant to s. 487.051(3)(b) of the *Criminal Code*" the order could be made if the Crown convinced the court that it would be in the best interest of administration of justice to so do. The accused does not satisfy the various factors which the Code requires the court to examine before making a DNA order. She "has no criminal record and, considering the nature of the offence and the manner in which it was committed, I would not expect her DNA to assist in solving other unsolved crimes or any future crimes she might commit" (para 50). There is no evidence that a DNA test would have negative impact on the accused's privacy and security. However, this is not a case in which the defence is seeking an exception to an otherwise mandatory order. As much as the current non-evasive procedure for obtaining DNA and implementing a DNA order has limited effect on privacy of the subject, nonetheless, "informational privacy is seriously engaged because DNA contains the highest level of private and personal information" (para 50).

Employment Contract and Confidential Information

The Supreme Court of Canada has delivered its decision in *RBC Securities Inc. v. Merrill Lynch Canada Inc.* In this case, the Cranbrook (BC) branch manager of RBC helped to coordinate a mass movement of virtually all the investment advisors under him from that branch to RBC's rival, Merrill Lynch without notice, resulting in the collapse of the branch. RBC sued both the manager and the departed advisors claiming compensatory, punitive and exemplary damages. At the trial level, the BC Supreme Court found that the advisors breached implied terms of their employment which required reasonable notice of termination be given to their employer. Also, the Court found that the manager breached his contractual duty to retain the advisors when he coordinated their departure without notice to the RBC management. The court assessed damages against the manager and the departed advisors. It also held Merrill Lynch Canada Inc. liable for inducing the mass movement of RBC staff. The Appeal Court varied some of the damages awarded by the trial judge. The Supreme Court was asked to consider whether the Court of Appeal properly overturned the award of damages against the former RBC employees and Merrill Lynch and its manager for losses caused over a five-year period and whether it applied the proximity test correctly in setting aside the award against the manger on the finding of breach of contractual duty of good faith.

The Supreme Court held that the majority of the Court of Appeal applied the proximity test wrongly. Instead of asking whether the damages of the sort sustained by RBC have been within the reasonable contemplation of the parties had they adverted their mind to the potential breach that has occurred when the contract was entered into, the majority of the Appeal Court was only concerned with whether the breach was foreseeable. Thus, the Appeal Court was wrong in concluding that the collapse of the Cranbrook branch of RBC was not a foreseeable consequence of the manager's action. In the opinion of the Supreme Court, the Court of Appeal's argument "conflates the unforeseeability of the consequence with the unforeseeability of breach" (para 12). In regard to unfair competition, the Supreme Court sided with Court of Appeal and held that as soon as the investment advisors left RBC, they were no long under any obligation not to compete with it. It also endorsed the observation of the Appeal Court that even then such departing employees "might be liable to specific wrongs such as improper use of confidential information during the notice period" (para 18). According to the Supreme Court, the current law is that in post-employment situations, employees have a duty not to misuse confidential information, including not breaching fiduciary and other duties that may arise from restrictive covenant. In allowing the appeal in part and reinstating the order of the trial judge, the Supreme Court set aside the awards made against the advisor for unfair competition arising out of the 2.5 week period that they failed to give notice. The Court held: "The contract of employment ends when either the employer or employee terminates the employment relationship, although residual duties may remain. An employee terminating his or her employment may be liable for failure to give reasonable notice and for breach of specific residual duties. Subject to these duties, the employee is free to compete against the former employer" (para 19),

Privacy in Email Services Outsourced to the United States

The Privacy Commissioner has concluded that Canada.com had met its obligations under PIPEDA when it outsourced its email services to a provider in the United States. Although this meant that some information was potentially be disclosed as a result of the *PATRIOT Act*, Canada.com had complied with its legal obligations.

CanWest Publishing Inc. (Canwest) operates canada.com, an interactive Web portal which provides email services. Those email services have been provided by third parties since 1998. In 2006 those services were out-sourced to a company in the United States. As noted in the decision, Principle 4.1.3 of the *Act* states that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing, and that the organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. In addition Principle

4.3 provides that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate and Principle 4.3.2 states that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information shall be used. Two complainants objected that these obligations were not complied with when the email services were outsourced.

