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

June 29, 2006/29 juin 2006

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Teresa Scassa, 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 Teresa Scassa, 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

Civil Procedure

The Nova Scotia Court of Appeal has delivered its judgment in *Barthe v. National Bank Financial Ltd.* In this case, the Appellants, Barthe and Ristow, were major investors in a failed company, Knowledge House Inc. [KHI]. They sued the bank for compensation, alleging that their loss resulted from fraudulent actions of the bank's broker. The bank counterclaimed on the basis that the Appellants were complicit in the said fraud and that they were a part of an illegal share price manipulation scheme. The bank's knowledge of the alleged role and complicity of the Appellants arose when its counsel wrongfully accessed a KHI computer server. That server contained details of correspondence between the Appellants and some officers of the failed company and discussions regarding the purchase of stocks at favourable prices. None of the Appellants claimed privilege over the information on the server. However, in accordance with other similar proceedings in various actions by the bank, they wanted all or parts of the bank's pleadings, including the counterclaim and defence, dismissed on the basis that "counsel had wrongly obtained the KHI computer server thus gaining access to material that was potentially subject to solicitor client privilege or, if not privileged, confidential" (para 4). The Chambers judge ordered the bank to take steps to remedy the wrong done by the counsel including debriefing the counsel from acting for the bank but declined to dismiss the counterclaim. The Court of Appeal agreed with the Chambers judge, clarifying that he did not make a blanket order to the effect that pleadings based on wrongfully obtained information (privileged or confidential) should be dismissed. Instead, the judge rightfully made a distinction between materials that are privileged prima facie and those that are based on confidential information but not subject to privilege (para. 5). The Appeal Court agreed with the Chambers judge that the documents about the Appellants discovered on the server which were relevant to the litigation would be subject to disclosure. Dismissing the appeal, the Court held that remedial steps ordered including the debriefing of counsel and removal of various parts of the bank's pleadings that relate to privileged materials was a sufficient remedy.

Defamation

In *Weekly v. Ajit Newspaper Advertising, Marketing and Communication Inc.* Justice Spence of the Ontario Superior Court found that comments made by the defendant in a weekly newspaper and published in print and online versions were defamatory. In addition to general damages, the plaintiff sought punitive damages on the basis that the defendant's conduct was malicious. The plaintiff also argued that the fact that the article was published online in October 2002 and remained available on the defendant's web site until April 2003 was relevant to the issue of punitive damages. Spence J. declined to take the online publication into account in assessing punitive damages, noting that: "The posting of the editorial on the website in this case was part of the standard practice of the newspaper and not a special step related to the plaintiffs. An Internet user would need to go through a few steps to access the editorial, which suggests that it would not come to the attention of such users as readily as it would have reached the readers of the newspaper in its distribution in print form in the week of October 2, 2002." (at para 49)

Evidence – Bill of Costs in Personal Injury Claim

The British Columbia Supreme Court has delivered its judgment in *Noon-Ward v. Carlson*. This case involved an assessment of the Plaintiff's bill of costs regarding a personal injury claim. The action was resolved prior to jury trial. The parties agreed on all but three disbursements. The first was the disbursement of $11, 128 to Meyer Norris Peny (MNP), a firm of chartered accountants and business advisors who provided a sophisticated variety of future wage loss scenarios relating to the Plaintiff. The Defendants led an expert witness in evidence to establish that the Plaintiff's retention of MNP's professional services was unnecessary and that the services rendered could have been better provided in a less sophisticated and less expensive manner. Despite a heavily discounted bill posted by MNP, the Court agreed with the Defendant that Plaintiff's involvement of MNP amounted to creation of "a rather sizeable sledgehammer to swat a fly" (para 10). Instead of gathering raw data and using a basic computer assisted arithmetic to calculate income loss, the Plaintiff's retention of MNP is akin to purchasing "a Cadillac when an Oldsmobile or Buick could have sufficed" (para. 17). The court fixed the bill of costs for income loss at $3,750 instead of $11,128.

