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

October 23, 2009/23 octobre 2009

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

Criminal Law and Privacy: "Search Incidental to Arrest"

The Alberta Court of Queen's Bench has delivered its decision in *R v. Franco*. Two Edmonton City Police Officers were conducting "moving radar" speed operation on a freeway in Edmonton. A vehicle, an Acura, driven by the accused passed the officers while going at a significantly excess speed. The officers stopped the vehicle, and demanded the accused's driver's licence, insurance and registration. The accused gave them the last two documents but indicated that he did not have his driver's licence with him, having left his wallet at home. He was then asked to identify himself with a warning that if he lied, he would be charged with obstructing a peace officer. The driver gave a name and a birth date among other information and pointed out that the vehicle belonged to his girl friend whose phone number he supplied to the officers. He also indicated that he has no tattoos. One of the officers searched the name given by the accused in the driver's licence registry using a laptop computer in his patrol vehicle. There was no record by that name. Another officer went back to the car to confirm the name from the accused, which the latter restated. Using a digital camera, at this point, the officer took a picture of the driver so as to facilitate a proof in court that the accused was the person who gave the false information. One of the officers now called the accused's girl friend via the phone number he supplied. She was found to be the owner of the vehicle as claimed by the accused. She confirmed that her boyfriend had the vehicle with her permission. She identified her boyfriend by a name and birth date different from the ones claimed by the accused. In providing his physical description, she indicated that her boyfriend had a dragon tattoo on his right arm. The officer conducted a computer search of drivers' licence registry using the name supplied by the girl friend and it showed that the license in that name was suspended. Consequently, the accused was arrested for driving while suspended and for obstruction of a peace officer. The officer then went to the vehicle to conduct a search incidental to arrest. Among other things, he unlocked the glove box and found a bag of substance believed and later confirmed to be cocaine for which the driver was re-arrested and charged. After that, he was advised of his charter rights for the first time. Subsequently, the officer prepared information to obtain a search warrant which was issued. The resulting search yielded four additional packages that were later confirmed to be cocaine. The accused's girl friend testified and disclaimed any knowledge or involvement in relation to the cocaine found in her car.

In a *voir dire* regarding the Charter issues, the Crown witnesses comprised the two police officers who dealt with the accused. The accused claims that his charter rights under s.8 dealing (security against unreasonable search and seizure) were violated by the officers. He argues that the first instalment of cocaine found in the vehicle should be expunged from evidence pursuant to s. 24(2) of the Charter. In that regard, he further argues that the information regarding that first instalment of cocaine should be expunged from the information to obtain search warrant with a consequence that the information to obtain would no longer, then, reveal reasonable and probable ground justifying the grant of a search warrant.

In reviewing the evidence and defence submission, the court held that the conduct of the officers regarding the search met the objective and subjective elements required for search incidental to arrest. The court noted that given the false representations of the accused, the issue of photo identification became imperative to remove any doubts. In responding to counsel's argument that since the car was impounded, there was no urgency in conducting further search as the police did without a warrant, the court held: "The absence of urgency might be relevant for the assessment of whether the search was subjectively and objectively reasonable, but I do not understand urgency to be an essential precondition to a valid search incidental to arrest ... it is reasonable [for the officer] though there was no urgency to conduct what would be very simple search of a place in respect of which there was little expectation of privacy, especially for the driver, who had acknowledged he did not own the vehicle" (para 27). The court found that the search was conducted within the officer's common law authority to conduct a search incidental to arrest and that the search warrant was justified on the basis of valid information to obtain.

Criminal Law and Sentencing: Sophisticated Sexual Harassment

The Alberta Court of Appeal has delivered its decision in the application by the Crown for leave to appeal in *R v. Wenc*. The accused and the victim met online in 2002 and subsequently got involved in sexual relationship until the victim terminated the relationship the following year. Following the termination, the accused embarked on a prolonged and elaborate scheme of sexual harassment and threats which did not abate until he was arrested in 2005. Pursuant to this scheme of sexual harassment, the accused used more than 20 aliases to conceal his identity while he contacted the victim through sexually suggestive e-mails, text and voice messages. Many of these were obscene and contained sexually explicit comments. The accused sent several e-mails and threatened therein to send naked pictures of the victim to other parts of Canada to reach the victim's relatives who lived there. Not done, the accused posted fake profiles of his victim in social-networking websites some which not only included the nude pictures of the victim and his phone number but also claimed, albeit falsely, that the victim was HIV positive. The accused also impersonated the victim in internet chat rooms and invited strangers to the victim's house with expectation of sexual encounters. Arising from this experience, the victim became fearful for his safety and life. He left Calgary for Toronto hoping that the harassment would cease but it did not. He returned to Calgary. When confronted by the police, the accused denied being involved in the harassment of the victim and was advised by the police stay away from the victim.

