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

April 14, 2005/14 avril 2005

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Anne Uteck and Teresa Scassa 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 Anne Uteck et Teresa Scassa 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.

Administrative Law

In *Keefe v. Clifton Corp.*, the Alberta Court of Appeal considered an appeal from a ruling that a by-law of the City of Edmonton was invalid due to a breach of procedural fairness. The by-law was the product of a process around a re-zoning application to allow the construction of a 5 storey apartment building. The area residents, who opposed the application had retained a transportation consultant from Vancouver. At a first hearing, the consultant presented arguments regarding the impact of the proposed change on traffic patterns, and challenged the analysis of the transportation department. The hearing was adjourned for two weeks. On the resumption of the hearing, Council members were to have an opportunity to pose questions, and parties would be given an opportunity to respond to new information.

The day before the hearing was to resume, the respondents learned that their consultant would not be able to attend due to an illness that would prevent him from flying. The respondents asked that he be allowed to participate by teleconference. Permission was denied. The by-law was ultimately passed by Council, and was then challenged on the basis that there was a breach of procedural fairness.

The Court noted that the City had passed a bylaw which permitted Council and Committees to conduct meetings "by means of electronic or other communication facilities under any procedures adopted by Council." City Policy and Procedure C470 also provided that "Any person may participate in a meeting of Council or a Committee using Communication Facilities" if a number of conditions are met. The conditions related to paying the cost of the use of the communication facility and giving adequate notice. The Court of Appeal upheld the decision of the trial judge that the failure of the Council to turn its attention to the issue of whether to allow telephone participation in the circumstances amounted to a breach of its duty of procedural fairness.

Constitutional Law

In the newsletter of November 11, 2004, we reported on the Quebec Provincial Court decision in *R. v. D'Argy*. In that case, Côté J. of the Quebec Superior Court ruled that s. 10(1)(*b*) of the *Radiocommunication Act* violated the guarantee of freedom of expression under s. 2(*b*) of the *Charter*, and could not be saved by s. 1. The case arose out of charges laid against two accused for possessing and selling cards and devices that would allow for the decoding of pay tv satellite signals. The signals in question were from a service provider located in the United States, DIRECTV. Section 9 (1)(*c*) of the *Act* prohibited the decoding of an encrypted subscription programming signal "otherwise than under and in accordance with an authorization from the lawful distributor of the signal or feed." Section 10(1)(*b*) makes it an offence to manufacture, import, distribute, lease, offer for sale, install, modify, operate or possess "any equipment or device, or any component thereof, under circumstances that give rise to a reasonable inference that the equipment, device or component has been used, or is or was intended to be used, for the purpose of contravening section 9."

The Crown appealed the decision, and on March 31, 2005, Décarie J. of the Quebec Superior Court overturned the decision of Côté J., and imposed convictions on the accused parties. Décarie J. noted that the trial judge had found that all of the elements of the offences had been proved by the Crown, and

that she would have imposed convictions had she not found that the provisions of the law violated s. 2(*b*) of the *Charter*. Décarie J. was of the view that because Côté J. had found that the respondents were engaged in illegal activities, and that they themselves could not avail themselves of s. 2(*b*) of the *Charter* with respect to their activities, she should not have gone on to consider whether the provisions of the *Radiocommunications Act* were, in the abstract, unconstitutional. He was critical of her decision to rule on matters without an appropriate factual basis. He was also critical of her finding that Canadian viewers who made false representations to the American service provider DirectTV did so as a result of the Canadian broadcast policy. He noted that in drawing this conclusion she ignored the fact that DirectTV did not have the necessary copyright clearances to broadcast its material in Canada. According to Décarie J., the activities of these viewers were a fraud against DirectTV, and against Canadian distributors who had paid for the Canadian distribution rights to much of the same content. Further, he noted that even if the law was unconstitutional, DirectTV could not be compelled to provide its service in Canada.

