

# IT.CAN NEWSLETTER/BULLETIN

Canadian IT Law Association

[www.it-can.ca](http://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 la Chaire en droit des technologies de l'information et du commerce électronique L.R. Wilson de la Faculté de droit de l'Université de Montréal ont rédigé la seconde partie du présent bulletin.

## Part 1

### Disclosure of Website Subscriber Information

The British Columbia Supreme Court has ordered a website to disclose the IP address, name, and any other identifying information they have concerning one of their users with its decision in [Pierce v. Canjex Publishing Ltd.](#) The petitioner, Pierce, was a stock promoter who had been subject to a cease and desist order by the Securities and Exchange Commission in the United States, as well as order to repay a large sum of money. Pierce had not appeared that the Securities and Exchange Commission hearing because of his fear that he would be arrested by US Federal authorities in connection with another matter. This activity was the subject of new item on a website, Stockwatch.com (operated by the respondent Canjex Publishing Ltd.) which is a website for news, quotes, trades and market information for companies listed on the major North American stock exchanges. Stockwatch.com has a reader comments section, in which users can post comments with regard to the news items.

A number of postings, many of them defamatory, were made about Pierce on Stockwatch.com between 2008 and 2011, including one in December 2010 by a user named "halcrow". Pierce obtained a *Norwich* Order requiring Stockwatch.com to disclose the IP addresses associated with all of those

postings. Stockwatch.com removed the postings in January 2011<sup>1</sup> and advised Pierce that it had "restricted posting privileges to paid subscribers". On receipt of a court order it disclosed the requested IP addresses to Pierce, who then followed up with the appropriate ISPs. In the case of halcrow the ISP was TELUS, who informed Pierce that they did not generate a subscriber log and therefore had no information which would help identify halcrow.

Subsequently, in March 2011, a posting under the username "halcrow" appeared again on Stockwatch.com. Although this posting had nothing to do with Pierce, it occurred after Stockwatch.com had indicated that it had restricted posting to paid subscribers. Pierce argued, therefore, that Stockwatch.com would have identifying information including name, address, contact information and payment information for the "halcrow" account. Accordingly he sought a further *Norwich* Order requiring Stockwatch.com to disclose that information.

The court considered the criteria for issuing a *Norwich* Order, which are:

- (a) the plaintiff must show that a *bona fide* claim exists against the unknown wrongdoer;
- (b) the defendant must establish that the information is required in order to commence an action against the unknown wrongdoer, that is, the plaintiff must establish that disclosure will facilitate rectification of the wrong;<sup>2</sup>
- (c) the defendant must be the only practicable source of the information;
- (d) there is no immunity from disclosure;
- (e) the plaintiff must establish a relationship with the defendant in which the defendant was mixed up in the wrongdoing. Without connoting impropriety, this requires some active involvement in the transactions underlying the intended cause of action;

(f) disclosure by the defendant will not cause the defendant irreparable harm; and

(g) the interest of justice favour granting the relief.

Stockwatch.com argued that Pierce could not meet several of these criteria.

First, it argued Pierce could not show a *bona fide* claim (or *prima facie* case, which it argued was the proper test) of defamation against the halcrow who posted in March 2011: the March posting was not defamatory, and there was no proof that the same person had posted the defamatory comment in December 2010. The court rejected this argument, holding that:

[19] I am satisfied that a strong inference can be drawn that the user who commented on Stockwatch under the name of “halcrow” and made the Defamatory Comment is the same “halcrow” who registered an account with Stockwatch after their change of policy. Although neither the respondent nor Halcrow are required to lead evidence to disprove this, they are the only parties that could have displaced this inference by the respondent notifying “halcrow” and allowing him or her to make submissions...

Second, Stockwatch.com argued that they were not the only practicable source of the information: Pierce could have looked in halcrow’s posts for personal information, and tried to cross-reference pseudonyms using private investigators. The court rejected this suggestion as well, holding that Pierce had taken other reasonable steps, and was not required to resort to the expense of a private investigator when the information was available from Stockwatch.com.

The court also held that Stockwatch.com was sufficiently “mixed up in the wrongdoing” because it provided the internet service used by halcrow and was an innocent but involved third party, not a mere witness.

Finally, the court concluded that the interests of justice favoured disclosure. Stockwatch.com’s privacy policy stated that it would disclose information if required to do so by law. Further, the website contained a link to another website which contained information about Canadian libel law. A reasonable user would therefore have contemplated, the court

held, that his or her identity might be disclosed if he or she engaged in defamatory activity on the website.