Through the victim's own painstaking investigations, he was able to link the accused to the crime. The victim kept copies of e-mails and website materials he received, tracked the telephone calls, and discovered that some of them originated from the accused's home and cell phones, while others were made from pay phones in the areas near where the accused lived. The victim obtained software that enabled him to track e-mail messages sent to him. The device traced the messages to a computer at the company where the accused worked. The accused gave the police this and additional but significant amount of documented information that enabled the police to conduct investigation at the accused's work place and his residence. In the work place, it was discovered that the accused was the only person with access to the computer used to post a number of the e-mails under several aliases. After the accused was arrested, the harassment stopped. The accused was charged and the matter pended in the court for three years before it was disposed of through a guilty plea by the accused.

The accused was sentenced to 90 days imprisonment which was to be served intermittently. He was also bound by a probation order for the term of the imprisonment. In the present application for leave to appeal the sentence, the Crown argues, inter alia, that the sentence did not suit the gravity of the offence, that it was demonstrably unfit and that the judge did not consider the domestic nature of the relationship and the aggravating circumstance. In its ruling, court of appeal held that the "sentence should be accorded deference and should not be altered unless it is clearly unreasonable, in that wrong principles were applied or the sentence imposed falls outside the acceptable range of sentences" (para 22). The

court observed that given the range, duration and sophisticated nature of the harassment, "the sentence imposed here is not within the appropriate range" (para. 39). It found that the appropriate range of sentence would be 12 months. However, the court noted that given the chequered trajectory of the case, "the reality is that the restriction to Wenc's liberty has been piecemeal and spread over a significant period ... Were we to impose a further imprisonment now, we would be returning Wenc to gaol for yet another short segment ... we are not persuaded that further imprisonment is warranted, and decline to grant the Crown's leave to appeal" (para 40).

Criminal Law: Reasonable Expectation of Privacy in ISP Subscriber Information

In *R. v. Cuttell*, L.C. Pringle J. of the Ontario Court of Justice heard a motion to exclude evidence in a trial relating to possession and sharing of child pornography. Over the course of several months in 2007, a detective with the Toronto Police Service's Sex Crimes Unit had identified several IP addresses with shared folders containing child pornography. In each case he was able to ascertain that Bell Canada was the ISP, and faxed a request to Bell asking for the subscriber information attached to the IP address. In each case, Bell provided the name and address of the accused, pursuant to an interesting process which was described by a witness from the company:

> The "Letters of Request" sent to Bell Canada by Detective Purchas were on a form drafted by Bell to be used by police in child sexual exploitation investigations. According to a Bell employee Leslie Costa who testified before me, Bell will only provide subscriber information to police in child exploitation investigations and will not provide it for fraud cases, copyright cases or anything else. Accordingly, the letter (sometimes referred to as a "Law Enforcement Request" or LER), states that the police are investigating a child sexual exploitation offence, and specifies that they are requesting the disclosure in accordance with the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*] and the *Police Act.* The form letter has a space to add the IP address, the date and time under investigation, and asks for the last known customer name and address of the account holder for that IP address. It goes on to say, "Should you agree to this request, please ... fax the information to Detective Purchas ...." (para. 8).

The witness noted that despite Bell's position that subscriber information was private, the company had made a decision to comply with requests under s. 7(3)(c.1) of *PIPEDA* from police in child sexual exploitation cases, without a warrant and "for the limited purpose of providing subscriber information linked to an IP address at a particular date and time" (para. 9). The police eventually received a warrant to search the accused's home and seized a computer and CDs containing numerous images and videos. At trial, the accused made a motion to exclude the evidence as having been seized in violation of section 8 of the *Charter*.

