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

May 7, 2010/7 mai 2010

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

Internet Defamation

In *Warman v. Fournier et al.*, Justices Kent, Heeney and Wilton-Siegel of the Ontario Divisional Court heard an appeal of a lower court decision that ordered the administrators and moderators of an internet message board to disclose the e-mail addresses and IP addresses of eight anonymous posters. The underlying proceeding is a defamation action by Richard Warman against the defendants and the eight "John Does" with regard to various posts on the "Free Dominion" message board, all of which were made using pseudonyms. Warman had brought a motion compelling the defendants to disclose the identifying information with regard to the John Does so that they could be served with the statement of claim. The motions judge, Kershman J., had ruled that Warman did not need to demonstrate a *prima facie* case of defamation via affidavit to obtain the order, as had been ruled in cases brought directly against third-party ISPs; rather, Warman had demonstrated that the documents in question were relevant and not privileged, and was thus entitled to disclosure. He also held that an individual has no reasonable expectation of privacy in "the IP address associated with an individual's e-mail address" (para. 13, citing the 2009 decision of *R. v. Wilson*, no hyperlink available), and that in the context of "an anti-hate speech advocate and a controversial website," there was significant public interest in disclosure.

Writing for the court on the appeal, Wilton-Siegel J. framed the issue as:

> whether there are *Charter* values that the Court must take into account in considering the Respondent's request for disclosure and, if so, the manner in which the Court is to balance such *Charter* protected interests against the public interest in promoting the administration of justice by providing the Respondent with full access to the information which will enable him to pursue his defamation action against the alleged wrongdoers (para. 14).

The Court acknowledged that the case involved a conflict between two constitutional values: freedom of expression, which is particularly important in defamation matters, and the right to informational privacy. The right to privacy in this case was relevant to both parties, as the plaintiff's right to good reputation is linked to his privacy right, while the John Does had an arguable expectation of privacy when they deliberately chose to post anonymously—"consistent with an implicit understanding of citizens that, to some degree at least, their identities will be protected when they use the internet anonymously" (para. 20). Under the law the court was bound to apply *Charter* values even to civil cases and in particular to the discovery process, where, "disclosure cannot be automatic where *Charter* interests are engaged. On the other hand, to prevent the abusive use of the internet, disclosure also cannot be unreasonably withheld even if *Charter* interests are engaged" (para. 24).

While there was no caselaw for guidance on the relevant considerations of this kind of disclosure in an ongoing case, the court held that the considerations that apply in *Norwich* pre-trial disclosure proceedings were analogous. That caselaw indicates that where privacy interests are involved, disclosure is not automatic but rather the plaintiff must demonstrate some kind of case (*bona fide* or *prima facie*, depending upon context) and the interest in disclosure must be balanced against

privacy interests. The court was not persuaded that there was any significant difference between the *Norwich* caselaw, which involved disclosing information about third parties, and where a party defendant was involved:

> this is not a meaningful distinction for present purposes. As has been pointed out, a third party can be made a defendant for the price of issuing a statement of claim. Moreover, the fact that the motion engages the important *Charter* value of freedom of expression as well as the right to privacy, heightens the need to have regard to considerations beyond the traditional concerns of relevance and privilege (para. 32).

Nor did the deemed/implied undertaking rule provide sufficient protection to justify automatic disclosure, since this would allow plaintiffs to bring unmeritorious claims simply to obtain the identities of anonymous internet posters and thus have an unwarranted chilling effect on freedom of speech. Accordingly, the motions judge was required to consider: (1) whether the unknown alleged wrongdoer could have a reasonable expectation of anonymity in the particular circumstances; (2) whether the Respondent has established a *prima facie* case against the unknown alleged wrongdoer and is acting in good faith; (3) whether the Respondent has taken reasonable steps to identify the anonymous party and has been unable to do so; and (4) whether the public interests favouring disclosure outweigh the legitimate interests of freedom of expression and right to privacy of the persons sought to be identified if the disclosure is ordered (para. 34).

The court finally noted that a "more robust" standard was required in order to address the threat to freedom of expression and properly balance all privacy interests, given that this was a case involving political discussion that could attract a defence of fair comment. Accordingly, the motions judge's decision that the plaintiff did not have to adduce a *prima facie* case of defamation before obtaining disclosure was held to be an error of law, and the motion was remitted to a different motions judge for reconsideration based on the principles laid out by the Divisional Court.