- 1 The decision gives the date as January 28 2010, but given the chronology it seems it must have been 2011.
- 2 Both this case and the source it cites say “defendant” at the start of this criterion, but it seems that “plaintiff” must be intended.

## Non-Disclosure of Video Evidence

The accused in *R. v. Banford* had been charged with impaired driving and driving with a blood alcohol level over .08%. He had been subject to a breathalyser test at the detachment, and the entire interaction would have been videotaped by the surveillance video system in place. The accused requested disclosure of those videotapes three weeks after charges were laid. By the time the Crown attempted to obtain them from the police, the tapes had been destroyed in accordance with a policy which required them to be held for only 55 days. The accused sought a stay of proceedings based on this destruction of evidence which was granted.

On appeal the stay was set aside. The Court of Queen’s Bench held that the lost evidence was not important to the case. Any observations which justified the breathalyser demand had been made at the roadside, not in the detachment. The Crown had stayed the impaired driving charge, making any issue of whether the accused appeared to be impaired irrelevant. Accordingly the Crown’s appeal was granted. However, the Court of Queen’s Bench added:

[18] In so holding, I am in no way condoning the practice of the RCMP in maintaining a retention period of only 55 days. Although the destruction was part of normal procedure, I agree with the trial judge that, given advances in technology, common sense dictates that the police must reconsider their retention period policy in order to fulfill their disclosure obligations...

## CRTC Policy on Usage-based Billing

The Canadian Radio-television and Telecommunications Commission (CRTC) has returned to the issue of usage-based billing for internet services with new regulatory policies issued on [November 15, 2011](#). As noted in the IT.Can newsletters of [January 26, 2011](#) and [February 9, 2011](#), the CRTC had initially approved a plan for usage-based billing relating to the purchase of bandwidth by smaller ISPs from larger providers for resale to consumers: the effect of the plan would have effectively required those smaller ISPs to sell to consumers on a usage-based model, and so would have negated their ability to offer unlimited use plans. Following a considerable public outcry (and negative comment from the Prime Minister and the Industry Minister) the CRTC suspended that decision pending further review. After additional consultation with industry and the public, it has now issued this revised policy.

The new policy does not completely abandon a usage-based approach, but it does provide greater flexibility to smaller ISPs in reselling the bandwidth to consumers. Smaller ISPs will be able to buy total bandwidth on a wholesale basis and then re-sell it to consumers on whatever pricing plan they choose: the smaller ISPs will be responsible for estimating their own need and dividing it as necessary, but on this policy would be able to offer unlimited usage plans.

In fact two arrangements between larger and smaller ISPs are provided for in the new policy, described by the CRTC as follows:

### *a) Capacity-based model*

The first option is known as the capacity-based model, which contains three separate components:

- a monthly access rate for each of the independent ISP's retail customers
- a monthly capacity charge, offered in increments of 100 megabits per second, and
- any applicable ancillary charges, such a monthly interface charge and associated service charges.

This model allows large telephone and cable companies to charge separately for access and usage, but at the same time recognizes that independent ISPs are in the best position to forecast their needs. By determining in advance the bandwidth they need, independent ISPs assume the risk and responsibility associated with planning and managing the impact their customers will have on the large companies' networks.

### *b) Flat-rate model*

The second option is the existing flat-rate model, which contains two separate components:

- a monthly access rate for each of the independent ISP's retail customers, and
- any applicable ancillary charges, such a monthly interface charge and associated service charges.

This model allows large telephone and cable companies to recover their costs by charging independent ISPs a flat monthly fee, regardless of how much bandwidth their customers use.

## Quebec court finds litigant in contempt for destroying evidence on a computer

The Superior Court in Quebec recently found a litigant to be in contempt of court and levied a fine, plus experts' costs, following the deletion of various information from a computer. In [World Assurances Inc. c. Al Iman](#), the defendant was accused of violating a court order related to the surrender of a laptop computer. Previously, the Court had issued an order to the defendant, which read as follows:

“Orders the Defendant to remit the laptop more fully described in Exhibit P-15 and bearing serial number 739270508 QT to the bailiffs Paquette and Associates, as guardian with the hard disc inside said laptop unaltered for future reference and analysis before October 29 at 5 PM;”

The Court was satisfied by testimony from a forensic analyst that prior to the surrender of the computer, the user of the computer searched for information on the internet on how to securely delete information from a Macintosh computer hard-drive. Subsequently,

---

the same user attempted to “scrub”, made a mistake and tried again and then deleted two pre-existing user accounts. The court was satisfied beyond a reasonable doubt that it was the Defendant who did this. The deletion was successful, so the Plaintiff was unable to determine what had actually been deleted. Nevertheless, it was in clear violation of the Court’s order that the laptop and its hard disc be returned “unaltered for future reference and analysis.”

