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

January 12, 2012/12 janvier 2012

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Robert Currie and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School, and David Fraser. 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 et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie, et David Fraser. 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

## Admissibility of Surreptitious Audio Recording in Civil Proceedings

The Quebec Superior Court has admitted evidence gathered by the plaintiff through the use of a surreptitious pocket recording device in *Sagman v. Politi*. The plaintiff was involved in a dispute with his older brother: the plaintiff alleged that he had been deceived into transferring title to a condominium to his brother for the sum of $1, rather than the $1.2 million which had been the agreed price. The two had verbally agreed, the plaintiff maintained, that he would sell the condominium to his brother for $1.2 million dollars but that the transfer deed would indicate a price of $1: once title was transferred, the brother failed to pay the money, despite repeated requests. The brother agreed that the condominium had been transferred to him for $1 but maintained in court that this had been the agreement, and that it was to compensate him because he did not receive a just share of the estate of their late father.

Although the property and the action were in Montreal, both brothers lived in Toronto. After the dispute arose, the two had arranged to meet at a Starbucks at the corner of Eglinton and Bathurst. The plaintiff had purchased a pocket recording device and had activated it before arriving at the Starbucks. It recorded for one hour and fifty-four minutes, which included the entire conversation except for the final few minutes. Upon returning home the plaintiff downloaded the contents onto his computer, copied it to a disk and gave it to his attorneys for safekeeping. He sought to introduce it into evidence.

The trial judge noted that under the Civil Code of Quebec all evidence of any fact under dispute is admissible and may be presented by any means. In addition the rules provide that a statement may be proved by means of any reliable recording technique, provided the authenticity of the statement is separately proved. Finally the Code also requires a court to reject evidence obtained in circumstances that breach fundamental rights or freedoms or the use of which would tend to bring the administration of justice into disrepute. The court concluded that based on these considerations, the taped conversation was admissible.

Both parties agreed that the conversation had taken place at the time and place indicated. The plaintiff demonstrated his ability to operate the recording device and that he downloaded its entire contents to present to the court. The contents of the conversation were clear and audible throughout, and the brother did not suggest that the recording had been altered in any way. The only points of contention were that the recording ended a few minutes before the conversation did, and that the recording was carried out surreptitiously.

The brother maintained that during the unrecorded final minutes he had denied owing the plaintiff any money. The trial judge rejected this claim, holding that it was "illogical and preposterous and contradicts the whole tenor of his prior conversation" (para 92). In fact the brother had acknowledged owing the money, tried to extort the plaintiff into assisting the brother in another matter as a precondition of getting the money, and had threatened the plaintiff and his family if he did not assist. The trial judge therefore rejected the suggestion that the final

few minutes of the recording were material and contained a denial by the brother that he owed any money at all.

The trial judge also found that use of the recording would not bring the administration of justice into disrepute. The brother had in fact asked the plaintiff whether he was recording the conversation, and the plaintiff had denied that he was doing so. The trial judge held that the denial was not important, because the plaintiff was entitled to record the conversation in order to protect himself and to have a faithful record of what was said. The brother continued of his own volition to talk notwithstanding his suspicions he may have had and, the trial judge said "must bear the consequences of that decision" (para 88).

## No Costs Award for Computer Research

The trend not to allow a costs award for the expense involved in computer research has continued with the Alberta Court of Queen's Bench decision in *Clancy v. Gough*. The trial judge rejected a claim for recovering the cost of computer research and the cost of faxes, holding that these were not truly disbursements:

> 53 ... these are not expenses that are truly paid to third parties. Rather, the costs of subscribing to legal databases and purchasing and operating fax machines are overhead expenses necessary to run an effective legal practice in modern times. These expenses are similar in character to rent, office furniture, employee salaries, and telecommunication services...

## Search Warrants, Documents and Computers

The British Columbia Court of Appeal has handed down a decision on the ability of police to search a computer with its judgment in *R. v. Vu*. This decision can be seen as a companion decision to that of the Ontario Court of Appeal in *R. v. Jones* (reported in the IT.Can newsletter of October 19, 2011). Jones had dealt with the ability of police who have a warrant to search a computer to search it for evidence of a crime other than the one for which the warrant was issued. *Vu* considers the ability of the police who have a warrant to search a building to rely on that warrant as authority to search a computer found in the building.