Privacy

Three recent decisions have been released by the federal Privacy Commissioner. In Finding #288, the complainant alleged that a telecommunications company required him to provide four pieces of identification to activate a cellular phone service, but it was later determined that three pieces of identification were required. The company stated that both bad debt costs and identity theft were major concerns, contending that the identification requirements are for the purpose of collecting an accurate and complete credit check and to ensure that the applicant is actually who he or she claims to be. The Assistant Privacy Commissioner disagreed that the Company's purposes could only be achieved with three pieces of identification. In her view, only two pieces of identification were needed by the company to achieve its objectives. For example, a picture identification with the date of birth in combination with a credit card or bank information meets the identity authentication and accurate credit information needs. Following previous findings involving telephone or wireless services, two pieces of identification for confirming creditworthiness and identity were considered reasonable. Therefore, the company was requiring more personal information than necessary contrary to Principle 4.4 and accordingly, the complaint was well-founded.

In Finding #289, a laptop computer in the custody of a bank financial planner/advisor containing the personal information of 960 bank clients was stolen from her locked vehicle while it was parked in her home's underground parking garage. A bank client made a complaint under *PIPEDA* that the bank failed to safeguard his personal information. The Bank had advised the complainant that the personal information on the laptop consisted of his name, address, telephone number and his mutual funds account number. The financial planner used this information to set up appointments and provide clients with information. The complainant indicated, however, that he did not have a financial advisor and had not sought the bank's advice and therefore did not understand why his information would be on a client contact list. According to the Bank, his information was included on the list of clients because one of his accounts met or exceeded a pre-set target and the account was not managed by a bank advisor. The complainant had received a privacy disclosure notice stating that if the client was not interested in receiving the direct marketing service, they could have their name removed from the bank's marketing lists. The complainant did not request that his name be removed.

With respect to the issue of inappropriate use of personal information, the Assistant Privacy Commissioner noted that the complainant's personal information was on the laptop because the Bank intended to market bank products and services to him. Since the complainant did not request his name be suppressed from the bank's marketing lists when given the opportunity to do so, according to the Assistant Privacy Commissioner, "it would appear that the bank had his implied consent to include his name on such a list." Therefore, the Bank was in accordance with Principle 4.5 and the complaint was not well-founded. However, the Assistant Commissioner concluded that the safeguarding complaint was well-founded. While the Bank had policies and procedures dealing with physical security that met the requirements of Principle

4.7, the financial planner, in this instance, had not followed them by leaving the laptop unattended on the seat of her vehicle. Therefore, the Bank was in contravention of Principle 4.7.

Finally, the Assistant Commissioner further considered the Bank's privacy policy, in particular, the requirement that the customer obtain and complete the appropriate form to have his or her name suppressed from the Bank's marketing lists. In previous complaints involving the issue of opt-out consent to use information for marketing purposes, the Privacy Commissioner's Office has found that an organization must provide for an immediate and convenient method for customers to opt-out. In this case, the Assistant Commissioner commented that "requiring a customer to fill out an application form did not meet the reasonable expectations of most individuals, namely, that an immediate, easy and inexpensive means of withdrawing consent to the optional collection, use and disclosure of their personal information must be provided."

The most recent Finding issued by the Privacy Commissioner's Office involves video surveillance cameras at a federally registered meat processing plant. An employee of the Canadian Food Inspection Agency (CFIA) complained that the meat processing plant was collecting personal information by video camera without his consent and had disclosed it to his employer. The CFIA oversees the meat inspection program at all federally registered facilities and appoints a Veterinarian in Charge at each facility. The Veterinarian works on site and is assisted by one or more lay inspectors. The complainant is the Veterinarian at the meat processing plant subject to this complaint.

The company installed 15 video cameras in 2001 located at entry and exit points and in all areas of the plant, including the evisceration room where CFIA employees have their workstations. The camera in the evisceration room captures the CFIA employees at their workstations. The company does not have policies or procedures governing the use of the cameras and did not consult with or inform CFIA employees prior to the installation. The cameras are motion-activated, record digitally on the hard drive and are used by the plant manager who has a monitor in his office. The company stated that the cameras are used for the purpose of addressing security concerns and to monitor hygiene, safety and product safety, as well as to enable the plant manager to respond quickly to problems at the plant site. There was some evidence to indicate that theft was an issue and thus, cameras could be useful for security purposes, but there were no examples provided of how cameras could help with product safety especially given that the cameras are unable to capture detailed images of the condition of the animal. The complainant had been told by the company that the cameras would not be used to observe him, but there were documented incidents where the company had disclosed information about the complainant, recorded by cameras, to his CFIA Supervisor and the company had shown CFIA managers videotape of the complainant's workstation to support the company's contention that the complainant was "overly zealous in his work." These incidents occurred prior to January 1, 2004 and there had been no subsequent use of videotape. As well, the CFIA wrote to the company informing them that it would not review video surveillance tapes "under any circumstances."