The second and third bills relate to litigation support and visual aid accounts. For these, the plaintiff retained Medi Tech Visual Aids and Ward Communications respectively. These are separate but mutually supportive businesses that create visual aids for litigation support. Medi Tech's agent, an ultra sound and MRI technician, reviewed about 240 ex-ray images from three computer discs and using her expertise and experience selected particular images to be used, ensuring they were such that laypersons (jurors) would be able to understand. Upon selection of the correct images, Medi Tech forwarded them to Ward Communications which then translated them from electronic disc to letter/poster size in hard prints for use by the jury. The Defendant downplayed the role of these two companies and argued that plaintiff "counsel should review the electronic images on the various discs, pick appropriate images (perhaps with the assistance of the medical specialists) and then attend at local Kinko or Jiffy Print outlet to have the images printed out" (para 23).

The Court rejected as flawed Plaintiff's attempt to undermine the expert support provided by both Medi Tech and Ward Communications. According to the Court, if counsel were to be involved with medical specialists in reviewing some 240 images in detail, that would be more expensive at the end of the day than using the expert services of Medi Tech. Similarly, patronizing a local copy shop for transfer of disc images to hard copy is "a bit like running off a copy of a Van Gogh on the local library Xerox machine" (para 25). The Court noted that "[t]he technology is available today to provide jurors, or any trier of fact, with extremely accurate helpful visual litigation aids at a reasonably modest cost. The use of professionals to accomplish this end is to be preferred to the process suggested by the Defendant's counsel" (*ibid*). Thus, the Defendants were successful in their challenge of the MNP bill whilst the Plaintiff's bill for both Medi Tech and Ward Communication services was upheld.

Evidence – Electronic Evidence

In *Desgagne v. Yuen*, Myers J. of the British Columbia Supreme Court considered a motion by the defendants to seek production of electronic evidence. In particular, they sought production of the plaintiff's home computer hard drive, Palm Pilot and video game unit.

The plaintiff had sued for damages for serious injuries arising from an accident she suffered while riding her bike. The defendant sought document files from the computer in which they hoped they would find correspondence from the plaintiff to her friends which would contain statements against interest. They also wished to access computer metadata in order to assess the frequency and duration of the plaintiff's computer activities (which presumably would be related to her claim that she was permanently disabled from competitive employment in her field as a systems analyst). Finally, the defendants were seeking access to the history of web sites visited by the plaintiff. They wished to determine whether she had visited web sites to learn the diagnostic criteria for the brain injuries she

claimed to suffer. The video game unit was sought for the purpose of accessing usage metadata in order to assess the plaintiff's cognitive abilities.

Myers J. expressed concerns about the breadth of the information sought. He noted: "The defendants are seeking disclosure of all available information to show virtually every element of the plaintiff's activities for all her waking hours. In a sense the disclosure would be even more intrusive than that obtained from an electronic monitoring bracelet, which only records physical location." (at para 14) He also noted that the document files were being sought on mere speculation that there might be relevant information in them. He stated: "It is true that documents contained in electronic form present new challenges. That does not mean, however, that the Court should lose sight of the underlying principles regarding document production." (at para 20) He went on to note that "A request to be able to search a party's filing cabinets in the hopes that there might be found a document in which an admission against interest is made would clearly not be allowed. Its digital equivalent should also not be allowed." (at para 20)

Myers J. took a different approach to the metadata, noting that in the case of this data, the defendant was seeking access to information about the patterns and degree of use of the computer made by the plaintiff. This information would be relevant to the assessment of her ability to use a computer following the accident. Myers J. noted that the Rules of Court relate to the production of "documents". Although he took the view that intuitively metadata is a report of recorded data and not a document, it nevertheless fell within the definition of "document" in the Rules, which include "any information recorded or stored by means of any device". Nevertheless, Myers J. ultimately denied the motion with respect to the metadata, stating that "it is not at all apparent to me how a series of questions as to how long particular computer files may have been open on the plaintiff's computer would assist in elucidating the issue of cognitive ability or ability to work on a computer." (at para 33) He also noted that the request raised competing privacy concerns, and stated: "Even if I were able to find that the metadata had some marginal probative value, that value would be offset by these interests." (at para 40) He declined to order production of the videogame unit for essentially the same reasons.