The police were investigating a theft of electricity (though it seems clear that their real interest was the expectation that the electrical meter was being bypassed in order to operate a marijuana grow operation without being detected). They had obtained a warrant allowing them to search a house for equipment used to divert electricity, and also to search for documentation which would identify the owner or occupier of the residence. When they executed the warrant, they found two computers and a cell phone in the residence. The police examined those pieces of equipment, discovering that one of the computers was logged in to MSN messenger (under the accused's email account) and was also logged in to the accused's account on Facebook. The police also searched files on the computer, discovering the accused's resume on it. In addition, the police found a photograph on the cell phone of the accused holding the cell phone and taking his own picture in a mirror.

The accused argued that none of this evidence should be admissible against him, on the basis that the warrant should not be construed as permitting a search of the contents of the computer or the cell phone. The trial judge had accepted this argument and excluded the evidence. However, on appeal the British Columbia Court of Appeal held that that was an error, and that the warrant did in fact authorise those searches. The accused argued before the Court of Appeal that the warrant in question, by only referring to searching for "documentation", did not include electronically stored information, and that a computer or similar device would have to be named specifically in a warrant for it to be searched. The Court of Appeal rejected both of those claims.

The word "document", they held, was one that had "to be interpreted having regard to the technology and practices of the times" (para 55). They pointed to authority from 1897 concluding that a photograph could qualify as a document. Today, they noted, documents are often stored electronically but "[a] n electronically-stored version of, for example, a resumé or photograph, is as much a document as a paper (i.e., hard copy) version of the same item" (para 58). For that reason, a warrant to search for

"documents" would, without more, authorize a search for electronically-stored versions of those documents where appropriate. The court held that a computer, in this regard, was essentially no different from a four-drawer filing cabinet: the police would not need to know of its existence in advance and specifically mention it in the warrant in order to be able to search it, if it was a potential repository of what was sought.

The Court of Appeal did acknowledge that computers can include extensive personal and confidential information that might be unrelated to the offence being investigated. However, that merely went, they held, to the manner in which the search warrant was executed. As in *Jones*, the fact that the police have authority to search a computer for one thing does not give them carte blanche to rummage through its entire contents. Similarly in this situation, although the police do not need specific authorization to search a computer:

> 68...When the police, in the course of executing a warrant, locate a device that can reasonably be expected to contain an electronically-stored version of a thing they have been authorized to search for, they can examine that device for the purpose of determining whether it contains that thing (i.e., information), but only to the extent necessary to make that determination.

In this case all the evidence discovered – the photograph, the resume, the email address from MSN messenger, and the Facebook account – all fell within the terms of the warrant as documents which might identify the occupant. Accordingly all were properly gathered under the warrant and were admissible. The Court of Appeal did caution, however, that this result depended on the particular facts that the computer was already logged in to both MSN messenger and Facebook. They cautioned:

> given the dearth of evidence regarding the technical aspects of how either MSN Messenger or Facebook operate, nothing in these reasons should be taken as having decided whether Constable George could have looked for further information accessible through the active pages, e.g., by accessing portions of the Facebook page that were not already loaded on the computer. That issue would likely involve a consideration of ss. 487(2.1) and (2.2) of the *Criminal Code*, that, amongst other things, permits searches for data that is not stored within a computer, but is available to it. Those provisions were not the subject of argument on this appeal. (para 73)

## Images of plaintiff on Facebook are relevant and must be produced

In a very short decision (*Morabito v. DiLorenzo*, 2011 ONSC 7379), the Ontario Superior Court of Justice agreed with a defendant's motion that the plaintiff in a motor vehicle accident be required to re-attend at discovery to answer questions regarding photos posted on Facebook and to produce such photos. The plaintiff was claiming damages, at least in part, for loss of enjoyment of life.

At examination for discovery, the plaintiff acknowledged the existence of a Facebook account but refused to answer any questions regarding it or its contents. The defendants brought a motion to compel the production of such information. The plaintiff cited *Leduc v. Roman*, [2009] O.J. No. 681 as standing for the proposition that the mere existence of a Facebook account does not automatically entitle the defendant to access to it.

In the *Leduc* case, the defendant sought all of the contents of the plaintiff's Facebook page not based on particular knowledge (which might have been gained at cross-examination), but due to the knowledge of the defendant that such a Facebook page existed. It did not foreclose the possibility that relevant, discoverable information was posted to the Facebook page.

