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

May 5, 2006/5 mai 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

DNA Databank Provisions Constitutional

In 2003 the Supreme Court of Canada rejected a *Charter* challenge in *R. v. S.A.B.*, and upheld the DNA warrant provisions of the *Criminal Code*. Those provisions allowed for the use of DNA warrants as an investigative tool by the police when they had a suspect and a DNA sample associated with a particular crime. Left for another day at that time were the DNA databank provisions in the *Criminal Code*, which allow for the police to gather DNA samples from various specified individuals and retain them for use in future unspecified investigations. The Supreme Court has now found those provisions to be constitutional as well in *R. v. Rodgers*.

The DNA databank provisions allow the retrospective collection of DNA samples from three groups of offenders who had already been sentenced when the provisions came into effect: (a) persons already declared to be "dangerous offenders"; (b) persons convicted of "more than one murder committed at different times"; and (c) persons convicted of "more than one sexual offence" and who, on the date of the application, are still serving a sentence of imprisonment of at least two years for one or more of those offences. In each case collection of the sample must be authorized in advance by a provincial court judge, based on an *ex parte* application. Other provisions of the scheme also allow orders to be made at the time of sentencing for the inclusion of a sample of the accused's DNA to be included in the databank, but this challenge concerned the retrospective provisions.

The accused was a repeat sexual offender covered by the retrospective provisions, and he brought a Charter challenge based on ss. 7, 8, 11(*b*) and 11(*i*). In particular he objected to the legislative scheme on the basis that: (a) the order allowing a DNA sample to be taken is made ex parte; (b) a DNA sample can be taken from a convicted offender without any reasonable grounds linking the offender to a particular unsolved crime; and (c) it punishes the offender again for an offence. He also argued that even if the legislation were constitutional the trial judge erred in choosing to proceed *ex parte* in this case in the absence of any evidence demonstrating the need to do so. A version of the latter argument had succeeded in the Ontario Court of Appeal, where it was held that although the legislation was constitutional, it should be read as requiring a presumptively *inter partes* application.

The Supreme Court rejected all of these arguments, and disagreed with the Ontario Court of Appeal's interpretation. They held that the legislation was constitutional as written, and that the legislation was clear in allowing *ex parte* applications without a presumption of *inter partes* applications.

With regard to the nature of the application, the Court held that an accused was guaranteed procedural fairness, but the nature of procedural fairness differed with the context: there was no freestanding right to *inter partes* proceedings. What was fair in a particular case would depend on the context. In this context, the accused would by definition already be known to law enforcement personnel and so might already be a logical suspect in future investigations. At most, therefore, what the offender loses through a successful application for a DNA databank sample is that his or her DNA profile is made available to the state for

identification purposes. This result could serve to exclude the offender as a suspect in future. Further, the application process provided the offender with a number of safeguards, including that the prior judicial authorization must come from a provincial court judge, that the judge has the discretion to give notice of the application or to choose not to order the DNA sampling of offenders, or to impose conditions, and that the police must report back in writing to the provincial court judge.

The more central issue was that the application procedure permitted a sample to be taken merely for the purposes of having it in the databank, without any suspicion connecting the accused to a crime. Rodgers argued that this violated the minimum requirements for searches set out in *Hunter v. Southam*: in particular the criterion that there are reasonable grounds to believe that an offence has been committed and that evidence of it will be found by the search. Since the samples were only being taken to be included in a databank for investigation of possible future offences, Rodgers, argued, the *Hunter* criteria were not met. The Court rejected this argument, on the basis that the *Hunter* criteria were not immutable. Although that case generally set the norm for searches, context could dictate that other standards could sometimes apply. In this context, the court held, the nature of the interference with individual privacy was more akin to fingerprinting than to anything else. Although an offender's DNA sample could be included in the databank, it was there only to identify the accused, not as in investigative tool. The Court noted that if a sample from the DNA databank were found to match DNA at a crime scene, that would not lead to release of the sample or constitute evidence against an accused: rather, it would be a basis upon which the police could then seek a DNA warrant in order to obtain a sample of the accused's DNA. Fingerprinting had long been held to be constitutional. Although the nature of the information potentially obtained about an individual from a DNA sample was much greater, and invoked a greater privacy interest than would fingerprints, the scheme was found to contain adequate protections for these interests. The use of non-coding DNA, for example, and the strict limits on the use to which samples could be put, among other factors, meant that the privacy interests of the accused were adequately respected. This was particularly so given the reduced privacy interest of the individuals potentially subject to the orders.

