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

March 20, 2009/20 mars 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

Contract: Electronic Acceptance of Electronic Offer

The British Columbia Supreme Court has delivered its ruling in *Burnett v. Rexel Canada Electrical Inc.* The Plaintiff, who worked for the Defendant for twenty years, was dismissed without notice and offered six months pay in lieu of notice. He rejected the offer and was paid statutory severance of eight weeks. The Plaintiff commenced an action against the Defendant. Parties subsequently agreed to settle. In a proposed term of settlement e-mailed to the Plaintiff on November 24, the Defendant offered to pay the Plaintiff a lump sum of $80,000 subject to detailed conditions. Of interest was the requirement that the Plaintiff signed a statutory declaration in which, among other things, he confirmed that he had been diligently searching for alternative employment and had not received an offer of employment (para. 6). The offer was accepted the next day by e-mail to Defendant's lawyer sent by Plaintiff's lawyer. On Nov. 26 at about 10.00-10.15am, the Plaintiff executed the statutory declaration, after having agreed that payment will be effected in 14 days time and after the implementation of other details in regard to tax assessments, RRSPs, etc. At 2.14pm the same day, Defendant's lawyer e-mailed the Plaintiff's lawyer indicating that the arrangement was acceptable to them, but indicated that his client's in-house counsel wanted to see scanned copies of the executed documents before the cheques are mailed out. That same day at approximately 4.30-5.00pm the Plaintiff received an offer of employment from an Alberta company with whom he had previously interviewed. He accepted the offer of employment the next day but did not tell his lawyer. That same day, his lawyer sent an e-mail to the Defendant's lawyer attaching the signed statutory declaration. When the parties discovered what happened, the Defendant alleged that the Plaintiff was in breach and that the declaration was false and misleading. The Defendant refused to pay the agreed settlement.

It is the Plaintiff's case that the settlement agreement was completed upon the acceptance of the offer on Nov. 25 and that when he signed the declaration, he did not have any job offer. Agreeing with the Plaintiff, the court rejected the contention of the Defendant that there was no acceptance of their offer until the time the documents were received on November 27. The court held: "The defendant required this statutory declaration. The Plaintiff signed it. It was true at the time he signed it. He complied with all the conditions of the agreement … the plaintiff is entitled to enforce the settlement agreement as set out in the defendant's letter of November 24, 2008, which was accepted by the plaintiff by email of November 25, 2008, or, at least, at 2.14pm on November 26, 2008 [when the plaintiff signed the declaration in his lawyer's office]" (paras. 40-41).

Criminal: Use of DNA Sample Pending Conviction Appeal

The Nfld. & Labrador Supreme Court has delivered its ruling in *R v. Newell*. The accused in this case was convicted for a prior robbery pursuant to which a DNA sample was provided. That sample matched evidence from other crime scenes. While his appeal from the robbery conviction was pending, police used information about the DNA match to support an application for a DNA warrant to obtain blood samples from the accused for comparison with biological evidence from other crime scenes. At

the time of their application for the DNA warrant, the police did not know that the accused's appeal against his conviction had been allowed and the DNA order set aside. However, the accused was convicted for theft. Meanwhile, the sample obtained from the accused pursuant to the warrant matched biological evidence from other crime scenes. The provincial court judge ruled that the accused's charter rights against unreasonable search and seizure were violated at the time the police used the information relating to the DNA match to secure the DNA warrant after the DNA sample order has been nullified. After excluding evidence procured from executing the warrant, the judge acquitted the accused. According to the court, the lawfulness of the DNA sample in the databank was compromised during the investigation of the accused on the present charges, specifically within the period between the time of the match and the application for the warrant. According to the court, there was no longer a basis upon which the accused should have reduced expectation of privacy in regard to his DNA sample.

In allowing the Crown's appeal, the Supreme Court set aside the provincial court's acquittal of the accused and remitted the matter to trial. The Supreme Court held that the provincial judge erred in finding that the accused's rights were violated. According to the Court, the accused remained a convicted offender at the time the warrant was issued, notwithstanding that the DNA order had been set aside. The Crown has a 60 day period to appeal against that decision which was yet to expire at the time the warrant was obtained. Accordingly, the Court held that contrary to the finding of the court below, the accused has a reduced expectation of privacy in regard to information that was released from an official DNA databank. The Court concluded by finding that there was no evidence of police misconduct or willful blindness, and that the "DNA information in the databank had already escaped Newell's possession and control when it was used, further reducing his expectation of privacy".

