



VOL. 17
N° 1
2007



PERSPECTIVES

COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE / ONTARIO

ANN CAVOUKIAN, Ph.D., COMMISSAIRE



La commissaire Ann Cavoukian prend la parole lors d'une conférence de presse que le CIPVP a tenue en octobre pour dévoiler les sept principes de l'identité axés sur la vie privée. Elle est accompagnée, à sa gauche, de Peter Cullen, stratège principal de la vie privée et, à droite, de Kim Cameron, architecte principal de l'identité, tous deux de Microsoft.

Dans ce numéro :

La commissaire dévoile des principes visant la création d'identités protégées sur Internet

Publications récentes

Calendrier des allocutions

La Semaine du droit de savoir est soulignée pour la première fois au Canada

Protégez les renseignements que vous sortez du bureau

Étudiants, pensez à votre vie privée dans les sites de réseautage personnel

« Indifférence totale » à l'égard de la vie privée d'une patiente, selon une ordonnance rendue en vertu de la LPRPS

Médiations fructueuses

Sommaires d'ordonnances

La commissaire dévoile des principes visant la création d'identités protégées sur Internet

Par Ann Cavoukian, Ph.D.

Commissaire à l'information et à la protection de la vie privée/Ontario

Il existe un écart croissant entre le monde réel et le monde en ligne. Dans le monde concret où nous vivons, nous nous identifions en fonction du contexte et de nos préférences; par exemple, nous achetons un café avec de l'argent comptant ou une carte, une carte d'adhésion nous donne accès au centre de conditionnement physique, un passeport nous permet de franchir la frontière. Notre portefeuille contient plusieurs cartes d'identité, et nous décidons de la nature des renseignements personnels que nous sommes disposés à divulguer. Dans le monde réel, nous pouvons également vérifier à qui nous avons affaire avant de révéler notre identité.

Dans le monde numérique, nous exerçons beaucoup moins de contrôle. Les mécanismes de suivi et de surveillance, la collecte de renseignements personnels excessifs et la fraude en ligne sont des problèmes de plus en plus courants. Les consommateurs accordent de moins en moins confiance à Internet, voire même l'abandonnent. Ce problème réside en partie dans le fait qu'il n'existe aucun moyen pratique de gérer ses différentes identités et sa vie privée en ligne aussi efficacement qu'on peut le faire dans le monde concret.

Le 18 octobre, j'ai annoncé mon appui à l'égard de la création d'un système mondial d'identité en ligne en dévoilant des principes

SUITE À LA PAGE 4



Publications récentes

Le CIPVP a publié les documents suivants (indiqués dans l'ordre de publication) depuis la parution du dernier numéro de *Perspectives* :

Get together, win together: Mediation at the IPC (vidéo). Mai 2006.

Lignes directrices régissant la protection de la vie privée pour les systèmes d'identification par radiofréquence. Juin 2006.

Conseils pratiques pour la mise en œuvre des lignes directrices régissant la protection de la vie privée pour les systèmes d'identification par radiofréquence. Juin 2006.

Rapport annuel 2005 de la commissaire Ann Cavoukian. Juin 2006.

Que faire en cas d'atteinte à la vie privée : Lignes directrices pour le secteur de la santé. Juillet 2006.

If you wanted to know... How to access your personal information held by a municipal organization. Septembre 2006.

Réduisez les risques du travail à distance - Guide élémentaire de protection des renseignements personnels sur votre ordinateur portable (Restez sur vos gardes). Septembre 2006.

Naviguez sans perdre le nord – Protection de la vie privée : Faites des choix éclairés. Octobre 2006.

7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age (document et brochure). Octobre 2006.

Breach Notification Assessment Tool. Décembre 2006.

Toutes ces publications, et d'autres, sont accessibles dans le site Web du CIPVP à www.ipc.on.ca.

Calendrier des allocutions

Le 9 février 2007

La commissaire Ann Cavoukian rencontrera le comité de rédaction de la CBC pour discuter d'aspects courants et nouveaux de la protection de la vie privée et de l'accès à l'information.

Le 13 février 2007

La commissaire Cavoukian prendra la parole devant l'Arizona Association of Certified Fraud Examiners, et abordera la nécessité de faire correspondre les mesures de protection de la vie privée et de sécurité.