Finally the Court held that as the DNA databank provisions were not punitive they did not invoke any of the s. 11 protections relating to additional punishments.

A minority of three of the seven judges would have found the legislation unconstitutional for failing to provide for an *inter partes* application. In their view *inter partes* applications should be the norm and should only be departed from in exceptional circumstances. Given that there was no increased flight risk from notice of an application as opposed to a notice to appear to give the DNA sample, and given that there was no risk of destruction of the evidence, the minority felt that a subject ought to be given notice of the application. The possibility of a "cumbersome and expensive *ex post facto* review on narrow jurisdictional grounds" (para 73) was not an adequate substitute.

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

Enforcement of Foreign Judgments

In *Disney Enterprises Inc. et al v. Click Enterprises Inc.*, Lax J. of the Ontario Superior Court of Justice considered an application to recognize and enforce a judgment of the U.S. District Court for the Southern District of New York against a respondent based in Ontario. The judgment awarded damages to the applicants in the amount of almost half a million dollars for copyright infringement and unfair competition.

The respondent corporation (defendant at trial in N.Y.) operated several websites, including FlicksUnlimited.com and DownloadFreeFilms.com. These sites offered memberships to consumers. Members were provided with access to various technological tools that would assist them in downloading films from the internet. Members were also entitled to seek online assistance in tracking down hard-to-find films. The websites were sponsored links on search engines such as Google, and featured pull-down menus of films available

for copying. Lax J. noted that the sites created the impression that activities were "100% legal", but at the same time, members were also offered access to software that would help them eliminate traces of their downloading and copying activities. Lax J. summarized the respondent's activities as follows: "In effect, the respondents conducted an Internet retail business for profit that facilitated the illegal copying and downloading of copyrighted motion pictures." (at para 6).

The respondent was properly served with notice of the action brought against it in New York. It did not appear at trial, and a default judgment was entered against it. There was no challenge made to the jurisdiction of the N.Y. court to hear the matter.

Lax J. considered the circumstances in which a foreign judgment would be recognized in Ontario. She noted that the determination of whether a court had properly exercised jurisdiction depended on two principles: "the need for 'order and fairness' and the existence of a 'real and substantial connection' to either the cause of action or the defendant". (at para 11) Lax J. noted that the requirements of "order and fairness" were met where "the originating court had reasonable grounds for assuming jurisdiction" (at para 12), and she found that those grounds existed in this case. In considering 'real and substantial connection', Lax J. noted that flexibility is necessary in the application of the test. She commented on the particular borderless nature of the internet, and cited the Supreme Court of Canada's decision in *SOCAN v. CAIP* for the principle that "either the country of transmission or the country of reception may take jurisdiction over a transmission linked to its territory". (at para 23) Lax J. had no difficulty finding a real and substantial connection in this case. She noted that the respondent company had:

> …a commercial purpose that utilized the Internet to enter the United States to carry out its activities. It contracted with payment services providers in the United States to carry out its activities. It contract with payment service providers in the United States to process Internet payments on its websites. (para 26)

Lax J. accepted that there was evidence that the web site services were made available to residents of the United States, and that the content of the downloads were American films. She stated: "It would not surprise anyone that the consumers of American films are Americans, not exclusively, but in large numbers." (at para 27). She also found that the services offered by the web site to help members obscure their downloading activities established that "the respondents were clearly aware of the illegal nature of their business and the infringing conduct of their customers." (at para 27)

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

Municipal By-Laws – Videotaping of Fights

The City of Regina has passed an *Anti Bullying and Public Fighting Bylaw* which makes it an offence for any person to engage in bullying of another person through written or electronic communication, as well as in person. "Bullying" was defined to include behaviour that would "intimidate, humiliate or isolate" another person or would cause "physical or emotional distress". In addition, the by-law makes it an offence to take pictures or videos of a fight and post them online. Violations of the by-law are punishable by fines of up to $2,000.00.