Criminal Sentencing: Online Dating Ban for Online Con-Man

The Ontario Court of Appeal has delivered its decision in *R v. Cagnotti*. In that case, Mr. Cagnotti appealed his sentence of 18 months' imprisonment following his conviction for three counts of breach of probation and a non-contact order. Under the probation order, he was required to not engage in online dating and not hold himself out online as a person available to a prospective partner. Before he was sentenced, the judge observed, that given Mr. Cagnotti's extensive record for fraud, the sentence proposed by counsel on both sides was insufficient. The trial judge gave parties notice of his intention to reject the sentence they proposed. The judge then proceeded to sentence Mr. Cagnotti to 18 months' imprisonment. Dismissing, Mr. Cagnotti's appeal, the Court of Appeal held that "Cagnotti was an incorrigible con-man who sought to victimize women for financial gain, and who showed no respect for court orders. The sentencing judge was justified when he imposed a higher sentence than that jointly proposed by counsel; the proposed sentence [by counsel] was contrary to the public interest and the administration of justice" (para. 1).

Defamation and Defence of Justification: Beyond Video Clip Evidence

The BC Supreme Court has delivered its ruling in *Kerr v. Ladner*. In that case, the Plaintiff sued the Defendant for defamation. The Defendant stated in a *CBC Radio One* broadcast while giving an account of what transpired at the Standing Committee Meeting of the Council on Planning and Environment that the Plaintiff, Mr. Kim Kerr, "after the meeting in the Council Chambers, came up to Councillor [Elizabeth Ball], and said, "you'd look good lying in an alley, on your back in an alley, with that red scarf tied around your neck" (para. 2). According to the Plaintiff, what he actually said to Ms. Ball at the contentious meeting was "May be you can take your red shawl and give it to a woman who is going to be cold on the street tonight, because as nice as it may look on you, it could come handy" (para. 6). This was in reference to the Committee's motion which deferred decision to future meeting of the Council on the issue of a moratorium on conversions of single resident accommodations, a subject in support of which the Plaintiff had spoken at the meeting. The version of what transpired as recorded by a filmmaker in attendance confirmed the Plaintiff as

saying: "May be you can take your red shawl and give it to a woman who is going to be cold on the street, because as nice as it looks on you, it could come in handy" (para. 9). Clearly, the death threat aspect was missing from the filmmaker's recording. After the filmmaker's attention was drawn to the controversial statement, he decided to post that portion or clip of his recording to YouTube. The filmmaker said he left after the Committee Meeting and did not attend the Council Meeting that started immediately after. The defence maintained that the part of the statement that contained a death threat was actually made by the Plaintiff even though it was not captured by the filmmaker's recording. The defence called witnesses who testified that the Plaintiff's rage continued after the Committee Meeting and suggested that the offensive statement could have been made between the end of the Committee Meeting and the beginning of the Council meeting. In upholding the Defendant's defence of justification, the court held that the five minutes interval between the end of the Committee Meeting and the beginning of Council Meeting was "too far short a time to rule out the possibility that Mr. Kerr returned to the Council Chambers again, after the Schmidt video clip, and made further comments to Councillor Ball…" (para 21). The court further ruled: "I accept that the impugned statements were made. This being so, defence of justification succeeds…the action is dismissed" (para 23).

Domain Name Disputes

"extremefitness.ca"

In *Extreme Fitness Inc. v. Gautam Relan*, a 3-member CIRA panel (Freedman, Martin and Richard, Chair) heard a dispute regarding the domain name extremefitness.ca. The Complainant, Extreme Fitness Inc. ("Extreme") is a Toronto-area fitness club operator that has 13 locations and which had revenues of over $45 million in 2004 and 2005. It owns the registered trademark EXTREME FITNESS (Design), the unregistered mark EXTREME FITNESS and a similar trade name, and operates a website at extremefitness.info. The Registrant ("Relan") is an individual who resides in Ontario, and was a member of one of the Extreme Fitness fitness clubs in January 2005, which is when the domain name was registered. As of August 2008 Relan was using the domain name to redirect users to the website "ripoffreport.com," a consumer protest site. Upon receipt of a cease and desist letter from Extreme, he redirected the domain name to the site of the Ontario government's Ministry of Small Business and Consumer Services. Some inconclusive negotiations were held regarding the sale of the domain name to Extreme, events which Relan denied but the Panel found as fact.