Le 16 février 2007

La commissaire Cavoukian sera conférencière invitée à la BC Privacy and Security Conference, au centre des congrès de Victoria.

Le 27 février 2007

La commissaire Cavoukian sera conférencière spéciale à l'Université de Waterloo. Elle discutera de l'identité dans le contexte de la protection de la vie privée.

Le 7 mars 2007

La commissaire Cavoukian prononcera une allocution spéciale sur l'accès à l'information et la protection de la vie privée devant le Canadian Armenian Business Council.

Le 15 mai 2007

La commissaire Cavoukian sera conférencière invitée au congrès national de l'Association canadienne du marketing. Elle discutera de la protection de la vie privée comme avantage concurrentiel.



La Semaine du droit de savoir est soulignée pour la première fois au Canada

Ann Cavoukian, commissaire à l'information et à la protection de la vie privée/Ontario, a collaboré avec ses homologues de l'ensemble du pays ainsi qu'avec le Commissaire à l'information du Canada pour créer et souligner conjointement la première Semaine du droit de savoir du Canada, à la fin de septembre, pour sensibiliser le public à son droit d'accéder à l'information que détient le gouvernement.

Cette semaine a été organisée pour coïncider avec la Journée internationale du droit de savoir, le 28 septembre. Comme l'a dit la commissaire lors d'un déjeuner-causerie tenu au Ontario Club à cette occasion, c'est le 28 septembre 2002 que des représentants d'organismes d'accès à l'information de divers pays se sont rencontrés à Sofia, en Bulgarie, pour créer un réseau de défenseurs de l'accès à l'information qui a convenu de collaborer en vue de promouvoir le droit d'accès à l'information des particuliers ainsi qu'un gouvernement ouvert et transparent.

« Il est absolument essentiel pour les citoyens d'avoir le droit d'accéder aux renseignements que détient le gouvernement, a affirmé la commissaire Cavoukian. Autrement, les responsables élus et nommés ne peuvent être tenus responsables à l'égard des électeurs. Sans ouverture et obligation redditionnelle, on ne peut avoir de société démocratique solide. »

La commissaire a animé un panel spécial lors du déjeuner-causerie de la Semaine du droit de savoir, qui a été organisé par le CIPVP et parrainé par l'Association canadienne des journaux et la section de Toronto de l'Institut d'administration publique du Canada.

La commissaire Cavoukian a souligné le message fondamental qu'elle voulait transmettre aux institutions provinciales et municipales de l'Ontario, selon lequel elles ne devraient pas invoquer systématiquement des exceptions à la

divulgaration de renseignements pour le seul motif qu'il est possible de le faire. Ces exceptions ne devraient être invoquées que si elles s'appliquent réellement. La divulgation devrait toujours être le premier choix.

Siégeaient à ce panel Brian Beamish, commissaire adjoint (accès à l'information) du CIPVP, Anne Kothawala, présidente et chef de la direction de l'Association canadienne des journaux et Robert Cribb, journaliste primé du *Toronto Star* et ancien président de l'Association canadienne des journalistes.

M. Beamish, qui a souligné le rôle du CIPVP comme organisme d'appel dans le cadre du processus d'accès à l'information, a expliqué l'importance de la transparence du gouvernement.

M^{me} Kothawala a décrit à son auditoire, composé surtout de fonctionnaires, certains problèmes qui ont été constatés lors d'une vérification de l'accès à l'information menée récemment

sous l'égide de l'Association canadienne des journaux. Des journalistes de 40 journaux et agences de presse du Canada s'étaient rendus dans des bureaux municipaux et fédéraux pour demander certains renseignements, d'abord en personne, puis par voie de demandes officielles d'accès à l'information en cas de rejet des demandes initiales. Les renseignements demandés ont été divulgués dans certains cas, mais dans d'autres, ils ne l'ont pas été alors qu'il s'agissait de renseignements du même type. (Consulter le site <http://www.cna-acj.ca/Client/CNA/cna.nsf/web/CNA+releases+2006+FOI+Audit?OpenDocument> pour des précisions.)

M. Cribb, qui a contribué à concevoir la vérification et à en examiner les résultats, a affirmé que certains responsables gouvernementaux ne comprennent tout simplement pas que la population canadienne a le droit d'accéder aux renseignements que détiennent les gouvernements.