The findings by the Assistant Privacy Commissioner are limited to the collection of the CFIA employees' personal information by the video camera directly trained on their workstation in the evisceration room. The company cited product safety as the reason for installing a video camera at the CFIA employees' workstation. The Assistant Commissioner considered whether this purpose for installing video cameras was appropriate and met the reasonableness as delineated by the Office of the Privacy Commissioner in past complaints involving video surveillance. In assessing the reasonableness of the surveillance measure: (1) Is the camera demonstrably necessary to meet the specific need? (2) Is it likely to be effective in meeting that need? (3) Is the loss of privacy proportional to the benefit gained? and (4) Is the a less privacy-invasive way of achieving the same end?

While monitoring food safety appeared to be an appropriate purpose, the Assistant Privacy Commissioner "found it difficult to understand how having a camera in this area – a camera that cannot provide a clear picture of the animals – ensures product safety when the very people responsible for ensuring product safety are in the room, monitoring production." Therefore, in her view, video surveillance in the evisceration room is not

demonstrably necessary to ensure product safety and is not effective in meeting that need. She also noted that the federal inspectors were addressing product safety concerns, responsible for monitoring employee hygiene and if there was a need to deal quickly with a situation in the evisceration room, it could be accomplished in a much less privacy-invasive way by using one of the lead hands. There was, according to the Assistant Privacy Commissioner, "a clear loss of privacy for the complainant and the other CFIA inspectors with respect to the camera that is trained on their workstations." Personal information was being collected by the company without the complainant's consent, contrary to Principle 4.3 and for purposes not considered appropriate in the circumstances in accordance with subsection 5(3). She concluded, therefore, that the complaint was well-founded.

This conclusion was supported by some evidence that the company had attempted to use the information gathered by video camera to undermine the complainant's work, although these incidents occurred before the company became subject to *PIPEDA*. The Assistant Commissioner determined that the federal Privacy Commissioner's Office did not have jurisdiction to issue a finding with respect to the disclosure of the complainant's personal information collected by videotape because the events in question took place prior to the full implementation of the *Act*.

Finally, the Assistant Commissioner recommended that the company remove the video camera from the evisceration room. Because there are cameras located in other areas of the facility that may inadvertently collect personal information, she further cautioned the company that it could only use the personal information of employees that it inadvertently collected without their consent in accordance with *PIPEDA* subsections 7(2)(a) and (b).

2ième partie

Diffusion de photos sur Internet – Injonction

Boyer tombe éperduement amoureux d'une croupière du Casino de Montréal, qui elle ne partage pas ses sentiments. Il persiste dans son harcèlement, si bien que la croupière dépose une plainte au criminel en 1994. Pour sa remise en liberté, il signe un engagement de s'abstenir de communiquer avec elle. Cependant, il récidive, est accusé de bris d'engagement et écope d'un sursis de sentence, assorti d'un engagement similaire au premier dans le cadre d'une probation. En 1996, et ce avant la fin de sa probation, Boyer se présente au Casino à la table de jeu où travaille la croupière; une autre plainte est portée contre lui et il est condamné à une amende. En 1999, il est à nouveau accusé de harcèlement contre la croupière et de voies de fait à l'endroit d'une employée du Casino. Il est trouvé coupable et on lui interdit, entre autres, de produire ou de gérer des sites Internet traitant des casinos du Québec.

Sous prétexte de se défendre des accusations en cour criminelle, Boyer obtient, avec l'autorisation de la Commission d'accès à l'information, la bande vidéo de la caméra de surveillance du Casino qui a enregistré la croupière au travail lors de l'incident de 1996. Au lieu de se servir de l'enregistrement pour se défendre au criminel, il a diffusé des extraits et des photos sur ses sites Internet sans autorisation et malgré les conditions ordonnées par la Cour.