Privacy and Access to Information Laws

In *Attorney General of Canada v. H.J. Heinz Company of Canada Ltd* the Supreme Court of Canada considered the relationship between the federal *Access to Information Act* and the *Privacy Act*.

The respondent Canadian Food Inspection Agency (CFIA) had received a request under the *Access to Information Act* that sought access to records of the CFIA relating to H.J. Heinz Company of Canada (Heinz). Since the CFIA was of the view that some of the records might contain confidential business information, it gave notice to Heinz so that that company could make representations under s. 28 as to why the information in the records should not be disclosed. After reviewing the representations made by Heinz, the CFIA decided to disclose the records, subject to a few redactions. Heinz sought a review of this decision under s. 44 of the

Access to Information Act. As part of the review procedure, Heinz argued that the records should not be disclosed because the contained confidential business information, and because, contrary to s. 19(1) of the *Act*, they would disclose personal information relating to individuals. At the review proceeding, the Attorney General argued that the s. 44 review procedure was limited to the argument in relation to business information, as it was an issue in relation to business information that triggered the whole process.

A narrow majority of judges were of the view that the position of the Attorney General was "too restrictive of the rights involved" (at para 2). Deschamps J., for the majority wrote that "The right of access to government information, while an important principle of our democratic system, cannot be read in isolation from an individual's right to privacy." (para 2) Moreover, "in a situation involving personal information about an individual, the right to privacy is paramount over the right of access to information, except as prescribed by the legislation." (at para 26)

Deschamps J. noted that within the scheme of the *Access to Information Act*, s. 44 provides the sole means by which a third party can seek to prevent an intended disclosure of personal information. She noted that the complaint mechanisms in the *Privacy Act* to remedy improper disclosures of personal information only provided an after-the-fact recourse. Section 19(1)(*b*)(ii) of the *Privacy Act*, which provides a more general opportunity for recourse to the Privacy Commissioner, is also inadequate because, as Deschamps J. notes "the Privacy Commissioner has no authority to issue decisions binding on the government institution or the party contesting the disclosure." (at para 37) Similarly, the Information Commissioner lacks the power to issue binding orders or injunctive relief, and, in any event, is meant to be an advocate for disclosure of information.

Deschamps J. acknowledged that s. 44 can only be triggered by a third party's right to notice in relation to the disclosure of documents containing confidential business information. Notwithstanding this, she took the view that the plain language of the *Act* "does not explicitly restrict the scope of the right of review." (para 41) Further, she found that the language of the *Act* supported a broad interpretation. She noted that a right is given to parties to make "representations", but no words limit the scope of the "representations". Section 44 gives the third party a right to apply to the court for a review of "the matter". Deschamps J. observed that "the matter" was a broad and general term and is not limited to a "decision" or an "order". She concluded that "The plain language of the statute, together with the legislative context and combined purpose of the *Access Act* and the *Privacy Act*, provides ample foundation for the conclusion that the reviewing court has jurisdiction to protect personal information on a third party application for review." (at para 46)

In reaching its decision, the majority of the Court referred to the privacy rights of individuals as "quasi-constitutional" (at para 63). Their view of the centrality and importance of privacy rights clearly drove their approach to the interpretation of the *Access to Information Act*.