In the similar Nova Scotia case of *Mosher v. Coast Publishing Ltd.* (reported in the last issue of this newsletter), the *Globe & Mail* has reported that counsel for the Chief and Deputy Fire Chief of Halifax Regional Fire Services has received identifying information regarding individuals alleged to have made anonymous defamatory comments. A Halifax chambers judge had previously ordered the online newspaper on which the comments were made, as well as Google Inc., to provide IP addresses for the individuals. A second (unreported) order was obtained requiring two Halifax ISPs to provide name and address information for the individuals, and all information was expected to be received in short order. Counsel for the Chief and Deputy Chief remarked that her clients now have one year to consider whether they will bring defamation proceedings.

Audio-recording of Medical Examinations

The Ontario Court of Appeal recently reconsidered its rule on whether medical examinations by defence experts in insurance claims should presumptively be recorded. The current rule, dating from *Bellamy v. Johnson* (1992), 8 O.R. (3d) 591 (C.A.) is that there is no such presumption: the decision in *Adams v. Cook* declined to change that situation at present, though there are suggestions in the case that the issue is not fully settled.

The plaintiff in *Adams* had sought an order to have the examination by the defendant's medical expert audio recorded, on the basis that such examinations were typically an attempt to gain admissions against interest in the guise of a medical examination. Audio-recording was intended as a way of avoiding that situation. No specific allegations were made against the particular doctor in this case; rather, the question was said to be one of systemic bias on the part of defence experts. In Bellamy, the Ontario Court of Appeal had decided that audio recording should only be ordered based on the facts of a particular case, and so suggesting that a claim of systemic bias could ground the order would amount to a change in approach.

The majority of the Court of Appeal (in a decision rendered by a five-person panel) rejected the application on the basis that the record in the case was not sufficient to demonstrate that a change in practice was warranted. They acknowledged that

arguments of a general nature could be made, but held that no general conclusions could be drawn from the limited evidence presented. They held that it was a matter for the Civil Rules Committee to consider.

Justice Lang, dissenting, would have held that the rule should be changed, and that evidence of a case-specific bias should not be needed. He held that for several reasons, a defence medical normally should be recorded unless there was some reason not to. He based this on the nature of the relationship between the plaintiff and the examiner, the changes in approach to expert reports, the advances in technology, and the advantages to be gained by an accurate record. Of most interest are his comments on changing technology. On that issue, the dissent would have brought in a presumption in favour of recording based on the following:

> 65 Second, the technology has changed dramatically. In *Bellamy*, the proposed examiner objected to a recording condition on the basis that the technology would physically interfere with the flow of the examination. In his concurring reasons, Doherty J.A. rejected this as a significant concern, noting at p. 597 that "tape-recorders are compact and tapes can be made for well over an hour without any interruption." Of course, in 2010, high quality digital recording is even less obtrusive, less costly, and more user-friendly than older technology. At the same time, it enables recordings that are more easily copied and transferred and are sufficiently unlimited in duration to meet the requisite purpose. Once activated, a device need not be touched again until the end of the recording session, and the digital files are easy to manage once completed. Any technology-based concerns voiced in 1992, even if valid then, are moot today.
>
> 66 Finally, we as a society have become inured to being recorded. Proceedings at the Court of Appeal for Ontario and the Supreme Court of Canada are now digitally recorded. Our conversations are recorded every time we call a major company for customer support. 911 calls are recorded, as are police interviews. Our movements at ATM machines, in institutional buildings, and many other locations, are routinely videotaped. There are police cameras posted at problematic intersections in our cities. Incidents and events are now captured on cell phone cameras and distributed on the internet within minutes. For security and other reasons, society finds these recordings largely acceptable. As Armstrong J.A. wryly put it at para. 28, "given this electronic world in which we now live, it is perhaps at least questionable whether the presence of a small recording device is likely to have any adverse affect on a medical specialist's examination."

Electronic Disclosure and Unreasonable Delay

The Newfoundland Court of Appeal has upheld a stay of proceedings based on a violation of the right to a trial within a reasonable time in *R. v. Taylor*. The delay, which was not acceptably explained, was more than 30 months on the charges of conspiracy to traffic in narcotics. The delays were partly due to problems with a transcript and scheduling, but the Court of Appeal noted that a significant portion of the delay was attributable to the decision to use electronic disclosure of documents rather than use paper copies. There were problems with the software, the material was incomplete and disorganized, and the material was frequently provided on or just before hearing dates, necessitating adjournments. The case was not close to the line, and a stay was warranted.