The Court in *Morabito* concluded:

> [5] Photographs of the plaintiff, taken before and after the accident, are relevant. Photographs after the accident show the effect of the injuries and whether and to what extent they affect his enjoyment of life. Photographs taken before the accident are relevant for comparison.

The plaintiff was ordered to re-attend at examinations for discovery, and to produce any responsive photographs.

## British Courts issue guidance on "tweeting" proceedings

The Lord Chief Justice of England and Wales has issued guidance on the practice of tweeting or other forms of live, text-based communications during hearings and trials (http://www.judiciary.gov.uk/Resources/JCO/Documents/Guidance/ltbc-guidance-dec-2011.pdf). It is generally unlawful, in English courts, to take photographs and to make sound recordings, and the reporting on court proceedings is regulated by the *Contempt of Court Act.*

Whether to permit tweeting from court is within the presiding judge's discretion. The guidance states that individuals who wish to do so must make a request of the presiding judge.

> Where a member of the public, who is in court, wishes to use live text based communications during court proceedings an application for permission to activate and use, in silent mode, a mobile phone, small laptop or similar piece of equipment, solely in order to make live, textbased communications of the proceedings will need to be made. The application may be made formally or informally (for instance by communicating a request to the judge through court staff).

A judge may also issue a decision on the matter on his or her own motion.

The criteria to be considered by the judge in determining whether to allow live-tweeting principally revolve around the impact on the proper administration of justice:

> 13) Without being exhaustive, the danger to the administration of justice is likely to be at its most acute in the context of criminal trials e.g., where witnesses who are out of court may be informed of what has already happened in court and so coached or briefed before they then give evidence, or where information posted on, for instance, Twitter about inadmissible evidence may influence members of a jury. However, the danger is not confined to criminal proceedings; in civil and sometimes family proceedings, simultaneous reporting from the courtroom may create pressure on witnesses, distracting or worrying them.

Notably, the guidance also suggests that "it may be necessary for the judge to limit live, text-based communications to representatives of the media for journalistic purposes but to disallow its use by the wider public in court."

## Ontario Privacy Commissioner campaigns against "Surveillance by Design"

Ann Cavoukian, the Information and Privacy Commissioner of Ontario has taken a very vocal and public stance against anticipated "lawful access" legislation, which is expected to be introduced by the federal government in the coming months. This legislation is expect to require telelcommunications service providers to only deploy technology that has built-in backdoors for law enforcement and national security access to communications and would permit telcos to provide a range of customer account information to law enforcement in the absence of a warrant.

The Commissioner is organizing a symposium titled "Surveillance by Design" in Toronto on January 27, 2012 featuring a range of high-profile speakers on the topic. More information can be obtained at www.realprivacy.ca.

# 2ième partie

## « Clavarder, c'est écrire »

La Cour devait déterminer si le contenu de conversations écrites, entre deux personnes, transmises sur un réseau de clavardage constitue de la pornographie juvénile telle que définie à l'article 163.1 du *Code criminel*. Autrement dit est-ce que ces propos constituent une infraction lorsqu'ils sont écrits en clavardant sur un ordinateur? En somme, est-ce que clavarder, c'est écrire ?

La Cour remarque que dans les articles 163.1 (1) b) et c) C.cr., par l'expression « de tout écrit », le législateur vise tout «document de quelque nature qu'il soit » et « tout mode d'après lequel et toute matière sur laquelle des mots ou chiffres, au long ou en abrégé, sont écrits, imprimés ou autrement énoncés… ». Par conséquent, le produit du clavardage est une conversation écrite utilisant des mots, au long ou en abrégé, sur support électronique, portée sur un forum virtuel, par exemple sur une page Web ou directement à l'écran de l'ordinateur de l'utilisateur. Ce ne sont pas de simples mots qui sont perdus dès leur expression. Le clavardage permet aussi à l'internaute de lire ce qui a été écrit précédemment, de sauvegarder la conversation en format électronique ou encore de l'imprimer. « Dès qu'une personne écrit un mot lors d'une séance de clavardage, le produit de cette communication est inscrit sur un serveur ou sur un ordinateur. Ce mot peut être lu, quel que soit son mode de présentation, suivant la définition de la Loi d'interprétation. » La Cour en conclut donc que le juge de première instance n'a pas commis d'erreur en décidant que les conversations sous forme de séances de clavardage auxquelles a participé l'accusé constituaient des écrits au sens des paragraphes 163.1 (1) b) et (1) c) du *Code criminel*, compte tenu de la façon de transmettre la communication (par l'écrit) et du support en permettant la lecture.