Bastarache J., wrote for the dissenting justices. He too characterized the case as relating to the "delicate balance" between privacy and access to information. Bastarache J. took the view that even if one accepted that privacy was paramount over access, "it does not follow that Parliament is obliged to create a notice and review mechanism prior to the disclosure of personal information." (at para 72)

The dissenting justices rejected the interpretation subscribed to by the majority. Bastarache J. expressed the view that "[t]he right to bring a s. 44 review flows from the notice a third party receives because of the believed presence of confidential business information in the requested record." (at para 94) If there were no confidential business information, the third party would not receive notice. The s. 44 review is thus intended to focus on the specific issue of the presence of confidential business information. To allow issues of personal information to be raised in the s. 44 proceeding would mean that it would allow "greater protection of certain individuals' personal information, depending on the possible application of s. 20." (at para 100) Bastarache J. stated "The structure of the *Access Act* and of the *Privacy Act* suggests that Parliament intended that the protection of personal information be assured exclusively by the Office of the Privacy Commissioner." (at para 97)

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

Warrantless Search – Sniffer Dogs

The Ontario Court of Appeal has handed down the first appellate level decision with regard to an issue which has been debated for the past 18 months in various trial courts across Canada: whether the Supreme Court of Canada's decision in *R. v. Tessling* that police use of a FLIR to detect heat emanations from a house did not infringe on an accused's reasonable expectation of privacy led to the conclusion that police use of a dog to sniff the belongings of people in public places was also not a search. In *R. v. A.M.* the Ontario Court of Appeal has held that such action does constitute a search.

The Principal of a high school in Sarnia had issued a standing invitation to the police to come to the school if they had a sniffer dog. On the date in question the police arrived and asked whether they could go through the School: other than the "standing invitation" the police were not in the School at the request of the Principal, and the Principal had no particular suspicions that day, beyond his general belief that there could always be drugs in the School. The Principal made an announcement over the School's public address system telling all students to remain in their classrooms: they were ultimately made to remain there for a period between 90 minutes and two hours. The police then began searching the school with the dog, eventually arriving at the gymnasium where they had the dogs sniff some backpacks that were against a wall. The dog indicated the presence of drugs in one backpack, and the police then opened it and found marijuana and magic mushrooms.

The Crown conceded that the police were searching the back pack when they opened it, but argued that no search had taken place simply by the dog sniffing the backpack. They argued that this conclusion followed from the decision in *Tessling*. The Court of Appeal rejected the argument, though its reasoning was quite brief. They held that the dog was a direct and integral part of the police officers' search and was essentially a physical extension of its handler. They also noted that when police officers personally tried to obtain information by smelling a location, this qualified as an "olfactory search": *R. v. Evans*, [1996] 1 S.C.R. 8. With regard to the FLIR analogy, the court held that there was a significant difference between a plane flying over the exterior of a building and taking heat pictures of a house which had been specifically targeted, and the actions of the police here in using a trained dog to sniff the personal effects of the entire student body at random. The court did not discuss issues about the nature of the information discovered which had been the focus of much of the lower court debate.

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

2ième partie

Environnements électroniques

En plus d'une édition spéciale sur l' « Immigration et sécurité », la revue juridique *Lex Electronica* (vol. 11, no 1, printemps 2006) présente son édition courante où on peut lire des articles ayant trait à des questions inhérentes aux environnements électroniques, à savoir le droit au gré d'Internet, l'influence des médias électroniques sur la formation de l'opinion publique, la diffusion du droit en Afrique de l'Ouest, le vol d'identité, le droit de la preuve, les enjeux juridiques de technologies telles que WiMAX et RSS.

- BERTHOU, Renaud, *Le droit au gré d'Internet: à propos d'une réseautisation fort peu anodine de l'univers juridique*
- CHARBONNEAU, Olivier, *RSS et la publication simultanée sur Internet*
- CHAWKI, Mohamed and ABDEL WAHAB, Mohamed, *Identity Theft in Cyberspace: Issues and Solutions*
- DINU, Irina, *Droit de la preuve appliqué au commerce électronique au Canada, droit civil / common law*
- LANGELIER, Richard, *L'influence des médias électroniques sur la formation de l'opinion publique : du mythe à la réalité*
- MIAN, Simon, *WiMAX ou l'évolution des réseaux sans-fil ?*
- TAGODOE, Amavi, *Diffusion du droit et Internet en Afrique de l'Ouest*

Les médias de service public dans la société de l'information – Conseil de l'Europe

