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

November 20, 2009/20 novembre 2009

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

Breathalysers and Presumptions

A narrow point of statutory interpretation and of the use of circumstantial evidence was settled by the Ontario Court of Appeal in *R. v. Mulroney*. The accused was charged with impaired driving and with driving with a blood alcohol level over .08. The Crown led evidence from a qualified breathalyzer technician he had used an Intoxilyzer 5000C, that it was designed to receive and analyze breath samples for blood alcohol concentration, that it appeared to be working properly, that the respondent blew into the mouth-piece of the instrument as instructed, and that this provided a suitable sample for analysis for both the first and second tests that he administered. The accused did not cross-examine, but at the close of the Crown's case moved for a directed verdict. He argued that section 258(1)(c(iii) required the Crown to prove that the breath sample "was received from the accused *directly* into an approved container or into an approved instrument operated by a qualified technician" (emphasis added): since there was no evidence the breath sample went directly into the approved instrument, he held, the presumption could not be relied upon. The trial judge rejected this argument, but the summary conviction appeal court judge accepted it and acquitted the accused.

The Court of Appeal rejected the Crown's argument that the word "directly" modified only "approved container" and not "approved instrument": they held that there was an obligation to prove that element in either case. However, they held that the evidence at trial did prove that element. The officer had testified "that the instrument was designed to receive and analyse breath samples, that it appeared to be working properly, that the respondent blew into the mouth-piece of the instrument as instructed, and that this provided a suitable sample for analysis" (para 20). This was, they held, sufficient circumstantial evidence for the trial judge to conclude that the sample had gone directly into the instrument.

CRTC Issues Traffic-Shaping Guidelines

Subsequent to its earlier public notice aimed at developing a policy to balance the use of the Internet for various purposes with the legitimate interests of ISPs to manage the traffic on their networks, consistent with legislation, including privacy legislation, (and which resulted in roughly 15,000 submissions) the Canadian Radio-television and Telecommunications Commission (CRTC) has issued a regulatory policy on the issue. The CRTC had earlier concluded that traffic-shaping was a legitimate exercise on the part of Internet Service Providers (ISPs), but in this policy attached guidelines, rather than bright line rules, to the practice.

In particular, in responding to complaints about their Internet Traffic Management Practices (ITMPs), ISPs are to identify the need for any practice which discriminates against or prefers any users, and must demonstrate that the ITMP is designed to address the need and achieve the purpose and effect in question, and nothing else. They must also show that the ITMP discriminates or prefers as little as reasonably possible, that there is as little harm to secondary ISPs or end-users as reasonably possible, and that network

investment or economic approaches alone would not achieve the same purpose as the ITMP.

Further, the policy requires ISPs to adequately inform consumers, by displaying information related to their technical ITMPs on their websites. Online disclosure should include information about why the ITMP is being introduced, who is affected by it, when the Internet traffic management will occur; what type of internet traffic is subject to management; and how the ITMP will affect a user's internet experience, including the specific impact on speeds. This disclosure must be made a minimum of 30 days in advance of a new technical ITMP being implemented or an existing one being modified, or in the case of existing ITMPs, within 30 days of the guidelines having been issued.

The guidelines also include provisions relating to wholesale services and protection of privacy.

Domain Name Disputes

"mrpita.ca," "handifoods.ca"

In *Handi Foods Ltd. v. Bob Jenkins*, a 3-member CIRA panel (Donovan, Groom, Magnusson (Chair)) considered a dispute over the domain names mrpita.ca and handifoods.ca. The Complainant ("Handi Foods") is an Ontario-based food manufacturer that specializes in pita bread, and owns several registered marks containing the words MR. PITA. It has used the trade name "Handi Foods" in Canada since 1977. The Registrant ("Jenkins") had registered an apparently fraudulent contact address in Calgary, Alberta, and did not respond to the complaint.