- *Gagné c. R.*, 2011 QCCA 2157 (CanLII), 22 novembre 2011.

## Diffamation par un maître de blogue – aucune preuve de dommages

Le demandeur poursuit le défendeur pour diffamation suite à la publication, sur son site Internet, d'une photo du demandeur estampillée « RCMP informant » et d'allégations qu'il qualifie de fausses et calomnieuses à son sujet. Le défendeur laisse entendre, entre autres, que le demandeur est un « RCMP informant », et ce, dans le cadre d'une conspiration de « terrorisme gouvernemental » dont il serait victime. De plus, le défendeur publie que le demandeur a déjà été accusé, dans une autre affaire, pour extorsion de fonds, et fait à noter, la Cour suprême du Canada a confirmé la culpabilité du demandeur à cette accusation.

Le tribunal constate que le défendeur n'épargne aucunement le demandeur par la publication d'allégations de toutes sortes. Nul doute, il existe une inimitié évidente entre le demandeur et le défendeur. Dans un tel contexte, la frontière de la diffamation est facilement franchie. Vu la grossièreté de certaines des allégations contenues dans les informations, le Tribunal conclut que le défendeur a diffamé le demandeur par la publication des informations sur le site. Mais au niveau des dommages, aucune preuve n'a été faite à cet égard. Le demandeur n'a produit aucun relevé des visites sur le site, ni fait entendre un seul témoin pour établir quelque dommage que ce soit relié à la publication des informations. Le tribunal déclare que le défendeur allègue tant de complots, et vise tant de personnes dans les informations, que la crédibilité du site en est sûrement affectée. Il est même possible que le public ait tout simplement ignoré les informations et le site vu la nature de ce qui y était publié.

- *Strecko c. Chamas,* 2011 QCCS 6085 (CanLII), 21 novembre 2011.

## Émergence des obligations de déclarer les incidents de violations de données à caractère personnel

La tendance du législateur est de prévoir, dans les textes relatifs à la protection des données personnelles, des dispositions imposant aux

responsables de ces données de déclarer les situations dans lesquelles la sécurité des données personnelles a été compromise. Ainsi, la directive européenne 2009/136/CE impose aux législateurs européens de prévoir des dispositions législatives obligeant non seulement à informer les personnes concernées que leurs données personnelles sont mises à risque mais également de déclarer aux autorités les situations de violations de données à caractère personnel. La tendance s'observe aussi au Canada où le *projet de loi C-12 modifiant la loi fédérale sur la protection des renseignements personnels et des documents électroniques* prévoit d'insérer une obligation de déclaration au Commissaire à la protection de la vie privée des atteintes importantes aux mesures de sécurité et une obligation d'informer les individus lorsque les atteintes présentent des risques de préjudice grave. Le Rapport quinquennal de la Commission québécoise d'accès à l'information recommande d'insérer une pareille règle dans la législation québécoise.

- Cynthia CHASSIGNEUX, « Regards sur la violation de données à caractère personnel », *Comm. et com. électronique*, décembre 2011, no. 23, p 10.
- Éric A. CAPRIOLLI, « Sécurité de l'information – Données à caractère personnel – Notification des violations de données à caractère personnel », *Comm. et com. électronique*, décembre 2011 no. 116, p 33.

## Internet et son impact sur les paradigmes de la régulation de l'audiovisuel

L'auteur démontre que les fondements sur lesquels repose la réglementation de l'audiovisuel sont radicalement modifiés par la banalisation d'Internet et son émergence comme principal canal de transmission des contenus. Sur Internet, l'audiovisuel se présente comme un univers dans lequel s'appliquent des régulations multiples qui s'entrelacent à l'image du réseau. Dans un tel environnement, chaque nœud du réseau est créateur ou réducteur de risques pour les autres. C'est à partir de ce phénomène que se structure désormais la réglementation de l'audiovisuel.