The defendant was found to be in contempt and was fined \$10,500 plus the costs of the forensic expert.

## **The computer ate my financial disclosure**

In the course of a pair of heated family law proceedings, two of the parties have been castigated for a failure to provide financial disclosure despite the fact that the requisite information was allegedly lost in a computer crash. In *Spettigue v. Varcoe*, Mr. and Mrs. Spettigue had been ordered to provide financial records for their business. They failed to do so and filed affidavit evidence that both a laptop computer and a desktop computer had crashed, causing the loss of the data. What was material to the Ontario Superior Court of Justice was that the crash occurred after the deadline for providing the information. Had they been timely in the first place, the alleged crash would have been subsequent to the disclosure and would not have made any difference. The Court considered remedies for this failure and decided against striking out their pleadings, but warned that further problems would result in such a sanction:

However, Mr. and Mrs. Spettigue have made some last minute efforts to provide some of the financial information and documents which they are obliged to produce. With respect to the outstanding items, Mr. and Mrs. Spettigue provided evidence that they are now taking reasonable steps to address the problems. Accordingly, I decline to make an order striking their pleadings. I do so with a strong warning to Mr. and Mrs. Spettigue that any further non-compliance or inordinate delay in complying with court orders will not be tolerated by this court, and could result in a different outcome if further Motions to strike their claims are brought in the future.



## 2<sup>ème</sup> partie

### Ordonnance interdisant la diffusion du nom, de l'image ou de vidéos

La demanderesse requiert une ordonnance d'injonction interlocutoire provisoire pour empêcher le défendeur de diffuser entre autres certaines photographies où elle apparaît nue, que ce dernier aurait prises dans le cadre d'un processus artistique, étant convenu que ces photographies devaient demeurer privées et confidentielles. Le défendeur a transmis des courriels à la demanderesse demandant de la rencontrer, à défaut de quoi il menace de diffuser sur Facebook un montage vidéo l'impliquant personnellement. Vu son refus, il aurait diffusé ce montage vidéo et la demanderesse craint qu'il fasse de même avec les photographies.

Étant donné son statut d'enseignante dans un établissement scolaire, la diffusion de ces photographies est susceptible de lui causer un préjudice sérieux ou irréparable. Son employeur est déjà en possession de quatre de ces photographies et un de ses représentants a rencontré la demanderesse, pour l'informer de la problématique que cela pourrait causer quant à sa réputation, celle de l'institution d'enseignement et à la poursuite de sa carrière comme enseignante. La balance des inconvénients penche en faveur de la demanderesse qui pourrait subir un préjudice sérieux tandis qu'il n'apparaît pas que le défendeur subira un préjudice de se voir interdire la diffusion des photographies de la demanderesse. De plus, le risque de diffusion immédiate des photographies justifie de rendre l'ordonnance avant la signification de la requête.

- *Plourde c. Mendonça*, 2011 QCCS 5500 (CanLII), 4 octobre 2011.

### Infraction d'avoir en main un appareil avec une « fonction téléphonique »

Le défendeur est accusé d'avoir conduit un véhicule automobile en faisant usage d'un appareil tenu en main muni d'une fonction téléphonique, commettant ainsi l'infraction prévue à l'article 439.1 du *Code*

*de sécurité routière*. Il est mis en preuve que le défendeur avait un appareil enregistreur à cassette entre les mains. Le tribunal conclut que la défense du défendeur concernant le mode de fonctionnement de l'entreprise et de l'utilisation de l'enregistreuse avec l'adresse du chantier pour qu'il puisse trouver son chemin et se rendre ainsi chez son client pour y effectuer les travaux est plausible et sème un doute dans son esprit. Il prononce l'acquiescement.

- *Notre-Dame-de-Lourdes (Municipalité) c. Dumas-Gagnon*, 2011 CanLII 70294 (QC CM), 21 septembre 2011.

### Outrage au tribunal suite à la transgression d'une ordonnance interdisant de modifier les données

Une ordonnance enjoignait le défendeur à remettre « unaltered » un ordinateur appartenant à son employeur. L'adjectif « unaltered » doit être compris dans son sens ordinaire impliquant de ne pas modifier ou changer quoi que ce soit dans l'ordinateur. La preuve a clairement établi qu'il y a eu des modifications. Bien plus, des données ont été effacées. Compte tenu notamment de l'importance grandissante des preuves électroniques devant les tribunaux, il est important de prononcer une sentence pour outrage au tribunal qui aura un effet dissuasif. Le tribunal condamne le défendeur à une amende 10,500 \$ en plus des frais d'expertise et autres dépens.