Myers J. also rejected the request for web browsing history on the basis that it was not relevant given the range of "plausible reasons why the plaintiff might consult these sources". (at para 45) Even if the information were marginally relevant, he stated that he would still not order its production because of the intrusive nature of such an order.

Comment on the issues raised in this case at the IT.Can Blog

Evidence – Re-imbursement for Production of Documents

The British Columbia Court of Appeal has delivered its ruling in *Canada (Attorney General) v. Pacific International Securities Inc.* In this case, authorities in New York State suspected that some individuals illegally obtained and used confidential law-enforcement information to fraudulently manipulate the price of publicly-traded stocks. They believed that the Canadian security-dealer respondent possessed record that would assist New York authorities in the investigation and prosecution of the case. Pursuant to the *Mutual Legal Assistance in Criminal Matters Act*, they asked the Crown to assist with obtaining the information from the respondent. Upon the request of the Crown via the Attorney General, the Supreme Court of BC made three orders directing the respondent to produce some evidence. The respondent complied with the first two. In regard to the third order by the Associate Chief Judge, the respondent complained that the order required a huge and onerous amount of information, involving in some cases electronic re-creation of a wide range of documents thus exposing the respondent to "substantial staff time and expense" (para 12). Also, the order set an unreasonable deadline. The respondent informed the Crown that it would be hiring additional temporary staff and asked whether its expenses would be reimbursed. Although the Crown declined to commit to re-imbursement, it was agreed that the respondent would reserve its right to make representation for re-imbursement at the transmittal hearing phase of the proceeding. At the transmittal hearing, the respondents invoked

sections 18(5) and (6) and sections 20(2) of the *Act* to support its re-imbursement claims: wages for temporary staff, hourly charges for permanent staff, costs of retrieving records from storage and incidental costs including photocopying which amounted to $57, 884.87. At first instance, Justice Boyd ordered the Crown to pay the respondent's reasonable expenses arising from the production of the documents. Her grounds for so ordering were based on section 20(2)(c) of the *Act* which vests discretion on the courts to make order on terms to protect third party interests. She ignored reference to section 18(5)(6) which covers the application of discretionary order in regard to both third parties and other persons ("the person named therein" in the order) who produced required evidence.

The majority of the Court of Appeal (Ryan and Saunders JJ.A) allowed the Crown's appeal holding that the judge did not have power to make a re-imbursement order and that the *Act* was a complete code for dealing with requests for information from the United States. According to them, the *Act* did not provide for re-imbursement of parties like the plaintiff. Accordingly, this lacuna in the law is for the Parliament to fix if it so desired.

In his dissent, Smith J.A. would have dismissed the appeal. However, he observed that Boyd J did not have jurisdiction to make the order pursuant to section 20(2)(c) and was also wrong to describe the respondent as a third party. However, under section 18 a judge can make discretionary orders including those dealing with "matters arising during and after transmission to the foreign state of evidence already obtained" (para 18). Smith J.A. observed that although there is no express provision in the *Act* with respect to re-imbursement, the discretion provided for under section 18(5) of the *Act* ought to cover orders made in respect of "expenses of an extraordinary nature". Such expenses are the responsibility of the Crown under the international agreement underlying the *Act*. (para 34). The judge acknowledged the Crown's argument that responsibility for maintenance of law and order is a collective social responsibility and that it would be contrary to public policy to interpret section 18(5) as creating obligation on the Crown to compensate persons named in production order for compliance expenses. However, the judge held that "the demands put upon citizens in modern society to co-operate in criminal proceedings by producing relevant records can be far more burdensome than was the case before the advent of the computer and the resulting proliferation of records" (para 32). According to Smith J.A., "the respondent was apparently required to hire additional staff to enable it comply with the order and was allegedly put to significant expense. To saddle it with these expenses is to impose a not insignificant financial burden" (para 33). He was not persuaded that traditional requirement that citizens participate in the administration of justice without expectation of compensation warrants compromising the discretion provided for under section 18(5) of the *Act* (para. 35).