The Panel had little trouble finding that the disputed domain names should be transferred to Handi Foods, given that they were "confusingly similar" to marks in which Handi Foods had rights (under 4.1(a) of the CIRA Policy) and had "no legitimate interest" in the names (under 4.1(c) of the Policy). The finding of interest was on the question of whether the registration had been made "in bad faith" under 4.1(b) of the Policy. The facts indicated that Jenkins had, fraudulently and unknown to Handi Foods, transferred the registration of the domain name to himself and transferred carriage of the domain name from Handi Foods' registrar to his own. The Panel focused on 3.7(b) of the Policy, which indicates that bad faith will be proven where a Registrant registers a domain name in order to prevent a Complainant from registering its own mark as a domain name. The Panel specifically found that this was the case here, since the registration "had the effect, from that point forward, of preventing the Complainant from continuing to register the Mark as a domain name"—and it was "reasonable to infer" that this was, in fact, Jenkins' purpose (p. 4).

However, 3.7(b) of the Policy also requires that the Registrant be shown to have "engaged in a pattern [of such activity]." To make this additional finding as to each of the domain names, the Panel used the fact that Jenkins had interfered with these two of Handi Foods' marks as evidence that there was a "pattern" of conduct. Accordingly, the fraudulent transfer of mrpita.ca was evidence of a pattern vis-à-vis whether registering handifoods.ca was part of a pattern, and vice versa.

"xchangecanada.ca"

In *United Business Media LLC v. TechnoPlanet Productions Inc.*, a 3-member CIRA panel (Haigh, Millar and Freeman (Chair)) presided over a dispute regarding the domain name xchangecanada.ca. The Complainant ("UBM") is a worldwide provider of business technology services, in particular the organizing and conducting of seminars and conferences, which it does under its CIPO-registered mark XCHANGE. The Registrant ("Techno") is an information technology firm which registered the domain name on October 28, 1998. In 2002 it entered into a licensing agreement with UBM for the holding of an "XCHANGE" event for Techno's benefit, which event apparently never materialized. It was not making any use of the domain name, which was parked.

The Panel first examined whether the domain name was "confusingly similar" to UBM's mark under 4.1(a) of the Policy. Noting the definition of the phrase "confusingly similar" in 3.4 of the Policy, the Panel noted that "the test is not one of confusion, as is normally found in Canadian trademark jurisprudence, but of resemblance" (p. 6). The Panel found that the domain name was confusingly similar to the mark, in that the domain name contained the mark and was phonetically similar, and because an Internet user who had knowledge of the mark might be led to think that the domain name user had some relation to UBM. The Panel then turned to the requirement

that the registration have been made "in bad faith" under 4.1(b) of the Policy, and found simply that insufficient evidence had been led by UBM to support a finding of bad faith under any of the criteria listed in 3.7 of the Policy.

It finally turned to whether Techno could be found to have "no legitimate interest" in the domain name. This finding was made easily by the Panel, for despite the previous business relationship between the parties that involved the use of the name, the name had not ever been used for any business purpose by Techno. Nor did it qualify under any of the other criteria for lack of legitimate interest in 3.6 of the Policy. The Panel did remark (at p. 8):

> The Registrant does not provide a plausible explanation of how it would employ the domain name in a legitimate business fashion if it were to do so. The Panel has to bring into question what the Registrant would do if their business requirements would dictate an otherwise use of the current domain name, and the commercial value thereof. Accordingly, the issues regarding bad faith would perhaps interact differently.

Because no bad faith had been shown, however, the Panel declined to order the domain name transferred to UBM.

"ontariocollege.ca"

In *OCAS Application Services Inc. v. iREx Corp.*, a 3-member CIRA Panel (Donovan, Groom and Magnusson (Chair)) heard a dispute regarding the domain name ontariocollege.ca. The Complainant ("OCAS") is an Ontario corporation established in 2001 to provide a centralized college application process for Ontario colleges, including all 24 of the province's public colleges. It claimed common law rights in the mark ONTARIOCOLLEGES.CA, which it registered as a domain name on 5 March 2002. The Registrant ("iREx") is an Ontario company which is in the business of obtaining generic domain names and providing for their use by advertisers. It registered the disputed domain name on 14 February 2003.