Justice Pringle first examined whether there was a reasonable expectation of privacy in the name attached to an IP address. She held that there was, on the basis that "the information discloses intimate details of a subscriber's lifestyle and choices" (para. 21), and noted that this was clearly the case here. In response to a Crown argument that the accused could have had no reasonable expectation of privacy given that both the IP address and the items seized were in the public domain, she noted that none of the publicly-available material had any link to the accused until the subscriber information provided the link, and invoked a statement by the Privacy Commissioner of Canada that "a subscriber's name and address can be a critical link between the subscriber and very private information" (para. 24). Some earlier caselaw was invoked as authority for the proposition that a contract between the ISP and a subscriber may have wording in it that diminished the reasonable expectation of privacy, for example a provision indicating that the ISP would respond to some police requests. While Justice Pringle agreed with this in principle, there was no evidence as to the agreement between Bell and the accused, and thus the finding of reasonable expectation of privacy had to stand.

Justice Pringle also rejected the Crown's argument (which has been the subject of controversy in other cases) that s. 7(3)(c.1) of *PIPEDA* creates a police search power, holding that it simply

authorizes disclosure of private information where the requesting government authority has lawful authority to make the request. She further held that such "lawful authority" does not stem from *PIPEDA* itself, or from the police's common law search power, or from the mere existence of reasonable and probable grounds, in the absence of a warrant. Also rejected was the argument that the involvement of a third party vitiated the reasonable expectation of privacy, given that Canadian caselaw has consistently protected the privacy of individuals vis-à-vis the state even where the information has been exposed to a third party.

Turning to whether the evidence should be excluded under s. 24(2) of the *Charter*, Justice Pringle held that it should not. She noted the police acted reasonably in assuming they did not need a warrant for the request to Bell, given the division among the Ontario courts and the fact that the balance of the caselaw supported this stance. Moreover: the subscriber information itself did not have much intrinsic privacy, the request was not overly intrusive; and the evidence was essential for adjudication on the merits of the case. Accordingly, the evidence was ruled admissible. In a parting comment, Pringle J. noted that most cases will be decided by way of the contract between ISP and customer, and stated:

> [This] means the police will be the ones to decide if there are grounds to believe a crime has been committed before making a request, and it will be left to ISPs to decide if they wish to comply with the police request for subscriber information. In short, it means that the safeguard of an independent judicial arbiter will no longer be available to assess, in advance, whether the individual's right to privacy should give way to the law enforcement goals of the state (para. 80).

National Security: Interception of Electronic Communications Originating Outside Canada

In *Canadian Security Intelligence Service Act (Re)*, Justice Mosley of the Federal Court gave his (redacted) reasons for granting applications by the Canadian Security Intelligence Service (CSIS) for warrants authorizing the interception of communications and collecting information obtained abroad. CSIS was investigating two Canadian nationals who, it suspected, were engaged in activities *outside Canada* that would threaten Canadian national security. In an earlier decision, Blanchard J. of the same court had refused similar applications, holding that the proposed activities would violate the presumption against the exercise of enforcement jurisdiction outside Canada which was set out by the Supreme Court of Canada in *R. v. Hape*. Renewing the application, the Attorney General of Canada argued, on behalf of CSIS, that while the communications and information themselves would be originating from outside Canada, all of the activities required to intercept and monitor the communications and obtain the information would be conducted and controlled entirely within Canada. Accordingly, there was no extraterritoriality engaged.

Justice Mosley concluded that most of the interceptions were permissible in that they were taking place within Canada. However, he had more concern about a particular set of interceptions. While it is unclear because of the redactions to the Court's reasons, it appears that CSIS was seeking authorization to technically intercept some cell phone communications within Canada, but the listening to the calls and information-gathering would be done abroad, and that some violation of the foreign law would be engaged. Certainly the issue was with regard to "investigative measures having an extraterritorial effect" (para. 67).

Mosley J. noted that international law prohibits one state from enforcing its jurisdiction upon the territory of another state, but that because of the free flow of information and individuals across borders there was a great deal of cooperation and comity between states in investigation, of which the European Cybercrime Convention (which Canada has signed but not yet ratified) was an example. Ultimately he distinguished between the exercise of enforcement jurisdiction and simple information-gathering, stating: "The norms of territorial sovereignty do not preclude the collection of information by one nation in the territory of another, in contrast to the exercise of its enforcement jurisdiction… technological innovation has simply made it easier to do this without physically crossing borders" (para. 74).