The Panel first considered the requirement under 4.1(a) of the CIRA Policy that a Complainant prove that the disputed name is "confusingly similar" to a mark to which the Complainant had rights and used prior to the registration. Even though the formal registration of the EXTREME FITNESS mark had occurred after registration of the domain name, the Panel was satisfied that Extreme had rights in the mark prior to that date, on the basis of magazine articles, print advertisements and promotional materials that dated back to 2001 and 2004, respectively. Given that the domain name was identical to the mark, it was found to be "confusingly similar." The Panelists next considered whether Relan had "no legitimate interest" in the domain name, as defined in 3.6 of the Policy. It noted that Relan had submitted no evidence on any of the criteria for legitimate interest and had failed to explain his use of the site to redirect to consumer complaint websites. Accordingly, he had no legitimate interest. Lastly the Panel turned to whether the registration had been made "in bad faith." It first examined whether, as per 3.7(a) of the Policy, the registration had been for the purpose of selling the domain name to Extreme or a competitor, noting that Relan had not denied Extreme's submission that this was the case nor had he provided any credible evidence for what his purpose was. The Panel found that he had, in fact, "patiently waited for the Complainant to initiate discussions regarding the sale of the domain name," and that this was his primary purpose in registering (para. 65).

The latter was by itself sufficient to ground a finding of bad faith, but the Panel also examined whether bad faith had been made out under 3.7(c) of the Policy, where an intention to disrupt the business of the Complainant constitutes bad faith. A majority of the Panel found that this criterion applied because Relan had been redirecting users to another website, making him a "competitor" because he was competing with Extreme for internet traffic. Panelist

Freeman disagreed with this finding, citing earlier decisions as authority for the proposition that what was required to be a "competitor" for this purpose was actual economic competition, and not just competition for traffic. He accordingly found that bad faith had not been made out under 3.7(c) and dissented on that point, but agreed with the overall result. The domain name was ordered transferred to Extreme.

International Cases of Interest

Self-Incrimination and Encryption Passwords

In *In re Grand Jury Subpoena to Sebastien Boucher*, Chief Judge W.K. Sessions of the Vermont District Court upheld a Government appeal of a subpoena issued to an accused requiring him to allow access to his laptop. The Canadian accused, Boucher, had been stopped at the border and arrested when a search of his laptop revealed evidence of child pornography. However, when investigators tried to access his laptop later, they discovered that the relevant drive was encrypted with PGP. A Grand Jury subpoena requiring Boucher to reveal his password had been quashed by a lower court. On appeal to Judge Sessions, the government submitted that it did not actually require the password—rather, it asked that Boucher be compelled to grant access to the drive's contents before the grand jury itself, literally by typing in his password without revealing it. Judge Sessions noted that the creation of the contents of the drive had not been compelled, and that the Government already had information about the drive, so that no privilege against self-incrimination attached to the contents themselves. The act of production before the Grand Jury would not actually form part of the government's case, since the government already had access to some of the information and could authenticate Boucher's possession of it without using the act of production as evidence. Accordingly, there would be no compulsory self-incrimination. The Government's appeal was upheld.

Indefinite Limitations for Internet Defamation

In *Times Newspapers Ltd. (Nos. 1 &2) v. The United Kingdom*, the European Court of Human Rights (ECHR) ruled on an application by *The Times* newspaper regarding the operation of the "Internet publication rule" in British defamation law. In December 1999 Grigori Loutchansky, a Russian businessman, had sued the paper, its editor and two journalists over two stories published in the fall of 1999 that linked Loutchansky to Russian organized crime. He brought a second action in December 2000, alleging that the continued availability of the impugned articles in the paper's web archives constituted a continuing publication of the libel. *The Times* sought to amend its defence to the second action to add a limitations defence, on the basis that the action was time-barred because the one-year limitation period had expired. Both the High Court and the Court of Appeal relied on an English defamation rule that each new publication gives rise to a separate cause of action—and thus, "in the context of the Internet, this meant that a new cause of action accrued every time the defamatory material was accessed" (para. 13). The House of Lords denied leave to appeal, and *The Times* petitioned the ECHR for a ruling that the "Internet publication rule" infringed its right to freedom of expression.