The Commission noted that that all new and existing customers were informed of the outsourcing by means of a pop-up when they attempted to log in to their accounts. Information provided at that time informed customers of the fact that some information was stored in the United States and therefore could potentially be accessed. Although some information had been transferred to the United States in anticipation of each customers log in, that information could not personally identify particular subscribers unless a customer consented at the time of login. If a customer did not consent, then the account was closed and the data which had been transferred was destroyed.

In this event the Commissioner held that Canwest had acted within the *Act*. Canwest could not use contractual arrangements to override the effect of US law. It had reliably informed customers of the change and given them an opportunity to consent, and so had complied with its obligations.

2ième partie

Signification du mot « presse » à l'article 68 C.p.c.

Cette décision est rendue dans le cadre d'une requête en exception déclinatoire à l'encontre d'un recours en injonction et en dommages-intérêts pour diffamation. Le message reproché était contenu dans un envoi sur un site Web ouvert au public. C'est d'ailleurs le reproche fait par le demandeur d'avoir diffusé à large échelle ces propos diffamatoires. Le débat est fort intéressant à savoir si le district judiciaire qui a juridiction pour entendre la cause est celui de l'endroit d'où origine le message diffamatoire ou si c'est tout district judiciaire où peut être diffusé ce message allégué diffamatoire. Le débat porte principalement sur la portée de l'article 68(2) du *Code de procédure civile* qui dispose que:

> 68. Sous réserve des dispositions du présent chapitre et des dispositions du livre X au Code civil, et nonobstant convention contraire, l'action purement personnelle peut être portée:
>
> (...)
>
> 2. Devant le tribunal du lieu où toute la cause d'action a pris naissance; ou, dans le cas d'une action fondée sur un libelle de presse, devant le tribunal du district où réside le demandeur, lorsque l'écrit y a circulé;

La version anglaise emploie le mot «newspaper» pour le mot «presse» et «écrit». La question qui est soumise au Tribunal est à savoir si le message diffamatoire provenant du défendeur et transmis par l'entremise d'un forum public sur le site Web de l'APBQ est ou non un libelle de presse qui a circulé dans le district où réside le demandeur. Pour décider de l'exception déclinatoire soumise, le Tribunal interprète les termes de l'article 68(2) C.p.c. à savoir si ce qui est visé par «libelle de presse», en anglais «newspaper», ayant circulé dans le district où réside le demandeur, peut être compris, par analogie, à une diffusion d'un message diffamatoire écrit sur un site Web, par Internet.

Le contexte dans lequel doit être interprété l'ensemble de l'article 68 C.p.c., l'esprit et l'objet de la loi sont à l'effet que l'action purement personnelle doit être intentée en priorité devant le tribunal du domicile réel du défendeur. L'article 68 C.p.c. n'emploie pas le terme «doit» mais le terme «peut» vu qu'il y a d'autres possibilités où l'action purement personnelle peut être intentée, mais ces possibilités doivent être considérées comme des exceptions à la règle générale. Comme toute exception, ces possibilités doivent recevoir une interprétation restrictive. Le Tribunal estime que le paragraphe 2 de l'article 68 C.p.c. ayant trait au « libelle de presse » ne doit pas être pris isolément mais dans le contexte global de l'article 68 C.p.c. Il devient donc contraire à l'esprit dans lequel le législateur a édicté cet article, d'étendre à d'autres modes de diffusion, comme Internet, le «libelle de presse» pour établir le district où l'action purement personnelle doit être intentée.

- *Vincent c. Forget*, Cour supérieure, 2008 QCCS 2466 (Canlii), 20 mai 2008.
- Cette décision fut portée en appel et dans un arrêt du 10 octobre 2008, la Cour d'appel a rejeté l'appel : *Vincent c. Forget*, 2008 QCCA 1892, Cour d'appel, 10 octobre 2008.