Unauthorized Access to Email

The trial judge rejected an application for a mistrial in *P.F. v. P.T.*, where the defendant alleged after the trial was over that the plaintiff had gained access to his email account and therefore had been privy to all of his trial preparation communications with his lawyer. The plaintiff acknowledged that she had gained access after the trial but the trial judge held that the evidence did not establish that she had had access prior to that.

Part of the evidence was that the plaintiff was in possession of emails sent by the defendant's daughter: the trial judge noted that this could also be accounted for by the daughter having given these emails to the plaintiff, or by the plaintiff having access to the daughter's computer.

There was evidence from a forensic computer expert, showing that the defendant's computer had on three occasions been used to log in to the TELUS email web page at a time when the computer was with the daughter and the daughter was with the plaintiff. The usernames logged in to the computer at these times were those of either the son or the daughter. The trial judge held that this only showed that some person was accessing email: it could have been the son or daughter accessing their own email accounts, or the plaintiff accessing her own email while logged in to the computer under one of the children's usernames. It did not show that the plaintiff was accessing the defendant's email. Accordingly the application for a mistrial was dismissed.

2ième partie

Sentence pour piratage de films

Il s'agit de déterminer la peine qui doit être imposée à un accusé ayant plaidé coupable d'avoir mis en circulation un exemplaire contrefait d'une œuvre protégée, contrairement à la *Loi sur le droit d'auteur,* et d'avoir enregistré une œuvre cinématographique sans le consentement du gérant du cinéma, en contravention au *Code Criminel*. L'accusé se présentait dans des salles de cinéma de Montréal et, à l'aide d'un dispositif d'enregistrement sophistiqué, procédait au piratage de films, qu'il mettait ensuite en circulation via Internet.

Quoique l'accusé ne tirait aucun profit important de ce stratagème, il appert que le piratage de films entraîne des pertes de plusieurs milliers de dollars à l'industrie du cinéma et que les coûts afférents à la lutte contre ces crimes sont appréciables. Une peine de 2 mois et demie paraît ainsi appropriée mais compte tenu de la détention préventive, l'accusé purgera une sentence de 7 jours et une probation de deux ans avec conditions.

- *R. c. Adam*, 500-73-002897-078, 16 mars 2010, Cour du Québec (Chambre criminelle et pénale), EYB 2010-171022.

Portée d'un communiqué publié sur Internet

Dans le contexte d'un recours en diffamation résultant de la publication de communiqués sur Internet, le tribunal estime que « La preuve révèle que ce communiqué a été publié sur CNW, un fil de presse qui reçoit une large couverture, qui est repris par d'autres agences et dont les communiqués se retrouvent sur Internet. De plus, CNW est largement consulté par ceux qui oeuvrent dans les médias et par les professionnels des affaires et de la finance. La Presse et The Gazette ont d'ailleurs communiqué avec Brassard après la publication de son communiqué, l'ont interviewé et ont donné une couverture à la poursuite dans leurs publications. Lorsqu'on tape le mot «Clemex» sur un site de recherche comme Google, le communiqué de Brassard apparaît encore aujourd'hui immédiatement dans les dix ou quinze premières entrées que l'on obtient. L'impact de ce communiqué a été et est encore très important. » Le tribunal ne retient pas l'argument selon lequel il incomberait au demandeur d'exiger le retrait de l'information sur Internet auprès des entités qui ont affiché les propos sur leurs sites. « L'obligation de minimiser les dommages ne va pas jusqu'à tout faire pour empêcher qu'ils soient causés puis, une fois le mal fait, de les réparer à la place de leur auteur. »

- *Brassard c. Forget*, 2010 QCCS 1530 (CanLII), 15 avril 2010.

Code source et sources codifiées : pour une cyberjustice québécoise ouverte et accessible

Dans cet article, l'auteur offre un survol des fonctionnalités offertes par les systèmes de dépôt électronique de la Cour fédérale et de la Cour canadienne de l'impôt afin de dégager les avantages et inconvénients de chacune des technologies proposées.

Cet exercice s'inscrit dans une réflexion plus large sur les conséquences de la migration progressive de certaines juridictions vers le dépôt électronique. Si cette tentative de moderniser le processus judiciaire se veut bénéfique, il demeure qu'un changement technologique d'une telle importance n'est pas sans risques et sans incidences sur les us et coutumes de l'appareil judiciaire.