In argument, *The Times* emphasized the chilling effect that the rule had on the maintenance of archives, since any story which was alleged to have been defamatory would need to have a qualification attached to it in order to avoid a subsequent action for "continued publication"—a daunting task for a database which receives 500 articles per day. Thus they were constantly exposed "to litigation, without limit in time" by operation of the rule (para. 44). In its ruling, the Court acknowledged the importance of maintaining Internet archives as a means of making information available and preserving it, and agreed with *The Times* that it was within the scope of the protection afforded to freedom of expression. However, "the duty of the press to act in accordance with the principles of responsible journalism by ensuring the accuracy of historical, rather than perishable, information published is likely to be more stringent in the absence of any urgency in publishing the material" (para. 45). The Court held that the

duty to attach a brief qualification to an article was not overly onerous, pointing out that *The Times* had done so in this case. Accordingly, it held that in maintaining the rule, the government of the United Kingdom was within the margin of appreciation it enjoyed to impose "justified and proportionate restriction[s]" on *The Times*' freedom of expression. The application was dismissed.

2ième partie

Droit d'un témoin de témoigner en s'aidant de son ordinateur

Dans le cadre d'une audience en expropriation alors que monsieur Saleh s'apprête à témoigner dans sa propre cause, le procureur de la partie expropriante s'objecte formellement à ce qu'il puisse utiliser son ordinateur et, le cas échéant, le « print-out » du contenu de ses notes comme aide-mémoire. Le tribunal a donc à décider si un témoin ordinaire peut déposer sa version des faits devant le Tribunal en lisant ou en se référant à son ordinateur ou au « print-out » du contenu de ce dernier pour relater les événements eu égard à son recours et répondre ainsi aux questions de son procureur visant à établir la preuve de la partie expropriée. La partie expropriante s'objecte à l'utilisation des notes informatisées de la partie expropriée principalement parce que ces dernières ne sont pas contemporaines et devant « l'extrême importance », dans ce dossier, plaide-t-elle, « des événements relatifs aux circonstances ayant mené à l'expropriation », et devant le fait aussi que « monsieur Saleh est un témoin essentiel à la cause des expropriés.» De son côté, la partie expropriée fait valoir que : « le droit de recourir à un aide-mémoire pour rafraîchir la mémoire d'un témoin est largement reconnu par la doctrine et la jurisprudence ». Elle revendique le droit à l'utilisation de son ordinateur par le témoin invoquant l'article 2 de la *Loi concernant le cadre juridique des technologies de l'information*.

Le tribunal déclare que la doctrine enseigne aussi unanimement que des notes auxquelles peut se référer un témoin doivent être contemporaines et donc, consignées manuellement ou informatiquement, dans les meilleurs délais suite à la survenance d'événements, c'est-à-dire lorsqu'ils sont tout à fait frais à la mémoire du témoin ordinaire. Le Tribunal retient aussi l'importance d'être en mesure d'évaluer et de conclure à l'intégrité et à la contemporanéité d'un document auquel peut se référer un témoin, ce que notre Code civil du Québec énonce clairement ainsi que la *Loi concernant le cadre juridique des technologies de l'information*, sans minimiser les principes émis par les articles 138 et 139 de la *Loi sur la justice administrative* et qui relèvent de la discrétion de ce Tribunal.

- *Mont-Royal (Ville) c. Saleh*, 2009 QCTAQ 02914 (CanLII).

Application d'une clause externe à un connaissement disponible sur un site web

La demanderesse réclame une somme de 2 000 $ à la défenderesse, Courrier Purolator Ltée, pour des dommages causés à un tableau, lors de la livraison de deux colis. La défenderesse conteste cette réclamation en invoquant l'exclusion de responsabilité de Purolator, relativement aux dommages causés, en raison de l'article 9 du document intitulé «Modalités et conditions de transport». Ce document n'est disponible que sur le site Internet ou dans les Centres de distribution de la défenderesse et ledit article 9 ne fut jamais porté à l'attention de la demanderesse.

Le Tribunal est d'opinion qu'il s'agit là d'une clause externe au contrat de connaissement, au sens de l'article 1435 C.c.Q. Il est déraisonnable d'exiger d'un client d'aller visiter le site Internet de Purolator, avant de faire affaires avec la défenderesse et de prétendre que ledit client est alors lié par cette clause d'exclusion, ou toute autre clause apparaissant sur le site Internet d'une entreprise. Le Tribunal est d'opinion qu'au-delà du connaissement, la défenderesse Purolator a une obligation d'informations face à ses clients qui, comme la demanderesse, font appel à ses services. Il incombe aux préposés de Purolator de s'informer de la nature du contenu des colis et d'informer les clients de la défenderesse des exclusions qui s'appliquent au contenu de ceux-ci. Compte tenu de ces circonstances, le Tribunal estime que la clause d'exclusion de responsabilité apparaissant sur le site Internet de Purolator ne s'applique pas.

- *Joannette c. Courrier Purolator ltée*, 2009 QCCQ 621 (CanLII), 4 février 2009.