On the first question of whether the domain name was "confusingly similar" to the mark, the Panel gave extensive consideration to the question of whether OCAS had established the common law rights in the mark that it asserted, or indeed any rights prior to the registration date. It provided the following interesting exegesis on the interaction of common law marks and domain names:

> While domain names can function as, and be protected in law as trademarks, mere registration of a domain name as such will not secure trademark rights in a domain name. For a domain name registrant to secure common law trademark rights in a domain name, the registrant must have actually used the domain name in association with some goods or services. Such use must generate a trademark reputation associated with the domain name among consumers. The nature of that acquired reputation is that the domain name (now a common law trademark) now points consumers to a particular trade source (the domain name registrant who used the domain name) for the type of goods or services in association with which the domain name was used. It is this reputation that is protected under trademark law. The law permits the owner of such common law trademark to prevent others from using that trademark so as to mislead consumers as to the trade source of the goods or services in association with which the trademark is used (at p. 3).

The Panel also highlighted that, where a common law mark is inherently descriptive of the nature of goods or services associated with it, then trademark law requires that it acquire "secondary meaning" in order to be protected, i.e. that it have been so extensively used for those products as to be explicitly associated with them. The alleged mark "ontariocolleges.ca" had such a requirement attached to it.

OCAS claimed that it had started using the website ontariocolleges.ca in the fall of 2002. Both parties directed the Panel to the "Wayback Machine" (at www.archive.org/web/web.php), which revealed that while the website had been functional in 2002 and up to the date of iREx's registration, it had simply contained a message indicating that the site was down. OCAS also made reference to print publications containing the domain name beginning in 2002, but apparently filed insufficient evidence of them. In the end, the Panel concluded that OCAS had not discharged the burden on it to establish that

it had rights in a mark upon which the registered domain name might infringe, and therefore that the "confusing similarity" inquiry was not justiciable.

While the complaint could have been disposed of because of OCAS's failure on the first test, the Panel went on to find that the registration had not been made "in bad faith," primarily because of the genericity of the name; and that OCAS could not prove that iREx had "no legitimate interest" in the domain name, because the latter had used the name in good faith association with its goods and services, prior to receiving notice from the Registrant that its use was contested. The Panel also heard a claim of "reverse domain name hijacking" made by iREx, which contended that it was entitled to costs under the Policy because OCAS had made its complaint "unfairly and without colour of right." The Panel found that OCAS had a honest but mistaken belief that it had rights in the mark, in that it was being used in some ways prior to registration, and also on the ground that "it may not have been unnatural for the Complainant's member colleges to think, 'in Ontario "college" practically means us' and so to think that use of the domain name **ontariocolleges.ca** for a relatively short time would be enough to secure trademark distinctiveness in that domain name as a common law trademark" (at p. 10). The Panel declined to order the domain name transferred to OCAS, and also declined to make the order of costs requested by iREx.

New Identity Theft Offences

Royal assent has been given to Bill S-4, creating new offences related to identity theft and adding them to the *Criminal Code*. Most specifically, the new section 402.2 of the *Code* makes it an offence to obtain or possess "another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence". "Identity information" is defined broadly, to include biological or physiological information, and in particular "a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's licence number or password".

Other additions to the *Code* prohibit trafficking in identity information and unlawfully possessing or trafficking in government-issued identity documents.

Passenger Manifests, Section 8, and PIPEDA

In *R. v. Chehil,* the Nova Scotia Supreme Court has overturned the judgement at trial (reported in the IT.Can newsletter for March 6, 2009), and has found that the accused was not subject to an unreasonable search when police, without a warrant, checked the passenger manifest for his flight in the offices of Westjet at the Halifax International Airport. Two RCMP officers, who were known to the Westjet personnel as members of the drug enforcement team, asked the Westjet employees for permission to view the computer manifest, and were granted it. The officers were looking for passengers travelling alone who had purchased a one way ticket with cash shortly before departure and checking a single bag, a profile consistent with the travel pattern of drug couriers. The officers identified the accused, the last passenger listed, as fitting this profile, and when the flight arrived, the accused's bag was set aside along with nine others and examined by a sniffer dog. That dog indicated the presence of controlled substances in the accused's bag, and so the accused was arrested when he came to collect it. His bag was opened and found to contain three kilograms of cocaine. The trial judge concluded that this search had not been authorized by a warrant nor under the *Protection of Privacy and Electronic Documents Act* (PIPEDA) and therefore had violated section 8: he excluded the evidence. On appeal the Court of Appeal overturned that decision.

