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

April 29, 2004/29 avril 2004

IT.Can NEWSLETTER/BULLETIN

Canadian IT Law Association

www.it-can.ca

Part 1 of this newsletter is prepared by Professors Michael Deturbide, Anne Mussett and Teresa Scassa of the Law and Technology Institute of Dalhousie Law School. Part 2 of this newsletter is prepared by Professor 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 Michael Deturbide, Anne Mussett 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.

Part 1

Criminal Law

Bill C-14, which, among other things, amends the *Criminal Code* and the *Financial Administration Act* to permit the use of intrusion detection systems for the protection of computer systems from harmful electronic communications such as viruses, received Royal Assent on April 22. Most of the provisions of the Bill came into force upon Royal Assent.

The Bill amends the *Criminal Code* to include s. 184(2)(e), which allows a person in possession or control of a computer system to intercept a private communication if the interception is reasonably necessary for managing the quality of service of the computer system, including the integrity and availability of the system and data, or protecting the computer system against any act that would be an offence under s. 342.1(1) or 430(1.1) (the so-called "hacking" and mischief to data provisions). Such interception can be used or retained only if it is essential to identify, isolate or prevent harm to the computer system, or for law enforcement reasons.

The Bill also adds s. 161 to the *Financial Administration Act*, which authorizes persons who perform duties relating to the management or protection of computer systems of a government department or Crown corporation to take reasonable measures for such purposes, including the interception of private communications in circumstances specified in paragraph 184(2)(e) of the *Criminal Code*. The appropriate Minister must take reasonable measures to ensure that only data that is essential to identify, isolate or prevent harm to the computer system will be used or retained.

A Competition Bureau investigation had resulted in several individuals being convicted of violating s. 52, the false or misleading representations provisions, of the *Competition Act*. The misrepresentation involved deceptive mailings from an Internet-based business directory operating under the name Yellow Business Pages.com. The mailings appeared to be bills or invoices from Bell Canada, but in fact were solicitations for the directory. According to an Industry Canada news release, "between May and December 2000, [the individuals] sent mail to virtually all businesses and non-profit organizations in Canada and generated sales of over $1 million."

Privacy

The Privacy Commissioner of Canada has released two findings under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) involving the use of security systems in the workplace. In Case Summary #262, two sets of complaints were filed by the same employee. The first set of complaints related to the requirement that employee pictures be placed on swipe cards. The complainant felt this was not necessary. He further claimed that the company failed to provide employees with information about the swipe card system and that his picture had been stored on a computer and later disclosed by management to other staff without his consent. The Assistant Privacy Commissioner found, in accordance with s.5(3) of *PIPEDA*, a reasonable person would consider the need to enhance safety and security by introducing a swipe card system at the worksite appropriate in the circumstances. She goes on to find that the actions of the company were consistent with Principles 4.2 and 4.4 because the company issued policy statements

and periodic communications to all employees advising them of the rationale for the security system and the purposes for which personal information is collected. Therefore, she concludes this complaint was not well-founded. However, the complaint relating to showing the employee's picture to other staff was held to be well-founded as there was evidence that a manager had inappropriately shown the complainant's picture to staff for purposes other than those for which it was collected without consent in contravention of Principle 4.5.

The second set of complaints concern the use of video cameras to collect personal information without consent and for use in disciplinary action. According to the Assistant Privacy Commissioner, the purpose of the security system was not to collect personal information nor monitor employee productivity. The cameras were located at entrance and exit areas where, it was held, no reasonable expectation of privacy exists. Thus, the Assistant Commissioner found it was not necessary to obtain employee consent and no exception to the requirement for consent need be applied. With respect to using the information obtained from video cameras for disciplinary purposes, the company became aware that the complainant was in breach of safety obligations when it undertook to review the videotapes in the course of investigating concerns that were raised by the complainant himself. The Assistant Commissioner concluded that the company could rely on the exception in 7(2)(a) because it became aware of the information in the course of its activities that could be useful in the investigation of a contravention of a law of Canada. Therefore, she went on to conclude that the third and fourth complaints were not well-founded.