Qualification d'un contrat de développement de logiciel accessible par Internet

Aux termes d'un contrat, Oceanwide, une entreprise de développement de services informatiques à travers Internet, réclame de la défenderesse Transit la somme de 27 350,76$. Le contrat prévoit le versement initial d'une somme de 6 000$ pour la mise sur pied par Oceanwide du programme informatique pouvant répondre aux besoins du client Transit, plus un montant minimal de 500$ par mois jusqu'à concurrence de 100 expéditions, et 5$ de plus pour chaque expédition supplémentaire.

D'abord, le tribunal constate le bien fondé de la réclamation de Oceanwide étant donné qu'elle a fait diligence pour développer dans un court délai le logiciel pouvant répondre aux besoins spécifiques de Transit et qu'elle lui a offert suffisamment de formation. Ensuite le tribunal détermine qu'il s'agit d'un contrat d'entreprise ou de service régi par les articles 2098 et suivants du Code civil en examinant l'objet du contrat. Oceanwide devait développer un logiciel qui réponde aux besoins et spécificités de Transit, eu égard à ses activités commerciales, auquel il donnait accès uniquement par Internet. Le logiciel n'était pas installé sur l'équipement informatique de Transit. Même si Transit pouvait utiliser le logiciel dans le cours normal de ses affaires sans l'intervention de Oceanwide, par un simple accès à Internet et l'utilisation d'un mot de passe, cela demeurait un contrat de service puisque non seulement Transit utilisait le logiciel de Oceanwide et traitait ses données à partir du matériel informatique de Oceanwide mais celui-ci offrait un service d'aide technique pendant toute la durée du contrat, et demeurait disponible pour tout développement selon l'évolution des besoins de Transit. Étant un contrat d'entreprise, Transit pouvait ainsi le résilier unilatéralement en vertu de l'article 2125 C.c.Q. en payant, en proportion du prix convenu, les frais et les dépenses actuelles et la valeur des travaux exécutés avant la notification de la résiliation.

- *Oceanwide inc. c. Gestion King City et Transit King City,* 2009 QCCQ 1001 (CanLII), 10 février 2009.

La protection de la vie privée et les interceptions de communication – Étude de droit comparé

Cet article étudie le droit fédéral américain, le droit français et le droit allemand. Ces pays correspondent à des modèles de régimes juridiques et d'interceptions de télécommunications. Pour la France et l'Allemagne, le texte de référence en matière de vie privée et de secret de la correspondance est la Convention européenne de sauvegarde des droits de l'homme et la jurisprudence de la CEDH. Aux États-Unis, on ne reconnaît pas, comme tel, de valeur constitutionnelle à la vie privée. Malgré ces différences, il y a des traits communs : les interceptions de télécommunications légales, qu'elles soient judiciaires ou de sécurité sont régulées par des organismes de contrôle, a priori ou a posteriori. Ces organismes constituent-ils un alibi ou bien sont-ils un instrument pragmatique de protection des libertés individuelles ? Il est trop tôt pour donner une réponse définitive mais il est possible de tenter une approche analytique des législations, de la jurisprudence, et, parfois de la doctrine. Il ressort qu'une convergence se dessine, au-delà des divergences de culture juridique : les interceptions coïncident avec l'apparition de micro-structures qui ont pour mission d'apporter des garanties aux citoyens.

- Claudine GUERRIER, « Aux USA, en Allemagne, en France, quelle protection de la vie privée en matière d'interceptions de télécommunication ? », *Juriscom.net*, 9 mars 2009.

La réparation du dommage résultant de la contrefaçon sur Internet – Belgique

Cet article part du constat que faire le point sur les principes applicables à la réparation du préjudice en matière de droit d'auteur s'avère des plus utiles. Et cela aussi bien vis-à-vis des personnes concernées que des juristes et voire même du grand public qui ignore la plupart du temps les risques encourus. Les dommages et intérêts nés de la contrefaçon sont la sanction essentielle infligée par le droit au

contrefacteur pour réparer le trouble social qu'il a causé par ses agissements. Ils sont souvent sans commune mesure par rapport aux sanctions pénales que pourraient infliger les juridictions répressives. Trop souvent les titulaires de droits d'auteur vont s'acharner à prouver la violation de leur droit en oubliant ou en négligeant d'étayer une preuve convaincante de dommages. C'est sans doute là un des éléments qui peut expliquer la modicité, parfois indécente, de certaines condamnations.