In this case, CSIS was receiving technical assistance from the Canadian Communications Security Establishment (CSE), which had a legislative mandate to gather information from communications and information technology systems and networks abroad. CSIS, for its part, was authorized to investigate individuals via legislation that had no geographical limitation upon the investigative activities. Accordingly, Justice Mosley ruled that "Where the statutory prerequisites of a warrant are met, including prior judicial review, reasonable grounds and particularization of the targets, the collection of information…, as proposed, falls within the legislative scheme approved by Parliament and does not offend the *Charter*" (para. 76).

2ième partie

Validité d'un avis de réclamation transmis par l'intermédiaire d'un site Internet d'une ville

Mme Deschênes réclame à la ville de Montréal la somme de 756,23 $ pour des dommages à sa voiture suite à un remorquage dans le cadre d'une opération de déneigement. Le 5 janvier 2009, à l'intérieur du délai de quinze jours prévu à l'article 585(2) de la *Loi sur les cités et villes* (L.R.Q., c. C-19), Mme Deschênes transmet à la ville de Montréal un avis de son « intention d'intenter une poursuite ». Cet avis est transmis par l'intermédiaire d'un site internet de la ville de Montréal sur lequel apparaît, notamment, une invitation à lui adresser « vos commentaires, questions, requêtes ou plaintes concernant les activités et les services de la Ville et de ses arrondissements. » Le 11 janvier 2009, une représentante du « Bureau Accès Montréal virtuel » accuse réception du courriel de Mme Deschênes et l'informe de la disponibilité du formulaire de réclamation via le site internet de la ville de Montréal. Suite à cette réponse, Mme Deschênes transmet sans délai un avis de réclamation selon le formulaire approprié. La ville de Montréal présente alors une requête en irrecevabilité fondée sur l'article 585(2) de la *Loi sur les cités et villes.*

Le tribunal rejette la requête en irrecevabilité de la ville et conclut que l'avis du 5 janvier transmis par Mme Deschênes à la ville de Montréal constitue un « Avis de réclamation » au sens de l'article 585 (2) de la *Loi sur les cités et villes*. En effet, pour le tribunal, il serait injuste de priver Mme Deschênes de son droit de poursuivre la ville de Montréal alors qu'elle a expédié, le 5 janvier 2009, un courriel à la ville faisant part des dommages causés à sa voiture, même si ce courriel faisait suite à une invitation de la ville de Montréal à lui adresser « vos commentaires, questions, requêtes ou plaintes». Mme Deschênes n'a peut-être pas transmis son avis de réclamation sur le bon bureau du fonctionnaire qui doit recevoir de tels avis mais la preuve démontre clairement qu'à l'intérieur du délai prévu par la loi, la ville de Montréal a reçu l'avis de réclamation de Mme Deschênes. La personne qui a reçu le courriel de Mme Deschênes le 5 janvier 2009 aurait pu l'aviser sans délai de la possibilité de remplir le formulaire approprié et de le transmettre à la bonne adresse courriel au lieu d'attendre jusqu'au 11 janvier 2009.

- *Deschênes c. Montréal (Ville de)*, 2009 QCCq 10115, 16 octobre 2009, SOQUIJ AZ-50580184.

Protection des enfants et nouvel environnement de l'information et de la communication – Conseil de l'europe

La protection de la liberté d'expression et de la dignité humaine dans l'environnement de l'information et de la communication, tout en assurant la protection des mineurs contre les contenus préjudiciables et le développement de leur capacité dans le domaine de l'éducation aux médias, est une priorité pour le Conseil de l'Europe. Le Comité des Ministres recommande aux États membres, en coopération avec les acteurs du secteur privé et la société civile, de développer et de promouvoir des stratégies cohérentes de protection des enfants contre des contenus et des comportements présentant des effets préjudiciables tout en préconisant leur participation active avec la meilleure utilisation possible du nouvel environnement de l'information et de la communication.

Il recommande d'encourager le développement et l'utilisation d'espaces sûrs (« jardins clos ») et d'autres outils facilitant l'accès à des sites et à du contenu en ligne adaptés aux enfants; de promouvoir la progression et l'utilisation volontaire de labels (ex : label paneuropéen) et de certifications permettant aux parents et aux enfants de distinguer aisément les contenus non préjudiciables de ceux qui présentent un risque d'effets préjudiciables; de promouvoir l'acquisition chez les enfants, les parents et les éducateurs de compétences leur permettant de mieux comprendre et manier les contenus et comportements qui présentent un risque d'effets préjudiciables. Des lignes directrices sur ces questions sont jointes à la recommandation à l'attention de toutes les parties prenantes concernées des secteurs privé et public.