The Court of Appeal concluded that, based on the totality of circumstances test, the accused had no reasonable expectation of privacy in the information obtained. In that event, the officers' action in looking at the manifest had not constituted a search, and so there could be no violation of section 8. They noted that information privacy was in issue, a category which included a biographical core of personal information, but also extended beyond that. There was no evidence that the accused had a subjective

expectation of privacy in the information, and no reason to think that he would. The intrusion occurred in Westjet's offices, which was not a public place, but was less of an intrusion than a search of the accused's home. Westjet's website indicated that information given to them might be subject to disclosure in accordance with legal requirements (note that the court of appeal is not relying on this disclaimer as an actual authority for the police to obtain the information, but merely as a factor going to whether there was a privacy interest). The search was not conducted intrusively, and the information obtained was not intimate. On this latter point, the method of analysis of the trial judge and the Court of Appeal differed. The trial judge had considered at some length the kinds of information which *might* have been contained in the manifest: religion, physical or mental disability, health, reasons for travelling, or virtually any other information. The Court of Appeal held that the issue was the information actually targeted and obtained, which in this case was much narrower.

The Court also concluded that PIPEDA did not assist the accused in finding a section 8 violation. First, they found that the broad definition of "personal information" in PIPEDA did not assist the accused. Whatever the definition in PIPEDA, they said, section 8 only protects information which tends to reveal intimate details about a person's lifestyle and personal choices or specific and meaningful information intended to be private and concealed and in relation to which there is a reasonable expectation of privacy. In their view, PIPEDA merely recognized existing privacy rights, it did not, for constitutional purposes, create new ones. Accordingly, "reasonable expectation of privacy" for Charter purposes remained to be determined on the totality of the circumstances. Secondly, the fact that there might have been a breach of PIPEDA did not mean there was a section 8 claim. The Westjet employees might have contravened PIPEDA, and certainly acted in violation of their own company's policy when they allowed the RCMP to view the manifest. However, the court held, that breach of PIPEDA by Westjet meant the accused could complain under PIPEDA about Westjet: it did not mean the RCMP had violated the accused's section 8 rights.

The Court of Appeal went on to conclude that, if it was mistaken about finding no violation of section 8, it would not have excluded the evidence.

2ième partie

Utilisation par l'employeur de photos provenant du site Facebook de la travailleuse

Dans cette affaire, la Commission des lésions professionnelles ne peut conclure que la travailleuse s'est infligée une entorse lombaire sur les lieux du travail, alors qu'elle était à son travail. D'abord, il n'y a pas de preuve quant au diagnostic. Il y a également les différentes versions données de l'événement par la travailleuse. De plus, certaines photographies produites à l'audience montrent la travailleuse en vacances en République Dominicaine, en janvier 2008, dans des positions peu compatibles avec une souffrance lombaire aussi importante que ce qu'elle décrit à ses médecins à la même période. En effet, des photographies prises lors de cette semaine de vacances, provenant du site de la travailleuse sur « Facebook », ont été imprimées par l'employeur et produites à l'audience. Ces photographies montrent la travailleuse en compagnie d'ami(e)s, dans différentes positions et s'adonnant à des activités diverses (baignade, aérobie). Ces photographies ne laissent pas voir que la travailleuse était souffrante à ce moment-là ou qu'elle avait de la difficulté à se mouvoir. Cela aussi vient entacher sa crédibilité.

- *Garderie Les « Chat » ouilleux inc. et Marchese*, 2009 QCCLP 7139 (CanLII), 26 octobre 2009.