In the second Finding dealing with video cameras, two railway employees complained that video cameras were being used to determine whether they were leaving work outside regular hours rather than for the operational purposes they were ordinarily used for. As a result, the employees were disciplined for leaving work without permission. First, the Assistant Commissioner rejected the company's argument that she use her discretion under s.13(2) of *PIPEDA* and decline jurisdiction because the disciplinary matter is being dealt with through the arbitration process. She stated that the Federal Court decision referred to by the company is currently under appeal and thus she had jurisdiction to investigate the complaints. Second, although the cameras do not record, the definition of personal information is not restricted to information that is recorded and therefore, the Assistant Commissioner concluded the cameras did collect personal information of employees and were used in this situation to collect personal information about the complainants. Third, there was no dispute that the customary use of the cameras to enhance safety is appropriate, but the Assistant Privacy Commissioner found a reasonable person would not consider the use of cameras to monitor a workplace performance issue appropriate in the circumstances pursuant to s.5(3). Finally, the Assistant Commissioner makes clear that there must be evidence of a possible breach of employment conditions for an employer to initiate the collection of personal information for the purposes of an investigation without the consent of the individual. She goes on to caution that any decision to use cameras, even in circumstances set out in 7(1)(b) may contravene *PIPEDA* where a less intrusive method of achieving the same result is available. The complaints were held to be well-founded.

Security

Canada's new national security policy has been published in the document *Securing an Open Society*, which describes several fundamental national security interests and proposes a framework for addressing a variety of threats, including economic espionage. The document highlights cyber-security as a critical priority, and calls for a strengthening of capacity to predict and prevent cyber-attacks. The document states that the federal government promises to improve its ability to defend its systems and respond to cyber-attacks, and to convene a high-level national task force, with public and private representation, to develop a national cyber-security strategy to reduce Canada's vulnerability to cyber-attacks.

Spam

The latest initiative taken to combat spam in Canada is a private member's Bill introduced recently in the Ontario legislature. Like other initiatives, it proposes

the creation of a "no-spam list" that persons who send unsolicited commercial email must first check. It also establishes a cause of civil action in nuisance for sending excessive spam and deems damage to have been caused if the volume is sufficient to cause inconvenience. If a person initiates spam from any place in a manner that allows it to be received in Ontario, the act of sending is deemed to have been effected in Ontario.

Recent Articles

Robert W. Crandall and Hal J. Singer, "Foreign Investment Restrictions as Industrial Policy: The Case of Canadian Telecommunications" (2004) 3 *Canadian Journal of Law & Technology* 19.

Richard Owens, "Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections" (2004) 3 *Canadian Journal of Law & Technology* 33.

Mary Paterson, "Following the Right Lead: Gutnick and the Dance of Internet Jurisdiction" (2004) 3 *Canadian Journal of Law & Technology* 49.

Eric J. Feigin, "Architecture of Consent: Internet Protocols and Their Legal Implications" (2004) 56 *Stanford Law Review* 901.

2ième partie

Protection des renseignements personnels – Québec

Le recours aux technologies de l'information par les organismes publics facilite la collecte et la circulation des renseignements personnels que les citoyens confient aux organismes. Dans ce contexte, le droit au respect de la vie privée et à la protection des renseignements personnels (PRP) est un enjeu important dans les projets de développement des services utilisant les technologies de l'information, tels les services électroniques rendus par l'État à ses clients ou employés.

La Direction du soutien en accès à l'information et en protection des renseignements personnels du ministère des Relations avec les citoyens et de l'Immigration du Québec a ainsi élaboré un *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics*. Ce Modèle de pratique des PRP est un document de référence destiné aux organismes publics pour faciliter le respect des principes et obligations légales de PRP lors de projets de développement faisant appel à des renseignements personnels.

Ce document fournit, entre autres, une description de pratiques et de biens livrables touchant la PRP et propose une approche de planification, d'organisation, de suivi et de contrôle pour que les organisations intègrent la protection des renseignements personnels dans le processus de gestion de leurs projets de développement.

Gouvernement du Québec, *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics*, Publications du Québec, 2004.

Commerce électronique – Nations Unies

Le groupe de travail sur le commerce électronique de la Commission des Nations Unies pour le droit commercial international (CNUDCI) a adopté des recommandations sur un projet d'instrument juridique visant à faciliter le commerce électronique, en éliminant les obstacles actuels. Ce projet de convention tente de créer un régime juridique uniforme pour les transactions faites via le commerce électronique, en s'attachant à l'échange des données et au régime du courrier électronique. Elle s'efforce d'être aussi neutre que possible du point de vue technologique, en raison des progrès rapides accomplis dans ce domaine.

Le groupe de travail de la CNUDCI sur le commerce électronique propose des recommandations sur un projet de convention, Voir A/CN.9/WG.IV/WP.108 – Aspects juridiques du commerce électronique – Contrats électroniques: dispositions pour un projet de convention.

Respect des droits de propriété intellectuelle – Europe

Une proposition de directive de la Commission européenne portant sur les mesures et procédures permettant d'assurer le respect des droits de propriété intellectuelle est en cours d'adoption au Parlement européen.