- Conseil de l'Europe, *Recommandation CM/Rec(2009)5 du Comité des Ministres aux États membres visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication*, (adopté par le Comité des Ministre le 8 juillet 2009 lors de la 1063e réunion des Délégués des Ministres).

Conséquences de la livraison tardive d'un bien en exécution d'un contrat de commerce électronique – France

Les retards de livraison constituent le principal motif des plaintes concernant les achats sur Internet. Face à l'inexécution par un cocontractant de son obligation de délivrance, plusieurs actions sont envisageables : la demande de résolution judiciaire du contrat ou l'assignation en exécution forcée et l'action en responsabilité afin d'obtenir des dommages intérêts. Il convient de distinguer entre les recours ayant une conséquence directe sur le contrat, telle que la résolution, de ceux qui n'ont de conséquences que sur le cybervendeur, comme la mise en œuvre de sa responsabilité. En droit français, le droit commun ne prévoit pas de régime spécifique au vecteur électronique pour le cas de la livraison tardive d'un bien en exécution d'un contrat de commerce électronique. Des dispositions ont toutefois été introduites pour la vente à distance dans le *Code de la consommation*.

- Matthieu VETTER, « Les conséquences de la livraison tardive d'un bien en exécution d'un contrat de commerce électronique », *Juriscom.net*, 16 octobre 2009.

Le système Google AdWords enfreint-il le droit des marques? – Cour de justice des Communautés européennes

La Cour de justice des Communautés européennes a été saisie par la Cour de cassation française de questions préjudicielles tendant notamment à savoir si l'utilisation d'un mot-clef correspondant à une marque doit être considérée comme un usage de cette marque, exposant ainsi l'utilisateur au délit de contrefaçon s'il n'a pas obtenu l'autorisation du titulaire de la marque pour une telle utilisation. Dans le cadre des questions préjudicielles qui lui ont été posées, la Cour de justice des Communautés européennes sera ainsi amenée à se prononcer sur la légalité de l'usage des mots-clefs par la société Google dans son système de publicité AdWords. L'avis rendu par l'Avocat Général plaide qu'il n'y a pas lieu d'étendre la portée de la protection conférée par le droit des marques aux agissements des parties tendant à faciliter des atteintes aux marques commises par des tiers. Lorsque la société Google propose son système de publicité AdWords, que ce soit au stade de la sélection des mots-clefs ou de l'affichage des annonces, à des annonceurs qui l'utilisent pour porter atteinte à des marques, la société Google n'est pas contrefacteur mais elle pourra voir sa responsabilité civile délictuelle engagée, au cas par cas. L'avis de l'Avocat Général ne s'impose pas à la Cour de Justice des Communautés Européennes, seule habilitée à répondre aux questions préjudicielles de la Cour de cassation française. L'avis de l'Avocat Général analyse en détail les aspects notamment juridiques du litige et propose en toute indépendance à la Cour de Justice la réponse qu'il estime devoir être apportée au problème posé.

- Vincent POLLARD, « Le moteur de recherche Google et le système de publicité Google AdWords n'enfreignent pas le droit des marques », *Juriscom.net*, 23 septembre 2009.
- *Conclusions de l'avocat Général Luis Miguel Poiares Pessoa Maduro présentées le 22 septembre 2009, Affaires C-236/08, C-237/08 et C-238/08*.

Réflexion sur un marché unique du numérique pour les contenus créatifs en ligne – Commission européenne

La Commission européenne a publié le 22 octobre un document de réflexion sur les difficultés à créer un marché unique européen du numérique pour les contenus créatifs en ligne tels que les livres, la musique, les films ou les jeux vidéo. Les

études de la Commission tendent à montrer qu'un véritable marché unique sans frontières pour les contenus créatifs en ligne pourrait permettre une multiplication par quatre des recettes de détail du secteur des contenus créatifs à condition que les professionnels du secteur et les pouvoirs publics prennent des mesures favorables au consommateur. L'offre de contenus au format numérique ouvre donc de grandes possibilités pour l'Europe, mais elle ne va pas sans poser de nombreux problèmes. La distribution des produits et des services culturels continue de se heurter à des obstacles d'ordre réglementaire et géographique susceptibles d'entraver la créativité et l'innovation. En outre, le téléchargement illégal à grande échelle est de nature à compromettre le développement d'un marché unique du numérique économiquement viable, et il convient d'inciter davantage aux offres transnationales légales. Dans ce contexte, le document de réflexion met en évidence les questions qui se posent pour trois catégories de parties prenantes: les titulaires de droits d'auteur, les consommateurs et les utilisateurs commerciaux. Ce document invite toute personne intéressée à participer à un grand débat au sujet des réponses communautaires que l'on pourrait y apporter. Les commentaires peuvent être adressés d'ici au 5 janvier 2010.