- Gilles De SAINT-EXUPÉRY, « L'impact d'Internet sur les paradigmes de la régulation de l'audiovisuel », [2011] 9 *CJLT* 51-72.

## La Commission européenne met en place une plateforme de règlement extrajudiciaire en ligne des conflits de consommation

La Commission européenne souhaite créer une plateforme européenne unique à laquelle les consommateurs effectuant des achats par Internet dans d'autres États membres pourront s'adresser pour régler en ligne tout litige de nature contractuelle dans un délai de trente jours. La Commission a modifié la directive relative au règlement extrajudiciaire des litiges de manière à garantir l'existence d'organes extrajudiciaires de qualité pour *tous* les litiges de nature contractuelle entre les consommateurs et les entreprises. La directive devra prévoir que les organes extrajudiciaires respectent des critères qualitatifs, tels que les principes de compétence, d'impartialité, de transparence, d'efficacité et d'équité, que les entreprises informent leurs clients de l'organe extrajudiciaire compétent en cas de litige de nature contractuelle et que les organes extrajudiciaires trouvent une solution aux litiges dans les quatre-vingt-dix jours.

De plus, le règlement relatif au règlement en ligne des litiges créera une plateforme européenne en ligne (« plateforme de RLL ») constituant pour les consommateurs et les entreprises un guichet unique de règlement en ligne des litiges liés à des achats effectués par Internet dans un autre État membre. Ce guichet unique européen transmettra automatiquement la réclamation du consommateur à l'organe extrajudiciaire national compétent et contribuera à ce qu'une solution soit apportée au litige dans les trente jours.

Les consommateurs auront accès à des moyens de recours efficaces et peu onéreux pour régler leurs litiges avec des professionnels, indépendamment du bien ou du service en cause, du mode d'achat (en ligne ou hors ligne) et du lieu d'achat dans l'Union (dans leur pays ou dans un autre). Les consommateurs en conflit avec des professionnels

d'autres États membres de l'Union pour des achats effectués en ligne pourront mener toute la procédure extrajudiciaire en ligne. Selon les estimations, les économies pour les consommateurs devraient atteindre environ 0,2 % du PIB de l'Union (22,5 milliards d'euros). Les entreprises, quant à elles, trouveront dans le règlement extrajudiciaire des litiges un moyen efficace de gérer leurs relations avec la clientèle et de soigner leur image de marque, ainsi que de s'épargner des procédures judiciaires coûteuses.

Le Parlement européen et le Conseil se sont engagés à adopter ces mesures, ce qui constitue l'une des actions prioritaires de l'Acte pour le marché unique, pour la fin de 2012. Ce train de mesures est également une action prévue par la Stratégie numérique pour l'Europe. Les États membres auront dix-huit mois à compter de l'adoption pour transposer la directive susmentionnée. Le territoire de l'Union devrait donc être couvert intégralement par des organes extrajudiciaires de qualité au second semestre de 2014. La plateforme européenne unique de règlement en ligne des litiges sera pleinement opérationnelle six mois après ce délai (au début de 2015), le temps de mettre en place ou à niveau les organes extrajudiciaires nécessaires à son fonctionnement.

- *Litiges entre les consommateurs et les entreprises: la Commission propose des mesures en faveur de moyens de recours rapides, simples et peu onéreux*, communiqué de presse, 29 novembre 2011.
- Le texte des mesures proposées.
- Questions et réponses sur les mesures proposées.
- Portail consacré au règlement extrajudiciaire des litiges.

## Sanction de la CNIL pour ne pas avoir anonymisé des décisions judiciaires publiques – France

Le 12 juillet 2011, la formation contentieuse de la CNIL a prononcé une injonction de cesser le traitement à l'encontre de l'association LEXEEK. Elle l'a également sanctionnée d'une amende de 10 000 euros. Cette association, qui numérise à la source de la jurisprudence afin de la rendre accessible à tous, publie sur son site Internet des décisions de justice publiques mais celles-ci n'étaient pas anonymisées. La Commission sanctionne ce qu'elle désigne comme une pratique attentatoire au respect de la vie privée des personnes et au « droit à l'oubli numérique ». L'auteure Agathe Lepage explique les raisonnements sous-tendant la décision de censure prononcée par la CNIL à l'égard de la diffusion de documents publics. La politique de la CNIL est présentée comme une « conciliation » entre le caractère public des décisions de justice et le « droit à l'oubli ». Mais l'auteure remarque que ce soi-disant « droit à l'oubli » ne correspond pas à un droit au sens strict. Ce droit correspond plutôt à une construction à laquelle prennent part divers éléments comme l'anonymisation ou le droit d'opposition.