Comment on the issues raised in this case at the IT.Can blog.

Privacy

The Privacy Commissioner of Canada has tabled her 2005–2006 Annual Report on the *Privacy Act*. This follows on the heels of a June 5 Report calling for significant reforms to that Act. It is not surprising, therefore, that the Annual Report also calls for reform of the legislation. In addition to reviewing complaints and investigations from 2005–2006, the Report comments on a number of significant policy issues. These include public interest disclosures, transborder data flows, international liaison, Radio-Frequency Identification Devices (RFIDs), videosurveillance guidelines and identity management in the context of the war on terror. The Annual Report also summarizes the Commissioner's findings from an audit of the Canada Border Services Agency in relation to the transborder flows of personal information.

The Final Report of the Privacy Commissioner of Canada on the OPC's Audit of the Personal Information Management Practices of the Canada Border Services Agency has also just been released. The Final Report makes 19 specific recommendations to improve the CSBA's information management systems and procedures. The OPC raised particular concerns about verbal exchanges of information that are not based on written requests and that are not consistently recorded. The OPC notes that the CSBA is currently not able to accurately report on the extent or frequency of its information sharing with the United States, and recommends the development

of a "coordinated method of identifying and tracking all flows of its trans-border data." (Section 1.3) The Audit also assessed the Passenger Information System (PAXIS) and the Integrated Customs Enforcement System (ICES). The Audit concludes that these systems are sound, but recommends some changes to reduce the risk of improper disclosure and use of personal information. The Audit also calls for more transparency with respect to trans-border data-sharing activities.

The Privacy Commissioner of Canada has made a Submission to the Standing Senate Committee on Banking, Trade and Commerce on the Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In it, Commissioner Stoddart sets out the difficult of assessing the proportionality of the impact of the regime on privacy given the difficulty in getting a clear sense of the scope of the problems of money laundering and terrorist financing, and the effectiveness of the current regime. Stoddardt notes that the proposed regime is unprecedented because it requires those entities covered by the legislation to act as agents of the state in collecting personal information above and beyond what is required for business purposes. It also creates a mandatory reporting system that would allow government officials to gain access to large quantities of personal information without warrants. Stoddart's submission concludes that the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* "is an inherently intrusive Act that is at odds with the protection of privacy."

The Ontario Privacy Commission has released new Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines). The aim of the document is to set out "best practices" for business who design or operate RFID systems. The OPC makes the point that privacy and security must be built into the design of RFID systems, and that the focus of privacy concerns should be on the systems in place rather than the technology itself. The preamble to the Guidelines calls for "open and transparent" use of RFID systems. The Guidelines themselves take the fair information principles identified in the CSA Privacy Code (now incorporated into PIPEDA) and explain how each should apply in the context of RFID systems.

2ième partie

Technologie d'identification par radiofréquence (RFID) – CAI

La technologie RFID (*Radio Frequency Identification*) repose sur l'utilisation d'une puce électronique qui est reliée à une antenne miniature généralement incluse dans une étiquette. Les étiquettes RFID remplaceront probablement les étiquettes à codes barres.

La Commission d'accès à l'information (CAI) a publié une analyse qui fournit un premier éclairage sur cette technologie et qui souligne les différents enjeux qu'elle pose en regard de la protection des renseignements personnels et de la vie privée. Ce premier document pourrait conduire éventuellement à l'établissement de normes ou de règles d'utilisation.

La CAI souligne que les applications de cette technologie sont multiples particulièrement dans le domaine commercial (ex : comptabilisation des achats à distance, gestion de l'inventaire des magasins), dans le domaine de la santé (ex : gestion des retours, des contre-indications, des diversions et des contrefaçons de médicaments) et dans le domaine du transport (ex : e-passport, contrôle des véhicules aux frontières).