La question de l'évaluation des dommages-intérêts prend donc une grande importance pratique et les titulaires des droits doivent dès lors s'attacher à prouver l'existence et l'ampleur de leur dommage.

- Alain BERENBOOM, « Contrefaçon sur l'Internet-Réparation du dommage », *Droit et technologies*, 13 mars 2009.

Qui est éditeur sur Internet ? – France

La détermination de celui qui assume une fonction d'éditeur sur Internet est cruciale lorsque vient le temps de déterminer la responsabilité à l'égard d'un contenu. Le défi n'est que plus grand lorsque le contenu est généré en tout ou en partie par les utilisateurs. Dans une affaire relative à la violation du droit à l'image d'une mannequin commise sur les pages web d'un jeune DJ, le Tribunal de grande instance de Paris a rejeté la demande tendant à obtenir la condamnation des sociétés Sivit, Universpodcast, MySpace Inc et ZePeople, qui hébergeaient ces pages, à payer des sommes à valoir sur les dommages et intérêts. L'ordonnance du 9 février 2009 a notamment refusé de suivre l'argumentation de la demande qui visait, pour les soustraire aux causes d'exonération de responsabilité attachée au statut d'hébergeur, à requalifier les sociétés défenderesses en «éditeurs». Le tribunal a plutôt insisté sur le fait « qu'il n'est pas soutenu que les sociétés défenderesses ont pu, avant la mise en ligne des contenus en cause, intervenir de quelque manière que ce soit dans leur création ». Selon Pierre Mimja, la déduction que fait le tribunal dans cette affaire serait en cohérence avec l'esprit du législateur. Il réfère au rapport des députés Jean Dionis du Séjour et Corinne Erhel du 23 janvier 2008 sur la mise en application de la LCEN indiquant que « La frontière entre le statut d'hébergeur et celui d'éditeur doit donc bien rester, comme l'a voulu la loi (…) la capacité d'action sur les contenus ».

- Pierre MIMJA, « La définition d'éditeur était dans la loi… », *Juriscom.net*, 11 mars 2009.
- *Kimberley P. c/ Vincent B., Sivit, Univerpodcast, MySpace Inc., ZePeople, Itunes Store*, Tribunal de grande instance, Paris, référé, 9 février 2009.

Obligation des hébergeurs de conserver les données d'identification – France

L'humoriste Roland Magdane a poursuivi Youtube suite à la diffusion non autorisée de certains de ses sketchs sur la plateforme de vidéos. Dans l'ordonnance de référé rendue le 5 mars 2009 par le Tribunal de grande instance de Paris, l'humoriste tire les conséquences de la qualification d'hébergeur de Youtube: une obligation de conservation des données d'identification des éditeurs, en l'espèce les internautes ayant mis en ligne les vidéos litigieuses, pèse sur le site. Il demande donc que lui soient communiqués les « noms, prénoms adresse, numéro de téléphone, et/ou raison sociale, nom du représentant légal, forme sociétale et/ou associative de l'éditeur se cachant sous divers pseudonymes ». Mais le tribunal a plutôt estimé que l'adresse IP et l'adresse de messagerie électronique suffisaient pour identifier les internautes à l'origine des diffusions litigieuses.

- *Roland Magdane et autres / YouTube*, Tribunal de grande instance de Paris, Ordonnance de référé, 05 mars 2009, *Legalis.net*.

La sécurité de l'individu numérisé – Réflexions prospectives et internationales

RFID, Web 2.0, « googleisation » … autant de néologismes et d'acronymes qui sont en train de devenir incontournables dans la société de l'information. Quelle est la place de l'individu dans cet univers ? Comment gérer les droits et libertés dans le monde des réseaux ? Comment assurer la sécurité dans les circuits informationnels qui envahiront les centres commerciaux, les rues et

les domiciles lorsque l'ubiquitous computing sera devenu réalité. Des spécialistes de divers horizons proposent des réponses à ces questions.

On peut signaler quelques textes: Stéphanie Lacour, « Ubiquitous computing et droit de la radio-identification »; Pierre Trudel, « Quelles limites à la 'googleisation' des personnes ? »; Claudine Guerrier, « La donnée biométrique et le document de voyage : le point de vue du juriste »; Jean-Jacques Lavenue et Gregory Beauvais, « La commercialisation des données personnelles, perspectives et prospective : l'exemple des données de santé et du DMP ».

- Stéphanie LACOUR, *La sécurité de l'individu numérisé – Réflexions prospectives et internationales*, Paris, L'Harmattan, 2008.

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.