L'objet de la disposition est d'harmoniser les dispositions législatives, réglementaires et administratives des Etats membres relatives aux moyens de faire respecter les droits de propriété intellectuelle et à assurer que les droits disponibles bénéficient d'un niveau de protection équivalent dans le marché intérieur.

Illiana BOUBEKEUR, *Proposition de directive relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle*, Juriscom.net, 14/04/04.

Spamming – Europe

Au sein de l'Union européenne, le spamming est qualifié, injustement et d'une façon réductrice, d'envoi non sollicité d'un courrier électronique. Dans cet article, l'auteur constate l'absence de définition légale du spamming et discute de l'importance de mieux différencier l'activité des acteurs légitimes du commerce électronique de celle des spammers si les états membres veulent se doter de moyens efficaces de lutte contre cette pratique.

Guillaume TEISSONNIÈRE, *La lutte contre le spamming : de la confiance en l'économie numérique à la méfiance envers ses acteurs*, Juriscom.net, 02/04/04.

Projet de loi pour la confiance dans l'économie numérique – France

Le 8 avril 2004, le Sénat a adopté, en seconde lecture, le projet de loi pour la confiance dans l'économie numérique. Il ne manque plus que l'aval de la Commission mixte paritaire pour qu'il soit définitivement adopté.

L'adoption du projet de loi par le Sénat a suscité des réactions du Forum des droits sur l'Internet concernant la refonte de l'architecture du droit des médias, la prescription des infractions de presse pour les communications au public en ligne et la responsabilité des personnes exerçant l'activité de commerce électronique. (Forum des droits sur l'Internet, *Réactions du Forum des droits sur l'Internet suite à l'adoption de la LCEN par le Sénat*, 24/04/04.)

Voir également :

Murielle CAHEN, *La LEN : état des lieux après l'examen en seconde lecture par le Sénat*, Clic-droit, 26/04/04.

Jean-Christophe BOBABLE, *Une conformité qui défrise la LEN*, Juriscom.net, 20/04/04.

Lionel THOUMYRE, *Hyperdossier sur la responsabilité des acteurs de l'Internet en France*, Juriscom.net, 02/04/04 (hyperliens des principales sources de documentation sur ce sujet).

Cybersurveillance des salariés – France

L'utilisation par un salarié de moyens de communication informatiques (Internet, télécopies) mis à sa disposition par l'employeur dans le cadre du contrat de travail peut poser le problème du détournement de ces moyens à des fins personnelles et peut conduire à un paradoxe. Comment l'employeur peut-il prouver le détournement des moyens mis à sa disposition par le salarié sans attenter à sa vie privée et à l'inverse, quand on est salarié, comment peut-on se voir protégé dans sa vie privée dans un cadre professionnel?

Cahen et associés, *Vie professionnelle, vie privée et informatique; la cybersurveillance des salariés*, Village de la justice, 10/04/02.

Contenus illicites – Co-régulation – France

La co-régulation est « un mode de régulation des réseaux informatiques dans lequel les autorités et tous les parties prenantes se mobilisent pour obtenir la meilleure régulation possible ». Un tel effort de co-régulation s'est concrétisé en France grâce à une initiative conjointe du gouvernement et de l'Association des fournisseurs d'accès et de services Internet (AFA). Cette dernière a publié une charte où les hébergeurs français s'engagent à renforcer leur contribution active à la lutte contre les contenus pédo-pornographiques, racistes ou antisémites mis en ligne sur le réseau Internet.

Les hébergeurs s'engagent, entre autres, à faciliter l'accès d'un dispositif de signalement de ces contenus pour le public et à placer leurs efforts dans toutes les diligences requises auprès des autorités publiques dûment habilitées à la répression de tels contenus. Ces mesures s'ajoutent aux efforts de coopération déjà mis en place depuis quelques années.

Étienne WERY, *Les fournisseurs d'accès se mobilisent contre les contenus illicites*, Droit-technologie, 20/04/04.

Voir Association des fournisseurs d'accès et de services Internet (AFA), *Charte des prestataires de services d'hébergement en ligne en matière de lutte contre certains contenus spécifiques*.

À signaler

Forum des droits sur l'Internet, *Cyber-consommation : les nouvelles tendances-Premier rapport du Forum des droits sur l'Internet sur la cyberconsommation*, 30 mars 2004.

Murielle CAHEN, *L'interception de données sur le réseau d'une école*, Clic-droit, 30/03/04.

Joost VERBEEK, *Nouveau dossier en ligne : commentaire sur l'affaire Jeboycottedanone.com*, droit-technologie, 23 avril 2004.

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 Michael Deturbide, Anne Mussett and Teresa Scassa 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 Michael Deturbide, Anne Mussett et Teresa Scassa 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.