- *World Assurances Inc. c. Al Iman*, 2011 QCCS 5792 (CanLII), 3 novembre 2011.

### Congédiement suite à l'usurpation d'un compte Facebook

La plaignante, qui est enceinte, s'oppose à son congédiement, se prévalant du recours prévu par l'article 122 de la *Loi sur les normes du travail*. La Commission des relations du travail conclut que la présomption selon laquelle le congédiement fait suite à l'état de la plaignante est repoussée. La plaignante a admis avoir utilisé un ordinateur pour usurper l'identité d'une collègue de travail, accédant

au compte Facebook de cette dernière et y inscrivant des propos disgracieux. N'eut été de cette usurpation d'identité sur Facebook, la Commission juge qu'il est clair que l'emploi de la plaignante n'aurait pas pris fin.

- *Durocher-Lalonde c. 9096-0469 Québec inc.*, Commission des relations de travail, (C.R.T., 2011-10-26), 2011 QCCRT 0490, SOQUIJ AZ-50804049.

## Le filtrage et l'affaire SABAM devant la Cour de justice de l'Union Européenne

L'auteur examine les enjeux de deux affaires qui sont devant la Cour de Justice de l'Union Européenne. Dans ces affaires impliquant la Société Belge des Auteurs, Compositeurs et Editeurs (SABAM), il est demandé l'instauration du filtrage et du blocage des communications électroniques. Selon l'auteur, si la Cour autorisait de telles mesures, sa décision aurait une portée considérable pour la régulation d'Internet. En raison des contraintes associées à leur fonctionnement, le filtrage et le blocage préconisés emporteraient de nombreux effets négatifs sur les plans juridique, économique et social.

- Cédric MANARA, *Bloquer le filtrage ! Une approche critique des affaires SABAM*, Juriscom.net, 4 novembre 2011.

## Politiques d'« Open Data » – France

Sous-titrée « Les données publiques au service de l'innovation et de la transparence », cette étude dresse un état des lieux de l'ouverture des données publiques en France, et du potentiel de leur réutilisation. L'administration publique collecte et produit un champ très vaste de données, du budget national aux mesures de la qualité de l'air. Pour les auteurs, ouvrir l'accès le plus large aux informations publiques (« l'Open Data »), c'est améliorer la transparence de l'État et de ses institutions, éclairer le débat démocratique, et rapprocher la puissance publique des citoyens. Favoriser leur réutilisation par les entrepreneurs pour leur inventer de nouvelles applications, c'est encourager l'innovation et les secteurs stratégiques, de l'économie numérique au

développement durable. Seize propositions concluent le rapport, remis au Ministre de l'Industrie, de l'Énergie et de l'Économie numérique en juillet 2011.

- Romain LACOMBE, Pierre-Henri BERLIN, François VAUGLIN et Alice VIEILLEFOSSE, *Pour une politique ambitieuse des données publiques – Les données publiques au service de l'innovation et de la transparence*, Juillet 2011.
- Emmanuelle BARTHE, *Données publiques: 16 propositions pour une politique nationale ambitieuse des données publiques-Un rapport audacieux*, 29 juillet 2011.

## Un moteur de recherche ayant le contrôle des mots clés proposés ne peut prétendre à un statut d'intermédiaire passif – France

La cour d'appel de Paris a rendu une décision condamnant l'interface de recherche Lo.st pour avoir tenu un rôle actif dans l'apparition des marques notoires de la SNCF sur sa page d'accueil. À des requêtes telles que « voyages-sncf .com » ou « voyage-sncf » ou « tgv », le moteur de recherche affichait des liens commerciaux sans relation avec la SNCF. Des constats produits par la SNCF démontraient que les résultats obtenus par Lo.st diffèrent de ceux obtenus par Google pour une même requête. De ce constat, la cour infère que « la société Eorezo dans le cadre du programme AdSense a mis en place son propre système d'annonces commerciales qui s'affichent avant les résultats naturels de Google tout en faisant croire qu'ils proviennent du moteur de recherche Google ». Elle est donc empêchée de prétendre au statut d'hébergeur puisqu'elle joue un rôle actif ayant connaissance et le contrôle des données stockées. La cour ajoute que l'interface de recherche « ne s'est pas bornée à stocker des informations de nature publicitaire fournies par les annonceurs mais elle a également de façon délibérée inséré dans sa page d'accueil le mot-clé SNCF lequel dirigeait l'internaute vers des liens concurrents ». L'entreprise offrait aux annonceurs des mots clés évoquant des marques notoires de la SNCF à partir d'un système de suggestion qu'elle proposait à ses clients.