Sentence pour le crime de leurre sur Internet

L'accusé a plaidé coupable à deux chefs d'accusation lui reprochant le crime de leurre d'une personne de moins de 18 ans. Le Tribunal considère qu'une peine d'incarcération s'impose sur le chef de leurre. Une peine d'emprisonnement avec sursis ne peut être envisagée sur ce chef à cause des circonstances de l'infraction, du manque de transparence de l'accusé et des difficultés rencontrées lors du suivi de la peine d'emprisonnement avec sursis imposée à celui-ci en 2007. La décision comporte une revue très complète de la jurisprudence relative aux sentences pour le crime de leurre.

- *R. c. Aubut*, Cour du Québec, 2008 QCCQ 7722 (Canlii), 16 septembre 2008.

Une simple référence à un site web ne peut être assimilée à une expertise médicale

Dans une décision relative à une requête en rejet de plainte, le Comité de discipline du Collège des médecins du Québec déclare qu' « Il est indéniable que la simple référence à un site internet ne peut

d'aucune manière être assimilée à l'expertise médicale. »

- *Lacelle c. Boissinot*, 2008 CanLII 50519 (QC C.D.C.M.), 19 septembre 2008.

Proposition en vue de revoir le statut de la « monnaie électronique » – Union européenne

La Commission européenne a présenté une proposition en vue d'un profond réexamen des règles régissant les conditions d'émission de monnaie électronique au sein du territoire de l'Union européenne. La proposition fait le constat que les règles actuelles, datant de 2000, ont freiné le développement du marché de la monnaie électronique et entravé l'innovation technologique. Les règles proposées entendent faciliter l'entrée sur le marché de nouveaux prestataires.

La proposition met de l'avant une définition de la «monnaie électronique» neutre d'un point de vue technologique, couvrant toutes les situations dans lesquelles un prestataire de services de paiement (établissement de monnaie électronique ou établissement de crédit) émet une valeur stockée prépayée, en échange de fonds. Dans le cadre actuel, la monnaie électronique était définie comme « une valeur monétaire représentant une créance sur l'émetteur qui est stockée sur un support électronique ; émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise et acceptée comme moyen de paiement par des entreprises autres que l'émetteur. » Dans le cadre proposé, la monnaie électronique se trouve définie comme une valeur monétaire stockée électroniquement lors de la réception de fonds et qui sert à payer des transactions. Cette définition vise la monnaie électronique détenue sur des instruments de paiement en la possession du détenteur comme les cartes prépayées ou stockées à distance sur un serveur.

La proposition apporte aussi une clarification de l'application des obligations en matière de remboursement. Le principe de la remboursabilité est la clé de voûte du régime légal de la monnaie électronique. Ce principe suppose que le porteur peut, pendant la période de validité, exiger de l'émetteur qu'il le rembourse à la valeur nominale en pièces et en billets de banque ou par virement à un compte sans exiger d'autres frais que ceux qui sont nécessaires à la réalisation de l'opération.

- COMMISSION OF THE EUROPEAN COMMUNITIES, *Proposal for a Directive of the European Parliament and of the Council of on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directive 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC*, 9.10.2008.
- Dossier des travaux sur la réglementation du « E-Money ».
- Étienne WERY, « Monnaie électronique: bientôt une version 2.0 du cadre juridique » *Droit & Technologies*, 16 ocotobre 2008.

Analyse de l'effectivité des politiques de confidentialité

Il revient aux gestionnaires d'environnements électroniques de préciser leurs intentions en matière de protection des renseignements personnels. Ces intentions sont habituellement affichées dans une politique de confidentialité qui doit forcément répondre aux questions suivantes : quoi, pourquoi, pour qui, comment, quelle sécurité, quels droits pour les personnes concernées.

Pour aider les gestionnaires d'environnements électroniques, diverses études ont préconisé des efforts afin d'améliorer la lisibilité des politiques de confidentialité. C'est ainsi que plusieurs experts recommandent que les informations relatives au traitement des renseignements personnels soient rendues disponibles aux usagers au moyen de politiques exprimées dans des textes courts et accessibles.

Cette étude passe en revue les nouvelles tendances qui sont désormais admises en matière de politiques de confidentialité , notamment pour les sites Internet.

- Cynthia CHASSIGNEUX, « Pour une analyse de l'effectivité des politiques de confidentialité », *Communication-Commerce électronique*, no. 9, septembre 2008, pp. 7-14.