Dans ce rapport, préparé pour le compte du Groupe de spécialistes sur le service public de radiodiffusion dans la société de l'information du Conseil de l'Europe, on présente une revue élaborée des tendances actuelles de l'évolution du monde des médias et des implications pour les médias de service public (MSP). Les mutations dans les fondements de la réglementation des médias découlant des technologies numériques sont examinées. L'approche se distingue de celle qui tient souvent lieu d'analyse en ces matières. On postule que les changements techniques n'emportent pas magiquement la disparition des raisons qui sous-tendent les demandes pour renforcer les services publics de radio et de télévision. On observe l'existence d'une tendance à prendre pour acquis que le service public est voué au confinement dans les créneaux traditionnels alors que d'autres soutiennent qu'il doit prendre les moyens d'assurer sa présence dans les environnements numériques.

Parmi les constats et conclusions du rapport, on relève qu'en principe, les médias de service public doivent être utilisés de manière régulière par tous les citoyens-ils doivent avoir une forte audience. Les médias de service public doivent offrir une gamme de contenus et de services à la fois différents de ceux proposés sur le marché et susceptibles d'attirer en même temps une large audience. Leur mission consiste également à offrir des contenus et des services spécifiques à des petits groupes présentant des besoins particuliers et aux citoyens en tant que consommateurs individuels. Elle comprend également la prestation d'un large éventail de services individualisés liés aux « nouveaux médias » tels que la production de programmes dans les petits pays européens. Le chapitre 7 insiste sur la nécessité de réévaluer le statut des entreprises de médias commerciaux qui, dans de nombreux pays, sont contractuellement tenues de remplir des obligations de service public. Enfin, des arguments sont avancés contre toute répartition des fonctions des MSP, celle-ci risquant d'aboutir à la solution radicale d'un démantèlement de l'institution publique au profit d'un « trust » de médias de service public. La question de la gouvernance, abordée au chapitre 8, constitue un aspect spécifique de l'organisation des MSP : comment garantir l'autonomie éditoriale compatible avec le mode de financement collectif que constitue le paiement d'une redevance ou le financement à même les budgets gouvernementaux.

Commentez cet article au Blogue de IT.Can

Christian S. NISSEN, Les médias de service public dans la société de l'information, rapport préparé pour le compte du Groupe de spécialistes sur le

service public de radiodiffusion dans la société de l'information, Conseil de l'Europe, Février 2006, disponible sur le site de la Division Médias du Conseil de l'Europe, et aussi en pdf.

Expulsion d'un élève blogueur annulée – France

En mars 2005, le principal du collège Teilhard de Chardin à Chamalières a procédé à l'exclusion définitive de Erwin S., fils de la requérante alors âgé de 14 ans. On reprochait à celui-ci d'avoir diffusé sur son site internet des propos injurieux et offensants à l'encontre de professeurs et d'élèves fréquentant le collège. Les instances d'appel prévues par les lois applicables ont maintenu la décision d'exclusion. Le Tribunal administratif relève la présence non contestée au sein du « blog » de l'étudiant « d'un ensemble d'élucubrations caractérisées par leur incontestable bêtise et une profonde vulgarité, mettant en cause nommément des élèves et des professeurs enseignant à l'intérieur de l'établissement public local » qui était de nature à justifier légalement le prononcé d'une sanction disciplinaire. Une sanction disciplinaire était justifiée même si l'acte reproché a été commis à l'extérieur de l'enceinte scolaire car, par sa qualification diffamatoire et injurieuse, il était de nature à perturber le bon fonctionnement du service public et que la charte d'utilisation d'internet ne régit que l'usage des ordinateurs appartenant au collège. Mais en dépit de « l'atteinte aussi sérieuse que compréhensible à la sensibilité de personnes outragées par un comportement puéril et irresponsable qui ne saurait être excusé d'une quelconque manière par l'ignorance alléguée de l'adolescent des dangers inhérents à la communication électronique », le tribunal observe que cet agissement n'a engendré aucune violence physique ni connu de réitération. De plus, le jeune Erwin - par ailleurs excellent élève - ne possédait aucun antécédent disciplinaire. Par conséquent, même si les faits dont il s'est rendu coupable justifiaient une sanction susceptible d'aller jusqu'à l'exclusion temporaire de l'établissement, ils n'impliqueraient cependant pas, en eux-mêmes, l'application immédiate de la sanction la plus sévère prévue, à savoir l'exclusion définitive. En prononçant une sanction disproportionnée par rapport au délit à l'encontre du jeune Erwin S. et à raison des faits considérés, le recteur de l'académie de Clermont-Ferrand a commis une erreur d'appréciation entachant sa décision du 15 avril 2005 d'excès de pouvoir ; celle-ci doit, conclut le tribunal, être annulée.