Lieu d'introduction d'une action fondée sur un libelle de presse dans un médium de communication électronique

La demanderesse réclame des dommages pour atteinte à la réputation. Le défendeur aurait placé une annonce dans la revue « Émeraude Plus » invoquant que la demanderesse a fait de la fausse publicité dans cette même revue, ainsi que d'autres propos diffamatoires affichés par la suite sur le site Internet du défendeur. Le défendeur, soulevant les articles 68 et 163 C.p.c., demande le renvoi devant le tribunal de Joliette. Le Tribunal doit décider si l'action présente un rattachement suffisant au district judiciaire de Montréal ou si les procédures doivent être renvoyées devant le tribunal du forum naturel de la résidence du défendeur qui est aussi le forum choisi par les parties dans un contrat formé entre eux (district de Joliette).

L'article 68 al. 2 indique que dans le cas d'une action fondée sur un libelle de presse, l'action peut être portée devant le tribunal du district où réside le demandeur, lorsque l'écrit y a circulé. La difficulté de ce dossier, souligne le tribunal, réside dans le fait que la requête introductive d'instance allègue deux formes de publicité faisant partie de la cause d'action : une annonce publiée dans une publication qui circule à Montréal et une annonce faisant partie d'un site web du défendeur. Si les allégations de l'action étaient strictement limitées aux propos tenus dans la publication de la revue, l'action serait clairement qualifiée d'une « action fondée sur un libelle de presse ». Le Tribunal est d'avis que le fait d'ajouter dans cette action des allégations de libelle diffamatoire subséquentes dans un médium de communication électronique ne change pas de façon fondamentale la nature de l'action. Les propos tenus sur le site web présentent une certaine connexité avec la publication initiale faite dans la revue et dans le contexte, tous ces propos forment un tout.

Et le tribunal de conclure qu'il *« est donc de l'économie de notre Code de procédure civile que l'ensemble des allégations fasse partie d'une seule action portée devant le tribunal du district où l'écrit de presse a circulé pourvu que la demanderesse y réside. Dire le contraire permettrait au défendeur ayant fait un libelle de presse d'éviter le principe de l'alinéa 68. o2. in fine en continuant la diffamation par un moyen électronique, tel l'Internet, frustrant ainsi l'intention du législateur de permettre au demandeur dans une action de libelle de presse de poursuivre devant le tribunal du district de sa résidence, pourvu que le journal y circule. »*

- *Blais c. Couture*, 2009 QCCQ 10968 (CanLII), 23 octobre 2009.

Protection des titulaires de cartes de débit victimes de transfert de fonds non autorisé

Depuis les années 1960, les nouvelles technologies ont favorisé l'émergence de mécanismes de paiements électroniques (carte de crédit, carte de débit, paiement préautorisé et paiement par Internet) et le chèque cède peu à peu le pas à ces derniers. À ce jour, seuls les chèques et les cartes de crédit font l'objet d'une protection législative au Canada et au Québec. La relation entre un titulaire québécois d'une carte de débit et un émetteur ou un commerçant n'est régie que par le Code civil du Québec. En raison de la popularité croissante de la carte de débit, le Groupe de travail sur le transfert électronique de fonds a adopté le Code de pratique canadien des services de cartes de débit en mai 1992 afin de protéger les consommateurs qui font usage de la carte de débit au Canada et de régir la responsabilité des parties lors d'un transfert de fonds non autorisé. Les contrats bancaires ont graduellement incorporé les dispositions de ce code d'application volontaire, mais ils comportent plusieurs divergences par rapport à ce dernier qui s'avèrent défavorables pour le consommateur. En comparant les protections offertes par les États-Unis et par trois pays de l'Union européenne, soit la France, la Belgique et le Luxembourg, l'auteur propose une réforme de la réglementation des cartes de débit au Canada, pour combler les lacunes causées par cette inadéquation entre le Code de pratique canadien des services de cartes de débit et les contrats bancaires. Cette réforme ne pourra se produire que par l'intervention du législateur.

- Marc LACOURSIÈRE, « Propositions de réforme pour une protection des titulaires de cartes de débit victimes de transferts de fonds non autorisés », (2009) 54 *McGill* L. J. 91-132.