L'auteur s'interroge sur la pratique de certains tribunaux judiciaires de développer en silo des solutions d'informatisation du processus de gestion des dossiers de la Cour. L'absence de compatibilité des systèmes et le repli vers des modèles propriétaires sont causes de soucis. Qui plus est, en confiant le développement de ces systèmes à des firmes qui en conservent la propriété du code source, ils contribuent à une certaine privatisation du processus rendant la mise en réseau de l'appareil judiciaire d'autant plus difficile. Or, dans la mesure où les systèmes de différents tribunaux seront appelés à communiquer et échanger des données, l'adoption de solutions technologiques compatibles et ouvertes est de mise.

Une autre problématique réside dans l'apparente incapacité du législateur de suivre l'évolution vers la virtualisation du processus judiciaire. Le changement technologique impose, dans certains cas, un changement conceptuel difficilement compatible avec la législation applicable. Ce constat implique la nécessité d'un questionnement plus profond sur la pertinence d'adapter le droit à la technologie ou encore la technologie au droit afin d'assurer une coexistence cohérente et effective de ces deux univers.

- Nicolas VERMEYS, « Code source et sources codifiées : pour une cyberjustice québécoise ouverte et accessible », *Lex Electronica*, vol. 14, no. 3.

Nouvelles règles de concurrence pour la distribution des biens et des services reflétant les contextes en ligne – Commission européenne

La Commission européenne a adopté un règlement qui exempte certaines catégories d'accords conclus entre les producteurs et les distributeurs pour la vente de produits et de services. Ce règlement et les lignes directrices qui l'accompagnent tiennent compte du fait qu'Internet est devenu ces dix dernières années un outil majeur pour les ventes en ligne et le commerce transfrontalier, deux formes de vente que la Commission souhaite encourager car elles offrent un plus grand choix aux consommateurs et renforcent la concurrence par les prix. Le principe de base reste inchangé: les entreprises sont libres d'opter pour le mode de distribution de leur choix, sous réserve que leurs accords n'incluent pas de restrictions en matière de fixation des prix ou d'autres restrictions caractérisées et que, ni le producteur, ni le distributeur, ne dispose d'une part de marché supérieure à 30 %. Les distributeurs agréés sont libres de vendre sur Internet sans se voir imposer de limite touchant aux quantités et au lieu d'établissement des consommateurs ou de restrictions en matière de prix.

- « Ententes: la Commission adopte de nouvelles règles de concurrence pour la distribution des biens et des services », IP/10/445, 20 avril 2010.

Vers des sanctions plus sévères contre l'exploitation et les abus sexuels concernant des enfants, ainsi que la pédopornographie – Commission européenne

La Commission européenne a proposé le 29 mars dernier une nouvelle réglementation obligeant les États membres de l'UE à durcir les sanctions à l'encontre des personnes qui se rendent coupables d'abus sexuels sur des enfants. Dans sa proposition, elle demande également que les activités telles que le « grooming » (se lier d'amitié avec des enfants à des fins sexuelles) et le « tourisme sexuel » soient poursuivies pénalement, même si les abus ont été commis en dehors du territoire de l'UE. La Commission souhaite également que davantage de mesures soient prises pour prévenir ces infractions et protéger les victimes. Elle veut notamment s'assurer que les auteurs de telles infractions reçoivent un traitement adapté pour éviter qu'ils ne récidivent.

- « La Commission européenne veut des sanctions plus sévères contre l'exploitation et les abus sexuels concernant des enfants, ainsi que la pédopornographie », IP/10/379, 29 mars 2010.

Gérer l'identité numérique en cas de décès

L'identité d'une personne est le fondement de l'existence de sa personnalité juridique. Dans le « monde réel », cette identité est définie par l'état civil, le nom et le prénom. Il n'est pas loisible à une personne de se « façonner » sur mesure une identité qui ne serait pas reconnue par les autorités publiques. Par contre, dans le « monde virtuel », aucune autorité n'intervient dans l'attribution d'une identité.