Le déploiement de ces diverses applications à l'insu du citoyen soulève des risques potentiels d'atteinte aux droits de l'individu étant donné que ce dernier n'a pas de contrôle sur certains usages de la technologie RFID (ex : la présence de la technologie dans le produit n'est pas toujours identifiée, il n'existe pas de norme ou de politique d'utilisation de cette technologie, il n'y a pas de possibilité de fournir un consentement à la saisie des données, possibilité de traçabilité de l'étiquette au-delà de l'achat). Cette technologie peut avoir de nombreuses implications en matière de vie privée, particulièrement si les données contenues dans une puce peuvent être associées à des renseignements nominatifs (ex : établissement de profils de consommation de la clientèle, augmentation des risques d'usurpation d'identité).

La CAI relève différents constats ou préoccupations en regard des principes de la protection des renseignements personnels qui méritent une attention particulière. Ainsi, si une entreprise ou un organisme public recueille, détient utilise ou communique à des tiers des renseignements personnels en association avec une technologie RFID, une réflexion sur les principes suivants doit être entreprise : la responsabilité des renseignements personnels, la finalité, la limite de la collecte, l'information au citoyen, la limitation de l'accès aux renseignements personnels, la communication des renseignements personnels, la qualité des renseignements, la sécurité, le droit d'accès et de rectification et enfin, la conservation et la destruction des données.

En attendant des réponses plus précises, souligne la CAI, le citoyen doit demeurer vigilant et la CAI, conformément à la loi, exercera une surveillance à l'égard de l'introduction de cette nouvelle technologie.

- COMMISSION D'ACCÈS À L'INFORMATION, *La technologie d'identification par radiofréquence (RFID)–Doit-on se méfier?*, document d'analyse, préparé par Gaétan Laberge, direction de l'analyse et de l'évaluation, mai 2006, www.cai.gouv.qc.ca/

Commentez cet article au Blogue de IT.CAN

Diffusion de photos sur Internet sans autorisation

La demanderesse a rencontré Duchesneau par l'entremise du site *Réseaucontact.com* en septembre 2003. Après quelques semaines, elle met fin à leur relation. En décembre suivant, un ami l'informe qu'il y a des photos compromettantes d'elle sur le site. Elle porte plainte au criminel, des accusations sont portées contre Duchesneau suite à une enquête, mais elles sont abandonnées car on n'estimait pas être en mesure de faire une preuve hors de tout doute. La demanderesse réclame $6 500 en dommages de Duchesneau qui aurait diffusé sur Internet des photographies intimes la représentant nue, sans son consentement.

Le tribunal a entendu le témoignage de l'enquêteur qui suite à un mandat de perquisition, a obtenu les coordonnées de l'utilisateur IP qui n'était autre que Duchesneau. Ce dernier aurait visité un site au nom

de la demanderesse sur Réseaucontact. Selon les renseignements, l'ordinateur de Duchesneau n'a pas fait l'objet d'intrusion, de sorte que l'adresse IP ne pouvait provenir que de son ordinateur. Duchesneau plaide qu'un virus appelé « cheval de Troie » a été détecté sur son ordinateur et que la demanderesse, pendant le temps passé chez lui, a pu introduire le virus ou prendre son adresse IP.

Le tribunal estime que la preuve est prépondérante à l'effet que c'est Duchesneau lui-même qui a diffusé les photographies de la demanderesse et qui a rédigé les messages à sa place. Aucune preuve ne révèle que Duchesneau a eu des problèmes avec son ordinateur et le tribunal ne croit pas que la demanderesse a mis elle-même ses photos dans l'ordinateur de Duchesneau. Duchesneau a ainsi porté atteinte à la dignité et à la réputation de la demanderesse. Dans les circonstances, le tribunal accorde 500$ pour l'atteinte à la réputation et 500$ à titre de dommages punitifs puisque l'atteinte est intentionnelle. Le dommage moral, souligne-t-il, est difficile à quantifier car il est impossible de savoir combien de personnes auront accès et diffuseront à leur tour une photographie sur un site Internet. Le tribunal relève également le manque de jugement de la demanderesse qui a remis des photographies intimes à une personne qu'elle n'a rencontré qu'à trois ou quatre reprises.