- CNIL, délibération no. 2011-238, 12 juillet 2011.
- Agathe LEPAGE, « 'Droit à l'oubli' : sanction de la CNIL » *Comm. et com. électronique*, décembre 2011, no. 115, p. 31.

## Statut d'un comparateur de prix sur Internet – France

Dans sa décision du 15 décembre 2011, le Tribunal de Grand Instance de Paris a considéré que le comparateur de produits Shopping.com est un éditeur et non un hébergeur étant donné qu'il exerce un contrôle sur les fiches-produits réalisées par les annonceurs se trouvant sur son site.

Le tribunal s'est demandé si le site comparateur a connaissance des fiches-produits rédigées par les annonceurs avant leur diffusion et s'il est en mesure d'exercer un contrôle préalable sur ces contenus. Or, les conditions contractuelles du service proposé par Shopping.com lui réservent un droit non exclusif d'accéder au site annonceur et de reproduire, modifier ou adapter son contenu. Le jugement explique à cet égard que *« Dès lors que la société Shopping epinions international se reconnaît le droit de sélectionner les informations fournies par les fichiers-produits des annonceurs, de les adapter et de les modifier, elle ne limite pas ses prestations à celles d'un hébergeur mais elle joue un rôle actif dans le choix des informations qu'elle porte à la connaissance des internautes. »*

- *J.M. Weston c. Shopping Epinions International*, Tribunal de grande instance de Paris, 3ème chambre, 4ème section, 15 décembre 2011, *Legalis.net*.

## Un hébergeur est responsable des données personnelles introduites par des participants à un forum de discussion – France

Le demandeur Jean-Marc D. a fait assigner la société JFG Networks devant le juge des référés du tribunal de grande instance de Béziers. Il exposait que participant sous le pseudonyme Nemrod à des forums de discussion sur le site Overblog.com, géré par la société JFG Networks, il avait été victime d'internautes qui, révélant sa véritable identité, divulguaient des informations touchant sa vie privée et propageaient des calomnies et qu'il était intervenu en vain auprès de cette société pour en obtenir la suppression. Les informations relatives à l'identité du demandeur avaient été mises en ligne par des participants aux forums de discussion. Le tribunal a rejeté la demande du demandeur et avait affirmé qu'en dehors des cas manifestement illicites, l'hébergeur ne devait pas se substituer au juge.

Le 15 décembre 2011, la cour d'appel de Montpellier infirmait cette ordonnance de référé. Pour la cour, le site Oberblog effectue un traitement automatisé de données personnelles. La cour précise qu'*« en l'espèce, la société JFG Networks, dans le cadre de la prestation qu'elle offre à ceux qui utilisent ses services de mise en ligne d'un blog, collecte les informations contenues dans les billets, les conserve tout en les organisant à la fois de façon ante-chronologique (les plus récentes étant mis en avant) et de façon à les regrouper ou agglomérer au fil du temps sur un thème donné, tout en se réservant, ainsi que cela résulte de ses propres "Conditions générales d'utilisation" (produites aux débats), la faculté d'en suspendre la transmission ou diffusion, en cas d'abus de la part des utilisateurs. Par ailleurs, ainsi que cela résulte du constat d'huissier, la société JFG Networks est amenée à traiter des données caractère personnel dès lors que les informations ainsi stockées, organisées et diffusées, sont relatives à une personne physique parfaitement identifiée par ses nom, prénom et lieu de résidence. »*. Le participant intervenant sous pseudonyme sur le forum de discussion était ainsi en droit à demander à l'hébergeur la suppression de ses noms et prénoms.

- *Jean-Marc D. / JFG Networks*, Cour d'appel de Montpellier, 5ème chambre, section A, Arrêt du 15 décembre 2011, *Legalis.net.*

## À signaler

- « Google Suggest : la cour de Paris confirme la condamnation au fond », *Legalis.net*, 27 décembre 2011.

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 Professor Robert Currie, Director of the Law & Technology Institute, at robert.currie@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 le professeur Robert Currie à l'adresse suivante : robert.currie@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.