La régulation du web 2.0

La *Revue du Droit des technologies de l'information* a publié un numéro consacré aux nouveaux services d'Internet face au droit. On y présente des « regards croisés sur le web 2.0 ».

Dans une étude introductive rédigée par Pierre Trudel, on peut lire que le rôle central de l'usager est souvent présenté comme une caractéristique majeure du web 2.0. L'expression « Web 2.0 » vise des situations dont le trait commun est une intensité accrue de l'implication des usagers dans les environnements en ligne. Alors que plusieurs fonctions emblématiques d'Internet des premières époques se présentent sous une forme analogue aux médias diffusés, le web 2.0 prend résolument l'allure d'un réseau. Au sein du réseau, les usagers, professionnels ou amateurs, assument des rôles déterminants aussi bien au plan des contenus que des processus de fonctionnement. Mais en plus, ils sont en situation d'engendrer des risques pour les autres, ce qui les investit d'une capacité de régulation.

Dans un réseau, les régulateurs et les acteurs sont en position d'accroître ou de réduire les risques pour eux-mêmes ou pour les autres. La technique produit des situations qui augmentent ou diminuent les risques. Il en est de même pour les lois étatiques et les autres normativités. Dans le cyberespace, les acteurs envisagent les contraintes et possibilités techniques de même que les lois qui sont susceptibles de s'appliquer à leurs activités comme autant de risques à gérer. La régulation agissante à l'égard du Web 2.0 est essentiellement la résultante des stratégies de gestion des risques des acteurs et des régulateurs.

Une analyse préparée par Valérie-Laure Benabou intitulée « L'œuvre poulpe » relève que l'évolution récente du droit d'auteur conduit à l'accroissement du pouvoir de contrôle des ayants droit sur leurs œuvres. Les titulaires peuvent prétendre contrôler toute réutilisation de chaque élément de leurs œuvres et ce malgré l'absence de ressemblances suffisantes entre l 'œuvre première et l'œuvre seconde. Une telle tendance pourrait avoir pour effet de bloquer la créativité des auteurs « dérivés » en suscitant des conflits entre titulaires et en réduisant l'étendue du domaine public par la privatisation des ressources disponibles.

L'ouvrage propose également une analyse des dimensions juridiques de la neutralité d'Internet par Peggy Valke, Liyan Hou, David Stevens et Eleni Kosta. Présentant les réponses des autorités européennes aux enjeux de la neutralité d'Internet, l'étude souligne les principaux arguments en faveur ou à l'encontre des interventions afin de garantir la neutralité du réseau ou encore afin de baliser les interventions qui pourraient se révéler comme étant des pratiques restrictives à l'égard de certains types de contenus.

Dans un article intitulé « Privacy 2.0 », les auteurs Gloria Gonzalez Fuster et Serge Gutwirth font le point sur certaines pratiques des sites de réseaux sociaux qui menacent la vie privée des internautes. Plaidant pour de nouvelles stratégies de protection, ils se demandent s'il ne faudrait pas garantir la protection de toute information circulant sur le réseau.

Une étude d'Étienne Montero examine les principaux problèmes relatifs aux responsabilités liées au web 2.0 au plan de la directive européenne sur le commerce électronique. À partir du constat que le web 2.0 fait apparaître des risques à ce jour passablement inédits, l'auteur approfondit la notion d'hébergement afin de mieux identifier les conditions auxquelles il est possible de bénéficier d'une exonération de responsabilité lorsqu'on assure ces fonctions. Une seconde partie dégage les obligations susceptibles de peser sur le titulaire de services web 2.0.

- *Les nouveaux services de l'Internet face au droit, Regards croisés sur le web 2.0*, Actes du colloque organisé le 10 octobre 2008, [2008] 32 R.D.T.I, 283-403.

À signaler

- Arnaud DIMEGLIO, « La suppression injustifiée d'un forum de discussion est sanctionnable en raison de la perte de données qu'elle engendre », *Droit & Technologie*, 1er octobre 2008.
- Franz WERRO, « Les services Internet et la responsabilité civile », [2008] *MediaLex* 119-132.

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.