Exigences du CRTC concernant le recours aux pratiques de gestion du trafic Internet

Dans sa politique réglementaire de télécom CRTC 2009-657, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a mis en place un nouveau cadre pour guider les fournisseurs de services Internet (FSI) lorsqu'ils utilisent des pratiques de gestion du trafic Internet (PGTI). Le Conseil exige que les FSI avisent les consommateurs concernant les pratiques qu'ils utilisent, ce qui aidera les consommateurs à prendre des décisions plus éclairées au sujet des services Internet qu'ils achètent et qu'ils utilisent. Pour le CRTC, les pratiques de nature économique sont les PGTI les plus transparentes. Elles associent l'utilisation que font les consommateurs des services avec leur volonté de payer pour une telle utilisation, laissant ainsi le contrôle aux utilisateurs et permettant aux forces du marché de s'exercer. Mais lorsqu'elles sont utilisées, de telles pratiques doivent répondre à des besoins précis et être appliquées en toute transparence.

Les FSI ont l'obligation d'informer leurs clients trente jours avant la mise en place d'une pratique à caractère technique. Ce délai sera de 60 jours pour leurs clients revendeurs. Les FSI devront alors préciser l'incidence que cette pratique aura sur le service qu'ils offrent à leurs clients.

Afin de répondre aux besoins en évolution des utilisateurs d'Internet, le Conseil invite les FSI à faire les investissements nécessaires pour augmenter autant que possible la capacité de leurs réseaux. Toutefois, le Conseil reconnaît qu'à certains moments, les FSI pourraient devoir recourir à d'autres mesures pour gérer le trafic sur leurs réseaux.

Dans la mesure du possible, les FSI devront favoriser les pratiques de gestion du trafic Internet à caractère économique. Ces pratiques sont les plus transparentes, car elles sont indiquées clairement sur les factures mensuelles – une information qui permet aux consommateurs de comparer les différents services Internet et de faire concorder leurs besoins de bande passante avec leur volonté de payer pour son utilisation. Quant aux mesures à caractère technique pour gérer le trafic, telles que le lissage du trafic, elles devraient être mises en place seulement en dernier recours.

- CRTC, Politique réglementaire de télécom CRTC 2009-657, *Examen des pratiques de gestion du trafic Internet des fournisseurs de services Internet*, 21 octobre 2009.

Google coupable d'exploitation contrefaisante d'une photographie – France

Monsieur R. est photographe et l'auteur d'une photographie de Patrick Bruel prise lors du festival de Marrakech en 2001. Le photographe et le producteur du cliché indiquent avoir constaté que cette photographie était accessible sur Internet au travers du site aufeminin.com avant d'être reprise par le moteur de recherche Google Images, sans qu'ils aient donné d'autorisation en ce sens. Ils ont notifié la diffusion litigieuse de cette image au site qui a procédé à son retrait. Ayant cependant constaté que la photographie était de nouveau accessible au travers des mêmes sites, ils ont fait assigner la société Google Inc, la société Google France et la société Aufeminin.com devant le Tribunal de Grande Instance de Paris pour l'exploitation contrefaisante de la photographie par son visionnage et la possibilité de téléchargement.

En ce qui concerne la société aufeminin.com, peu importe que ce même cliché avait été posté par deux internautes différents, le tribunal met en cause la responsabilité du site. Le site aufeminin.com n'a pas accompli les diligences nécessaires pour rendre impossible la remise en ligne de la photo déjà signalée comme illicite. Le site ne pouvait donc pas se prévaloir de la limitation de responsabilité prévue par la *Loi pour la confiance dans l'économie numérique* (LCEN) pour les hébergeurs. Quant aux sociétés Google, le tribunal reconnaît des actes de contrefaçon de droits d'auteur. Les éléments d'identification de la photographie sur le service Google Images ne comportent aucune mention relative à l'auteur, portant ainsi atteinte à son droit de paternité. Au surplus, la photographie a été recadrée, ce que les sociétés Google ne sauraient utilement contester dans la mesure où figure sur le site incriminé la mention "il est possible que l'image soit réduite"; ainsi, un tel mode de diffusion ne permet qu'une visualisation de mauvaise qualité en raison notamment de la taille du cliché. L'atteinte au droit patrimonial du photographe est également constituée du fait des diffusions successives sans autorisation. Le tribunal condamne les sociétés Google Inc et France ainsi qu'Aufeminin.com à verser solidairement 10 000 euros de dommages-intérêts au photographe au titre de l'atteinte à ses droits patrimoniaux et 10 000 euros pour l'atteinte à son droit de paternité et à l'intégrité de l'œuvre constitué d'une photographie de Patrick Bruel prise lors d'un festival.