Steve Faughnan, arbitre au CIPVP, a reçu un prix de la Society of Ontario Adjudicators and Regulators (SOAR) à son récent congrès annuel des conseils et organismes, auquel ont participé des présidents, vice-présidents et membres d'organismes décisionnels de l'Ontario. M. Faughnan a été l'un des quatre lauréats de ce prix, qui lui a été décerné pour son travail comme membre du comité d'éducation de SOAR et comme premier président du sous-comité de refonte du cours de formation des arbitres.



d'envergure axés sur la vie privée, qui aideraient les consommateurs à vérifier l'identité des organismes pour s'assurer de leur légitimité avant d'effectuer des opérations en ligne.

Ces principes s'inspirent des « sept lois de l'identité » formulées à la suite d'un dialogue mondial entre des experts de la sécurité et de la vie privée, sous la direction de Kim Cameron, architecte principal de l'identité à Microsoft. Ce document propose la création d'une « couche d'identité » révolutionnaire pour Internet, et constitue un cadre conceptuel d'envergure visant la mise en place d'un système d'identité universel et interexploitable.

Les sept principes de l'identité axés sur la vie privée que j'ai dévoilés en octobre intègrent d'autres éléments tirés du domaine de la vie privée. Ces principes, qui s'appuient sur les sept lois d'origine, préconisent l'intégration de caractéristiques de protection de la vie privée dans la conception de l'architecture des technologies de l'information, dès le début de la mise en place du système universel d'identité.

Internet a été conçu d'une façon qui ne nous permet pas de déterminer à qui et à quoi nous avons accès. Cette situation limite la marge de manœuvre des utilisateurs et les expose à la fraude. Si l'industrie des technologies de l'information et les gouvernements négligent d'agir, les cas de vol et de fraude se multiplieront rapidement et finiront par miner la confiance du public, phénomène qui a déjà commencé à cause des pourriels, du hameçonnage et du vol d'identité. Les sept principes de l'identité axés sur la vie privée vont dans le sens de l'initiative mondiale visant à habilitier les consommateurs à gérer leurs propres identités numériques et les renseignements personnels qui les concernent d'une façon beaucoup plus sécurisée, vérifiable et privée.

Internet a connu une croissance phénoménale grâce à l'interconnexion de différents réseaux propriétaires; de même, on pourrait s'attendre à une révolution sur le plan de l'identité après l'élaboration d'une méthode ouverte, non propriétaire et universelle pour relier les systèmes d'identité et protéger la vie privée des utilisateurs conformément aux principes de protection de la vie privée. Microsoft a lancé un mouvement mondial en faveur de la protection de la vie privée. Déjà, une liste de plus en plus longue d'entreprises et de particuliers ont accordé leur appui aux sept lois de l'identité et s'emploient à concevoir des systèmes d'identité qui s'y conforment.

Les principes axés sur la vie privée contribueront à réduire le risque qu'un lien puisse être établi entre ses identités en ligne et ses activités sur Internet.

En outre, les systèmes d'identité qui sont conformes aux sept principes de l'identité axés sur la vie privée aideront les consommateurs à vérifier l'identité des organismes avec qui ils envisagent de faire une opération en ligne.

La prochaine génération de services Web intelligents et interactifs (« Web 2.0 ») exigera un plus grand nombre de preuves d'identité vérifiables et une confiance mutuelle beaucoup plus solide pour réussir.

Bref, les sept principes de l'identité axés sur la vie privée offrent aux particuliers :

- un contrôle plus facile et plus direct sur les renseignements personnels qui les concernent quand ils sont en ligne;
- une meilleure capacité de réduire au minimum les données identificatoires qu'ils révèlent en ligne;
- une capacité accrue de réduire au minimum les liens entre leurs identités et leurs activités;
- une capacité accrue de déceler les messages et sites Web frauduleux, et de minimiser ainsi les cas de hameçonnage et de détournement de domaine.

Nous encourageons les concepteurs de logiciels, les intervenants du domaine de la protection de la vie privée et les décideurs du secteur public à étudier en profondeur les sept principes de l'identité axés sur la vie privée, d'en discuter publiquement et de les adopter.