Commentez cet article au Blogue de IT.Can

Corinne N. c. Collège Teilhard de Chardin, Tribunal administratif de Clermont-Ferrand, 2e chambre, 6 avril 2006.

Voir aussi : *Indulgence du tribunal administratif envers un collégien blogueur*, LEGALIS.NET, 20 avril 2006.

Sanction de pratiques de « typosquating » – France

Dans une ordonnance de référé du 10 avril, le Tribunal de Grande Instance de Paris enjoint une société à transférer les noms de domaine « rueducommerc.com » et « rueducommrece.com » à l'entreprise titulaire des marques « rue du commerce », « www.rueducommerce.com et .fr », « RDC.fr », et « la rueducommerce, fr et .com ». La société défenderesse exploitait les noms de domaine litigieux (en modifiant l'orthographe du terme de la marque) pour rediriger les internautes qui tapaient par erreur ces appellations vers des sites concurrents de ceux de la société détentrice des marques « rueducommerce ». Le tribunal estime que la requérante dispose de marques notoires et, sur le fondement de l'article L.713-5 du *Code de Propriété intellectuelle*, conclut que l'utilisation des marques à l'orthographe erronée par la société intimée constitue un trouble manifestement illicite justifiant le prononcé d'une ordonnance de référé.

Commentez cet article au Blogue de IT.Can

Société Rue du Commerce c. Société Brainfire Group et Société Moniker Online Service inc., Tribunal de Grande Instance de Paris, Ordonnance de référé, 10 avril 2006.

Voir aussi : *Cybersquatting : condamnation de l'unité d'enregistrement aux frais de justice*, LEGALIS.NET, 24 avril 2006.

Le fait d'avoir pour prénom « Milka » ne confère pas le droit de s'opposer à l'usage de la marque « milka » – France

Confirmant une décision de première instance, la Cour d'appel de Versailles a donné raison à la société Kraft qui reprochait à l'intimée, une couturière, d'exploiter un site sous le nom de domaine « milka.fr » et présentant un fond d'écran de couleur associée aux produits vendus sous la marque Milka. L'intimée se plaint pour sa part que Kraft a utilisé son prénom et cela lui cause préjudice. La Cour d'appel estime que l'utilisation par l'appelante de l'expression « milka » constitue une exploitation injustifiée de la marque sur laquelle Kraft possède un droit. Elle ordonne le transfert du nom de domaine « milka.fr ». Par ailleurs Kraft ne commet aucune faute en utilisant le nom qui s'avère être aussi le prénom de l'appelante. Le prénom ne confère pas un droit privatif opposable à l'encontre d'un titulaire de marque.

Milka B. c/ Kraft Foods Schweiz Holding AG, Cour d'appel de Versailles, 27 avril 2006.

À signaler

Anne COUSIN, *Internet au bureau : les leçons d'un jugement*, Journal du net, 3 mai 2006.

Cynthia CHASSIGNEUX, Pierre TRUDEL, Bartha Maria KNOPPERS, L'encadrement juridique du traitement informatisé des données relatives à la santé : perspective europeo-canadienne, GenEdit, 2006 - Volume IV, No.1.

Caroline VALLET, *La lutte contre la pédopornographie est déclarée : renforcement de l'article 227-23 du Code pénal*, Juriscom.net, 24 avril 2006.