- *Pelchat c. Duchesneau*, 2006 QCCQ 5569, 25 avril 2006.

Utilisation malveillante de l'identité d'autrui, dénigrement et atteinte à la vie privée – France

Une jeune femme a décidé de se moquer d'une de ses collègues en utilisant son identité sur des sites de rencontres. Dans une décision du 16 juin 2006, le tribunal de grande instance de Carcassonne qualifie ces agissements de violences volontaires, avec préméditation. Dans un but de vengeance contre une collègue qui n'avait pas voulu participer à un mouvement de grève, la défenderesse a usurpé son identité dans des sites de rencontre en la décrivant *« comme une fille facile, désireuse de relations sexuelles »*. En plus, elle avait communiqué les coordonnées téléphoniques de la victime. Cette dernière a reçu plusieurs appels d'hommes intéressés par son profil. Gravement perturbée, elle a été obligée d'interrompre son travail pendant dix jours. La prévenue a répété la blague et a été surprise en flagrant délit. Occupant un poste de responsable informatique dans une entreprise, elle avait utilisé le poste de travail de son directeur, dont elle avait les codes d'accès, pour tenter d'éviter que les faits lui soient imputés.

Le tribunal a conclu que la prévenue avait agi dans l'intention de nuire à la victime dont elle connaissait la fragilité psychologique. Il constate aussi une circonstance aggravante de préméditation, soit le fait d'avoir « utilisé non pas son propre ordinateur mais celui du directeur de la mission d'insertion, ce qui induit nécessairement que les faits n'ont pas été commis de façon spontanée ».

- *Ministère public, Carine G. et autres / Christine S.*, Tribunal de grande instance de Carcassonne, 16 juin 2006.

Responsabilité en vertu de la loi française d'un hébergeur situé en dehors du territoire français – France

La cour d'appel de Paris a confirmé, par un arrêt rendu le 14 juin 2006, la condamnation de Bell Med Limited et CATL, deux hébergeurs maltais d'un site de paris hippiques en ligne. Ces derniers n'avaient pas agi promptement pour en rendre impossible l'accès, une fois que le contenu illicite avait été porté à leur connaissance. Bien que le site illicite était hébergé à Malte, le tribunal français réaffirme compétence dans la mesure où le dommage avait été subi en France.

- *BML, CATL c. PMU*, Cour d'appel de Paris 14ème chambre, section A, 14 juin 2006.

Commentez cet article au Blogue de IT.CAN

Responsabilité de l'hébergeur de pages personnelles qui y place des publicités payantes – France

Tiscali offrait un service par lequel elle héberge des pages personnelles tout en proposant aux annonceurs d'y placer des publicités payantes. Dans un arrêt rendu le 7 juin 2006, la cour d'appel de Paris conclut que Tiscali possède en fait la qualité d'éditeur. Elle est du coup responsable des reproductions illicites des bandes dessinées sur le site personnel d'une personne impossible à identifier. L'entreprise est condamnée à verser 10 000 euros de dommages-intérêts aux éditeurs des bandes dessinées ainsi contrefaites. Dans une décision du 16 février 2005, le Tribunal de Grande instance de Paris avait condamné Tiscali, en tant qu'hébergeur, pour avoir failli à son obligation légale de détenir et de conserver les données d'identification des personnes dont il héberge le contenu. La cour d'appel confirme que Tiscali a été négligente pour n'avoir pas porté attention au caractère fantaisiste des coordonnées communiquées.

- *Dargaud Lombard, Lucky Comics / Tiscali Média*, Tribunal de grande instance de Paris 3ème chambre, 1ère section, 16 février 2005.

Commentez cet article au Blogue de IT.CAN

À signaler

- Caroline Vallet, *La lutte contre la pornographie juvénile : une longue saga au Canada!*, Juriscom.net, 11 juin 2006.
- Depuis le 20 juin 2006, les noms de domaine en « .fr » sont ouverts aux particuliers en France. Voir *Juin 2006 : l'appel du « .fr »*, Forum des droits sur l'Internet, 20 juin 2006.