- *Tuto4PC.com (anciennement Eorezo) c. SNCF*, Cour d'appel de Paris, Pôle 5, Chambre 2, Arrêt du 28 octobre 2011.
- « Liens commerciaux : Lo.st condamné pour son rôle actif dans l'apparition des marques de la SNCF », *Legalis.net*, 4 novembre 2011.

le prestataire d'un service du commerce électronique soit soumis dans l'État membre d'accueil à des exigences plus strictes que celles prévues par le droit de l'État membre dans lequel le prestataire est établi.

- *eDate Advertising GmbH c. X et Olivier Martinez, Robert Martinez c. MGN Limited*, arrêt du 25 octobre 2011, affaires C-509/09 et C-161/10.

## Lieu d'introduction du recours des victimes d'atteintes aux droits de la personnalité commises via Internet

Dans un arrêt rendu suite à une demande de décision préjudicielle, la Cour de justice de l'Union européenne a statué que les victimes d'atteintes aux droits de la personnalité, commises via Internet, peuvent saisir les juridictions de leur État membre de résidence au titre de l'intégralité du dommage causé. Toutefois, le gestionnaire d'un site Internet relevant de la directive sur le commerce électronique ne peut être soumis, dans cet État, à des exigences plus strictes que celles prévues par le droit de l'État membre de son établissement

Dans son arrêt, la Cour constate que la mise en ligne de contenus sur Internet se distingue de la diffusion territorialisée d'un imprimé en ce que ceux-ci peuvent être consultés instantanément par un nombre indéfini d'internautes partout dans le monde. Ainsi, d'une part, la diffusion universelle est susceptible d'augmenter la gravité des atteintes aux droits de la personnalité et, d'autre part, de rendre extrêmement difficile la localisation des lieux de la matérialisation du dommage résultant de ces atteintes. Dans ces circonstances, – étant donné que l'impact d'un contenu mis en ligne sur les droits de la personnalité d'une personne peut être le mieux apprécié par la juridiction du lieu où la victime a le centre de ses intérêts –, la Cour désigne cette juridiction comme étant celle compétente au titre de l'intégralité des dommages causés sur le territoire de l'Union européenne. Dans ce contexte, la Cour précise que l'endroit où une personne a le centre de ses intérêts correspond en général à sa résidence habituelle.

Enfin, en interprétant la directive sur le commerce électronique, la Cour juge que le principe de la libre prestation de services s'oppose, en principe, à ce que

---

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](mailto:robert.currie@dal.ca) if they relate to Part 1 or Pierre Trudel at [pierre.trudel@umontreal.ca](mailto:pierre.trudel@umontreal.ca) if they relate to Part 2.

Disclaimer: The IT.Can Newsletter is intended to provide readers with notice of certain new developments and issues of legal significance. It is not intended to be a complete statement of the law, nor is it intended to provide legal advice. No person should act or rely upon the information in the IT.Can Newsletter without seeking specific legal advice.

Copyright 2011 by Robert Currie, Stephen Coughlan, David Fraser, Pierre Trudel and France Abran. Members of IT.Can may circulate this newsletter within their organizations. All other copying, reposting or republishing of this newsletter, in whole or in part, electronically or in print, is prohibited without express written permission.

Le présent bulletin se veut un outil d'information à l'intention des membres d'IT.Can qui souhaitent être renseignés sur les développements du droit canadien et du droit international qui pourraient avoir une incidence sur le Canada. Le comité exécutif et le conseil d'administration de l'Association s'en serviront également pour vous tenir au courant des nouvelles concernant l'Association, telles que les conférences à venir.

Pour tous commentaires ou toutes suggestions concernant la première partie du présent bulletin, veuillez contacter le professeur Robert Currie à l'adresse suivante : [robert.currie@dal.ca](mailto:robert.currie@dal.ca) ou en ce qui concerne la deuxième partie, veuillez contacter Pierre Trudel à [pierre.trudel@umontreal.ca](mailto: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.

© Robert Currie, Stephen Coughlan, David Fraser, Pierre Trudel et France Abran 2011. Les membres d'IT.Can ont l'autorisation de distribuer ce bulletin au sein de leur organisation. Il est autrement interdit de le copier ou de l'afficher ou de le publier de nouveau, en tout ou en partie, en format électronique ou papier, sans en avoir obtenu par écrit l'autorisation expresse.