- *H & K, André R. / Google*, Tribunal de grande instance de Paris, 3ème chambre, 2ème section Jugement du 9 octobre 2009, disponible à *Legalis.net*.

Suspension du dispositif de « whistleblowing » en vertu de la législation sur les renseignements personnels – France

Le tribunal de grande instance de Caen a suspendu le dispositif d'alerte de la société Benoist Girard, filiale du fabricant américain de matériel médical Stryker, pour non-conformité avec la Loi Informatique et libertés. La loi américaine Sarbannes-Oxley impose aux sociétés cotées en bourse ainsi qu'à leurs filiales étrangères de mettre en place un dispositif d'alerte (whistleblowing) permettant aux salariés de dénoncer les fraudes et les malversations comptables ou financières dont ils auraient connaissance.
En France, ces systèmes sont licites, à condition notamment de respecter la Loi Informatiques et libertés.

- *Comité d'Entreprise Benoist Girard et autres / Benoist Girard*, Tribunal de grande instance de Caen, Ordonnance de référé, 5 novembre 2009, disponible à *Legalis.net*.

Nouveau cadre juridique pour la monnaie électronique – Europe

La nouvelle directive 2009/110/CE du 16 septembre 2009 sur la monnaie électronique définit celle-ci comme « une valeur monétaire qui est stockée sous forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement [...] et qui est acceptée par une personne physique autre que l'émetteur de monnaie électronique » (article 2). Sont autorisés à émettre de la monnaie électronique: les établissements de crédit, les établissements de monnaie électronique

(EME), les offices des chèques postaux habilités en droit national à émettre de la monnaie électronique, la banque centrale européenne, les banques centrales nationales ou les États membres eux-mêmes.

Pour créer un EME et obtenir l'agrément, il faut actuellement un capital initial d'1 million d'euros. La nouvelle directive abaisse ce seuil à 350 000 euros (article 4 de la directive 2009/110/CE), ce qui devrait permettre à des opérateurs plus petits d'entrer sur le marché et ainsi diversifier l'offre de services.

La directive précise en effet dans son article 16 que « les États membres ne peuvent maintenir en vigueur ni introduire des dispositions différentes de celles contenues dans la présente directive ». Les États membres ont jusqu'au 30 avril 2011 pour transposer la nouvelle directive dans leur droit interne. Des dispositions transitoires sont néanmoins prévues pour faciliter les démarches des opérateurs ayant déjà obtenu un agrément. Les EME qui ont commencé leur activité avant le 30 avril 2011 conformément à la législation précédente pourront continuer leur activité jusqu'au 30 avril 2012 sans solliciter un nouvel agrément.

- Etienne WERY, « Un nouveau cadre juridique européen pour la monnaie électronique », *Droit & Technologies*, 16 novembre 2009.
- « Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE », *Journal officiel de l'Union européenne*, 10.10.2009, L 267/7, disponible à *Droit & Technologies.*

À signaler

- Christine LEBRUN, « L'avocat a-t-il l'obligation de chiffrer ses courriels confidentiels en vertu de l'article 34 de la Loi concernant le cadre juridique des technologies de l'information ? », *Lex Electronica*, vol 14 no 2 (Automne 2009).
- Christine RIEFA, « The reform of electronic consumer contracts in Europe : towards an effective légal framework? », *Lex Electronica,* vol 14 no 2 (Automne 2009).
- Rajab ALI, « Technological Neutrality », *Lex Electronica*, vol 14 no 2 (Automne 2009).
- Lionel THOUMYRE, « Atelier ''Droit à l'oubli" ou comment remédier à la postérité d'un postérieur », *JURISCOM.NET*, 13 novembre 2009.

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.