Bon nombre l'ont déjà fait, ont présenté leurs propres projets de gestion de l'identité et ont décrit des solutions axées sur les utilisateurs, respectueuses de la vie privée et susceptibles de renforcer la protection des renseignements personnels. Le CIPVP a entrepris des pourparlers avec les responsables de plusieurs initiatives coopératives de gestion de l'identité d'exploitation libre, notamment les membres de la Liberty Alliance (qui comprend des entreprises telles que Sun et Oracle) et des membres du projet Higgins (qui regroupe IBM et nombreuses autres entreprises), pour promouvoir la protection de la vie privée à notre époque où l'identité revêt tant d'importance.

Pour obtenir des précisions sur les sept principes de l'identité axés sur la vie privée, consulter <http://www.ipc.on.ca/index.asp?navid=67&fid1=15>.



Protégez les renseignements que vous sortez du bureau

Avant de quitter le bureau, apportez avec vous le moins possible de données, et assurez-vous de les protéger.

Cependant, en cas de perte ou de vol de données, notamment des renseignements personnels sur les clients ou le personnel, agissez immédiatement.

Voilà deux conseils contenus dans le dépliant *Réduisez les risques du travail à distance - Guide élémentaire de protection des renseignements personnels sur votre ordinateur portable (Restez sur vos gardes)*, produit conjointement par le CIPVP et BMO Groupe financier, qui a été publié en septembre.

Au cours des deux dernières années, les médias ont signalé des atteintes importantes à la vie privée, à la suite de la perte ou du vol d'ordinateurs portatifs ou d'autres appareils contenant des renseignements personnels sur des milliers de personnes.

Cette brochure fournit une série d'aide-mémoire et des étapes à suivre pour réduire le risque d'atteinte à la vie privée à l'intention des gens qui doivent utiliser des renseignements personnels hors de leur bureau.

« Nous répétons toujours que les organismes doivent prendre des mesures concrètes pour prévenir la divulgation de renseignements qui pourrait mener au vol d'identité », a affirmé Ann Cavoukian, commissaire à l'information et à la protection de la vie privée. « Cette brochure très pratique donne des suggestions concrètes et représente un outil précieux; elle aide à créer ce que nous appelons une culture de la vie privée. Je félicite BMO d'avoir adopté cette approche. »

Voici certaines des recommandations de la commissaire et de BMO qui figurent dans cette brochure :

- Utilisez toujours un mot de passe fort, de préférence en chiffrant les données;
 - Demandez l'autorisation de votre superviseur avant d'extraire des renseignements sur la clientèle se trouvant dans le réseau ou les bureaux de votre entreprise;
 - Ne laissez aucun renseignement confidentiel ou d'appareils contenant de tels renseignements à la vue dans votre véhicule;
 - Verrouillez vos objets de valeur dans le coffre arrière **avant** de partir, et non dans le parc de stationnement de votre destination;
 - Dans les endroits publics, ne divulguez pas de renseignements confidentiels quand vous parlez au téléphone cellulaire;
 - Ne manipulez pas de données confidentielles et ne faites pas d'opérations commerciales dans des endroits publics ou au moyen d'ordinateurs ou de réseaux publics; utilisez uniquement un ordinateur d'entreprise ou un ordinateur personnel.
- Les ordinateurs portables, les assistants numériques et, depuis récemment, les téléphones cellulaires, sont très prisés par les voleurs d'identité. Voici certaines précautions qui sont recommandées dans la brochure pour réduire les risques :
- Veillez à ce que l'accès à tous vos appareils nécessite un mot de passe, que ce soit pour la mise en marche, dans le protecteur d'écran ou pour accéder à vos comptes. Un mot de passe fort doit se composer d'au moins huit caractères, y compris des majuscules et des minuscules, des chiffres et des caractères spéciaux. Le mot de passe ne devrait pas être un mot qui se trouve dans le dictionnaire;
 - Réglez votre appareil pour qu'il se verrouille automatiquement après cinq minutes s'il n'est pas utilisé;
 - Chiffrez vos données selon les politiques de votre entreprise. Cette étape est essentielle si vous transportez des renseignements personnels ou des données confidentielles sur la clientèle; ces données ne devraient jamais être laissées à la vue de tous;
 - Éliminez tous les renseignements confidentiels de vos appareils quand vous n'en avez plus besoin au moyen d'un utilitaire de nettoyage numérique. La fonction de suppression ne suffit pas;
 - Si vous utilisez des renseignements confidentiels ou effectuez des opérations financières en ligne, votre ordinateur portable (et parfois aussi votre