Pour exister virtuellement, l'internaute doit se créer une « identité numérique » composée le plus souvent d'un compte personnel, de son mot de passe et d'une adresse email électronique. Ces attributs de l'identité numérique sont librement choisis par celui qui la créée. Elle peut par conséquent être tout à fait fantaisiste via l'utilisation d'un pseudonyme

ou le reflet de l'identité réelle : les internautes peuvent donc se créer des dizaines d'identités différentes. L'identité numérique peut aussi résulter de l'ensemble des traces ou informations qu'un internaute laisse, ramenant à sa personnalité, son caractère, son entourage, ses habitudes : par exemple ses coordonnées (email, numéro de téléphone, adresse IP etc.), ses photos, ses vidéos, ses achats effectués qui permettent de modéliser ses habitudes de consommation, ses articles dans Wikipédia ou ses avis sur des forums. Il est donc important d'avoir une vision nette de toutes les traces que nous laissons au quotidien sur Internet de manière à maîtriser l'image que l'on donne de nous-même.

- Murielle CAHEN, « Comment gérer l'identité numérique en cas de décès? », *Droit & Technologies*, 4 mai 2010.

Ordonnance contre Facebook pour omission de retirer des documents « manifestement illicites » – France

L'évêque de Soissons, Mgr Giraud, a adressé une notification à la société Facebook France fondée sur l'article 6-I de la *Loi pour la confiance dans l'économie numérique*. La notification avait été servie par lettre recommandée avec avis de réception le 9 mars 2010. Les images et propos n'ont pas été supprimés malgré une relance le 17 mars suivant. Il était allégué que l'image associée à une légende libellée ainsi : « Courir nu dans une église en poursuivant l'évêque » constituait une atteinte à la vie privée, une provocation à la haine et à la violence d'une personne à raison de son appartenance à une religion et une injure publique. Une fois la décision rendue, Facebook a retiré la page litigieuse, alors que le retrait de la photo associée à sa légende était demandé. Le juge des référés a ordonné le retrait de la photographie de Mgr Giraud, de même que le retrait des propos insultants. Facebook est également condamnée à des dommages et intérêts et il lui est ordonné de communiquer les données permettant d'identifier le créateur anonyme de la page.

- *Hervé G. c. Facebook France*, Tribunal de grande instance de Paris, Ordonnance de référé, 13 avril 2010.
- « Ordonnance de référé dans l'affaire Mgr Giraud contre Facebook », *La Croix,* 14 avril 2010.
- Nicolas SENÈZE, « Facebook condamné pour outrage contre l'évêque de Soissons », *La Croix*, 14 avril 2010.
- « Une première condamnation de Facebook en tant qu'hébergeur », *LEGALIS.NET*, 21 avril 2010.

Un site de courtage de noms de domaine qualifié d'éditeur et non d'hébergeur – France

Le Tribunal de grande instance de Paris a estimé que le site Sedo.fr, consacré à la vente aux enchères et de « parking » de noms de domaine, ne peut être qualifié d'hébergeur. Le tribunal s'est appuyé sur le degré d'intervention du site dans la relation acheteur/vendeur. Le tribunal en a conclu que le site exerce une activité d'intermédiaire et de conseil qui va beaucoup plus loin que le stockage des informations. Sur le contenu des pages parking constituées de mots clés appelés à produire des liens commerciaux, son action est également considérée comme déterminante. En plus, Sedo.fr exploite commercialement les pages litigieuses en percevant une rémunération des annonceurs.

Le Tribunal a également écarté la demande de poser une question préjudiciable à la Cour de justice des communautés européennes qui, dans son arrêt du 23 mars 2010, a posé le principe que pour appliquer ce régime de responsabilité à un prestataire technique, il convient d'examiner si son rôle est neutre, à savoir si son « comportement est purement technique, automatique et passif, impliquant l'absence de connaissance ou de contrôle des données qu'il stocke ». Dans la présente affaire, le tribunal estime plutôt que le site Sedo.fr exerce un important contrôle sur les informations.

- *Dreamnex c. Sedo GmbH*, Tribunal de grande instance de Paris, 3ème chambre, 2ème section, Jugement du 12 mars 2010, LEGALIS.NET.
- Voir: « Le site de courtage de noms de domaine Sedo est éditeur et non hébergeur », *LÉGALIS.NET,* 20 avril 2010.

À signaler

- Jean-Ludovic SILICANI, « La neutralité du net : concilier liberté et efficacité », 27 avril 2010, *Forum des droits sur l'internet*.
- Nathalie MALLET-POUJOL, « Synthèse-Droit des communications électroniques janvier 2009-février 2010 » *LÉGIPRESSE*, no. 271, avril 2010, II, 61-68.
- *Les marques dans l'entreprise de communication, LEGICOM*, no. 44 2010/1.

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.