- COMMISSION EUROPÉENNE, « Consultation publique sur «les contenus en ligne », Octobre 2009.
- Document de réflexion : *Creative Content in a European Digital Single Market: Challenges for the Future (Contenus créatifs dans un marché unique européen du numérique: les défis à relever)*, disponible à http://ec.europa.eu/avpolicy/other_actions/content_online/index_fr.htm

Appel de partenaires majeurs pour la création de nouvelles plateformes de licence comprenant les répertoires de plusieurs sociétés de gestion des droits d'auteur – Commission européenne

Les sociétés de gestion des droits d'auteur, les labels, les magasins de musique en ligne, les groupes de consommateurs et les fabricants se sont mis d'accord sur une déclaration commune appelant à mener à bien la création de nouvelles plateformes de licence comprenant les répertoires de plusieurs sociétés de gestion des droits d'auteur. L'accord est de nature à favoriser le renouveau d'artistes nationaux en facilitant les téléchargements licites et moins coûteux. Élaboré par la commissaire de la concurrence, l'accord est sujet à des négociations plus poussées afin de régler différentes modalités d'application.

L'accord vise l'établissement d'un portail commun facultatif et non exclusif pour inclure le répertoire le plus large possible. Une telle approche permettra aux magasins de musique en ligne, tels qu'iTunes ou Amazon, d'accéder aux œuvres et CD des artistes européens sans être confrontés aux législations nationales et sans se retrouver en conflit avec les sociétés de gestion des droits d'auteur. À ce jour, les règles fragmentées ont eu tendance à limiter les offres et à une différenciation de prix en fonction des pays d'origine des internautes. Ces règles auraient même empêché l'achat de la musique dans les boutiques en ligne enregistrées dans d'autres pays européens. Les sociétés de gestion des droits d'auteurs françaises, italiennes, espagnoles et scandinaves ont annoncé leur intention de créer un répertoire commun pour dynamiser les offres de musique en ligne. Pour sa part, la société anglaise PRS for music a annoncé qu'il y aurait certainement plus d'un répertoire commun.

Les labels majeurs comme Universal ou EMI pourront mettre leurs catalogues sur le portail commun ou bien les vendre directement aux circuits de commercialisation au détail. La société EMI a déjà annoncé qu'elle signerait bientôt un accord de non

exclusivité avec les sociétés de gestion des droits d'auteur françaises et espagnoles.

On estime aussi que l'accord devrait aider à combattre le piratage. L'élargissement des répertoires et la simplification des procédures pourraient réduire les coûts et encourager des baisses de prix qui pourraient inciter à choisir des moyens légaux de téléchargement.

- *Concurrence : la table ronde en ligne sur la musique organisée par la Commission ouvre la voie à une amélioration des possibilités de musique en ligne pour les consommateurs européens*, 20 octobre 2009, Europa Press release IP/09/1548.
- *EurActive.com*, « Accord européen sur la musique en ligne, un défi pour les grands labels », 22 octobre 2009.
- *Joint statement from the Online Commerce Roundtable participants on « General principles for the online distribution of music »*, 19 octobre 2009.

Appel à l'intensification de la lutte contre le spam et à la meilleure protection de la vie privée des internautes – Commission européenne

La Commission européenne a de nouveau appelé les pays de l'UE à lutter de manière plus déterminée contre les menaces qui pèsent sur la vie privée des internautes. Une étude financée par la Commission, publiée le 8 octobre, a montré que si plusieurs pays de l'UE ont pris ces dernières années des mesures pour que l'interdiction du spam soit respectée, notamment en imposant des amendes aux spammeurs, le nombre de poursuites et le montant des sanctions varient considérablement selon les pays. L'étude confirme l'importance des améliorations législatives proposées dans le cadre de la réforme des règles communautaires en matière de télécommunications: des règles d'application plus claires et plus cohérentes et des sanctions dissuasives, une meilleure coopération transfrontalière et des ressources suffisantes pour les autorités nationales chargées de protéger la vie privée des citoyens en ligne.