Étudiants, pensez à votre vie privée dans les sites de réseautage personnel



La commissaire Ann Cavoukian a parlé de la vie privée et des réseaux personnels lors de l'ouverture de la série de conférences sur l'éthique Ryerson au Arts and Letters Club de Toronto, en octobre. On la voit ici juste avant son exposé accompagnée, de gauche à droite, de Ken Anderson, commissaire adjoint (vie privée), de Chris Kelly de Facebook, de Mozelle Thompson, consultant en vie privée et ancien commissaire fédéral au Commerce des États-Unis, ainsi que de Brian Jensen et d'Ifoma Smart de Privasoft.

Les sites de réseautage personnel en ligne, où les particuliers affichent toutes sortes de renseignements personnels à leur sujet et au sujet de leurs amis, y compris des photos, sont devenus un véritable phénomène social et technologique.

Après la parution dans les médias de reportages sur certains problèmes causés par l'affichage de tels renseignements, la commissaire Ann Cavoukian a constaté que de nombreux étudiants de collège et élèves du secondaire qui fréquentent certains des sites les plus populaires ne sont pas tout à fait conscients de ce qui pourrait se produire s'ils affichent certains types de renseignements personnels sans tenir compte des possibilités qui s'offrent à eux en matière de protection de la vie privée.

Des incidents de harcèlement et de vol d'identité ont été signalés dans les médias. On a également rapporté d'autres problèmes plus subtils. Par exemple, les étudiants que l'on voit en ligne en train de participer à des fêtes d'un goût douteux ou dans des situations équivoques pourraient voir leur candidature rejetée par des employeurs

éventuels. (De plus en plus d'entreprises effectuent des recherches sur le Web au sujet de leurs employés potentiels, selon plusieurs sondages.) Et ce ne sont pas seulement les photographies qui posent problème. Des observations amusantes d'ordre social ou des commentaires politiques satiriques affichés dans un profil accessible au public ont déjà été employés comme motifs de congédiement ou de refus d'emploi.

La plupart des réseaux personnels en ligne ont adopté des politiques en matière de vie privée et sont dotés de réglages facultatifs qui peuvent limiter l'accès à des renseignements délicats, mais la commissaire a découvert que de nombreux étudiants ne se donnent pas la peine de vérifier les choix qui s'offrent à eux en ligne en matière de protection de la vie privée.

La commissaire Cavoukian a constitué un petit groupe de discussion sous la direction du CIPVP. Avec des étudiants de six universités canadiennes, elle a discuté de la fréquentation des sites Web de réseautage personnel, a demandé aux étudiants s'ils avaient pris connaissance des options en matière



Médiations fructueuses

« Médiations fructueuses » est une rubrique régulière décrivant plusieurs appels récents ou plaintes en matière de vie privée qui ont été réglés récemment par voie de médiation.

La police et l'appelant collaborent pour résoudre un appel

Le Service de police de Pembroke a reçu une demande d'accès à l'information en vertu de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* pour obtenir des notes d'enquête ainsi qu'une copie de tout document concernant l'enquête au sujet d'un sac de dépôt manquant. La police a refusé l'accès aux documents visés par la demande en invoquant les alinéas 8 (2) a) et 14 (3) b) de la *Loi*. L'auteur de la demande (désormais l'appelant) a interjeté appel de la décision devant le CIPVP.

Lors d'une première rencontre avec le médiateur, le représentant de l'appelant a indiqué que la demande d'accès à l'information avait été présentée en vue d'obtenir une preuve écrite démontrant que l'appelant ne faisait plus l'objet d'une enquête. Le médiateur a organisé une téléconférence entre les deux parties afin de donner à chacune l'occasion de faire part de ses préoccupations à la partie adverse.

Lors de la médiation par téléconférence, le représentant de l'appelant a fait part de ses inquiétudes, et le service de police a indiqué qu'il n'était pas disposé à revenir sur sa décision, mais qu'il rédigerait volontiers une lettre selon laquelle il disposait de renseignements insuffisants pour considérer l'appelant comme le seul suspect.