Le tribunal ordonne à Boyer de cesser de porter atteinte au droit à la vie privée de la croupière. Les droits propres à la protection de la vie privée, dont l'image fait partie, peuvent être violés même si l'image publiée n'a aucun caractère répréhensible et n'a aucunement porté atteinte à la réputation de la personne. À plus forte raison, en l'espèce, puisque la photo a été publiée plusieurs fois sur un site qui peut être relié à un site érotique. De plus, la publication de la photo n'était pas dans l'intérêt public. Quoique le tribunal ne soit pas convaincu que la bande vidéo constitue une œuvre protégée par le droit d'auteur, son contenu n'en demeure pas moins la propriété du Casino, et Boyer doit lui remettre toute copie pour fins de destruction.

Société des casinos du Québec c. Boyer, 2005 IIJCan 7808 (QC C.S.), 500-05-062084-007, 2 mars 2005.

Sur les règles applicables en matière de protection de l'image diffusée sur Internet en France, voir Philippe BELLOIR, *La protection de l'image publiée sur Internet – À propos de l'arrêt de la Cour d'appel de Lyon du 27 janvier 2005 FathiaX…c/SA Société G…*, Juriscom.net, 11 avril 2005.

Utilisation de la vidéosurveillance avec enregistrement dans les lieux publics

La Commission d'accès à l'information (CAI) a rendu public son rapport d'enquête concernant l'installation de caméras de surveillance dans le quartier latin par le Service de police de la ville de Montréal (SPVM). Le rapport conclut que l'utilisation de caméras de surveillance n'est pas justifiée considérant les règles élaborées sur le sujet par la CAI.

La Commission s'interroge sur la nécessité d'installer des caméras pour réduire le nombre d'infractions relatives aux stupéfiants, alors que ce type d'infractions est considéré en régression grâce à des opérations policières antérieures. La Commission n'a pas pu constater que l'organisme a examiné des solutions alternatives à l'utilisation de caméras, moins invasives de la vie privée. De plus, certaines règles entourant l'utilisation des caméras de surveillance n'ont pas été suivies (images enregistrées 24 heures sur 24 et conservées plus longtemps que prévu; information inappropriée et incomplète du public visé par la surveillance; l'une des caméras était dirigée vers un endroit inapproprié; rien n'indique que les personnes qui assurent le fonctionnement des appareils étaient au fait des règles visant à protéger la vie privée; le processus d'évaluation de l'utilisation de caméras et de ses effets est imprécis et n'est pas confié à un tiers indépendant).

La CAI rappelle que tout projet d'utilisation de caméras de surveillance avec enregistrement doit respecter *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, 9 juin 2004.

Laurent BILODEAU, *Rapport final d'enquête concernant l'installation de caméras de surveillance par le Service de police de la ville de Montréal*, 23 février 2005, http://www.cai.gouv.qc.ca.

Diversité culturelle – Projet de convention de l'UNESCO

L'Union européenne de radiodiffusion (UE) a publié une note d'information concernant le projet de Convention de l'UNESCO sur la diversité culturelle. Adoptée par le Groupe Europe le 1er février 2005, la Note d'information énonce les principes sur lesquels se fondent les positions de l'organisme, notamment dans le cadre de la seconde réunion intergouvernementale de l'UNESCO sur le projet de Convention, qui s'est tenue à Paris du 31 janvier au 12 février 2005. On y souligne la nécessité:

- de clarifier la légitimité des politiques nationales destinées à préserver et promouvoir la diversité culturelle et le pluralisme des médias;
- de reconnaître l'important rôle des institutions de service public, en particulier des organismes de radiodiffusion publics;
- de sauvegarder la liberté et le pluralisme des médias;
- de clarifier la relation avec le droit commercial international afin que la gouvernance internationale gagne en cohérence.

UNESCO, *Projet de Convention sur la diversité culturelle*, Note d'information de l'UER.

À signaler

Thibault VERBIEST, *Vie privée et santé : le dossier médical personnel fait son chemin en France*, Droit & Nouvelles technologies, 6 avril 2005.

Iliana BOUBEKEUR, *Une entreprise peut se voir attribuer la qualité de fournisseur d'accès à l'Internet*, Juriscom.net, 4 avril 2005.

Philippe AMBLARD, *Régulation de l'Internet- L'élaboration des règles de conduite par le dialogue internormatif*, Bruxelles, Cahiers du Centre de recherches informatique et droit (CRID), Bruylant, 2004.