Au nombre des principales conclusions de l'étude, l'on relève que presque tous les pays de l'UE disposent désormais d'un ou plusieurs sites web où les citoyens peuvent trouver des informations ou se plaindre s'ils sont victimes de spam ou de logiciels espions ou malveillants.

L'analyse de plus de 140 cas de poursuites dans 22 pays de l'UE a fait apparaître des différences considérables dans le nombre de poursuites par pays et dans les sanctions imposées. Les poursuites les plus nombreuses ont été engagées en Espagne (39 cas), en Slovaquie (39 cas) et en Roumanie (20 cas). Les sanctions financières les plus élevées ont été appliquées aux Pays-Bas (1 000 000 €), en Italie (570 000 €) et en Espagne (30 000 €). En revanche, dans certains pays tels que la Roumanie, l'Irlande et la Lettonie, les spammeurs ont été condamnés à des amendes légères allant de quelques centaines à quelques milliers d'euros.

Une lutte efficace contre les menaces en ligne suppose de combiner prévention, répression et sensibilisation. Les autorités publiques (notamment les autorités de régulation des télécoms, les institutions chargées de la protection des données et de la défense des consommateurs, ainsi que les autorités policières) doivent se voir confier un mandat clair et mettre en place des procédures de coopération bien définies. En outre, le secteur public et le secteur privé doivent également coopérer. Le degré de coopération diffère fortement selon les pays de l'UE. De tels accords ont été conclus en Allemagne, en Belgique, à Chypre, en Estonie, en France, en Italie, en Lettonie, en Lituanie, aux Pays-Bas, en Roumanie et au Royaume-Uni, tandis qu'à Luxembourg et à Malte, par exemple, la coopération est informelle.

Le spam est un problème mondial. Une coopération internationale plus étroite, tant au niveau communautaire qu'international, est nécessaire pour lutter efficacement contre le spam. Mais les pays de l'UE devraient doter les autorités nationales de ressources suffisantes pour recueillir des preuves, mener des enquêtes et engager des poursuites dans ce domaine.

- *La lutte contre le spam doit s'intensifier et la vie privée des internautes doit être mieux protégée, constate un rapport de la Commission*, 8 octobre 2009, Europa Press release IP/09/1487.

- *Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software*, SMART 2008/ 0013, october 2009.

La télévision à l'ère d'Internet

Le livre ne traite pas des dimensions juridiques mais documente dans un style accessible les transformations du modèle de la télévision en raison des nouvelles technologies et de l'usage généralisé d'Internet. Le contexte technologique contemporain fait en sorte que tout le monde peut devenir producteur. En utilisant son téléphone photographique, un caméscope, un magnétophone miniature et en combinant le tout avec les environnements Internet comme les blogues et les réseaux sociaux, il devient facile de faire de la télévision. Mais l'auteur constate que la télévision demeure un média important qui se conjugue désormais au je, une sorte de confessionnal à aires ouvertes où l'on raconte son histoire, où l'auditoire veut qu'on lui fasse voir le vrai et l'authentique.

- Jean-Paul LAFRANCE, *La télévision à l'ère d'Internet*, Montréal, Septentrion, 2009, 217 p.

Les infractions commises sur Internet

Ce livre s'attache à découvrir un sens au traitement juridique de la cybercriminalité. On remonte aux sources conceptuelles dont prétendent s'inspirer les internautes – la philosophie du 'partage' - qui pourrait faire de la toile une zone de non-droit. L'ouvrage fait le point sur les concepts de la cybercriminalité. Il expose les principes juridiques relatifs à la criminalité de la communication comme les atteintes au réseau de même que sur la criminalité par la communication comme les menaces et les gestes qui accentuent la vulnérabilité des victimes. L'intérêt de la démarche tient notamment au fait que l'auteur prend la peine d'expliquer en quoi les gestes posés sur Internet sont de nature à intensifier les risques pour les usagers ou pour certaines personnes vulnérables comme les enfants.

- Abbas JABER, *Les infractions commises sur Internet*, Paris, l'Harmattan, 2009, 315 p.

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.