Le représentant de l'appelant n'a pas obtenu accès aux documents en litige, mais il s'est dit quand même satisfait du processus et de la volonté du service de police de fournir le plus de renseignements qu'il jugeait possible de donner en vertu de la *Loi*.

En collaborant pour trouver des solutions au lieu de se poser en adversaires, les parties ont convenu d'un règlement négocié qui répondait à leurs préoccupations.

Élaboration d'une formule et d'une politique à la suite d'une plainte en vertu de la LPRPS

Le CIPVP a reçu une plainte en vertu de la *Loi sur la protection des renseignements personnels sur la santé* de la part d'une personne à qui le service de santé au travail de son ancien employeur avait refusé une demande de rectification de son dossier de santé

au travail. Cet employeur est un établissement de soins de santé.

Le service de santé au travail avait répondu par écrit à la demande de la plaignante de rectifier son dossier. Dans sa lettre de réponse, le service a refusé cette demande, et a indiqué que la lettre de la plaignante serait ajoutée au dossier.

La plainte est passée à l'étape de la médiation au CIPVP, et le médiateur a eu plusieurs conversations téléphoniques avec les deux parties.

La plaignante a indiqué que le document en cause était une inscription d'une infirmière de santé au travail dans le dossier de santé au travail de la plaignante. Cette inscription avait été faite à la suite d'une visite de la plaignante au service de santé au travail de son employeur parce qu'elle s'était sentie mal à l'aise alors qu'elle était à son poste. La plaignante était d'avis que cette inscription était incomplète et inexacte, et qu'elle devait être rectifiée afin d'indiquer que son sentiment d'inconfort était lié au travail, et peut-être aux exigences physiques de son emploi. La plaignante a également indiqué que l'établissement n'avait pas motivé le refus de sa demande.

L'établissement a souligné que l'inscription reflétait ce qui s'était passé, selon l'infirmière, lors de visite de la plaignante. Plus précisément, l'infirmière avait pour habitude de demander à chaque employé qui se présentait si ses symptômes étaient liés au travail et, dans l'affirmative, de le documenter et de fournir à l'employé un rapport à remplir. Dans ce cas, la plaignante n'a pas rempli un tel rapport. De plus, l'établissement a indiqué que l'infirmière ne pouvait modifier son inscription afin d'indiquer un diagnostic possible, car il est interdit aux infirmières de poser un diagnostic. L'établissement a également indiqué qu'il n'existait aucun document à l'appui pour justifier la rectification de l'inscription.

En outre, l'établissement de soins de santé a indiqué qu'à la suite de la plainte, il avait élaboré une formule permettant aux personnes concernées de demander la rectification de leurs renseignements personnels sur la santé, et qu'il élaborait également une politique concernant la rectification. En outre, la directrice de la vie privée a suggéré à l'établissement de l'informer chaque fois qu'il reçoit une demande de rectification de renseignements personnels sur la santé. Elle a également suggéré de fournir aux



« Indifférence totale » à l'égard de la vie privée d'une patiente, selon une ordonnance fondée sur la *LPRPS*

En juillet, la commissaire Ann Cavoukian a rendu sa deuxième ordonnance en vertu de la *Loi sur la protection des renseignements personnels sur la santé (LPRPS)* de l'Ontario, à la suite d'une enquête sur une atteinte grave à la vie privée d'une patiente à l'Hôpital d'Ottawa.

Cette patiente avait dit au personnel qu'elle ne voulait pas que son mari, avec qui elle n'habitait plus, de même que la petite amie de ce dernier, deux employés de l'hôpital, soient mis au courant de son admission ou aient accès aux renseignements personnels sur sa santé.

Or, il est arrivé exactement le contraire, car la petite amie du mari de la patiente, une infirmière qui n'a pas participé à son traitement, a pu accéder aux dossiers de la patiente à l'hôpital, avant et après que les infractions initiales eurent été portées à l'attention des responsables de l'hôpital.

Après avoir reçu la plainte, l'hôpital a ajouté immédiatement une note au dossier de santé électronique (DSE) de la patiente, et une vérification a confirmé que la petite amie de son mari avait accédé à son DSE sans autorisation. Cependant, l'hôpital n'a pas pris de mesures immédiates pour empêcher l'infirmière d'accéder à nouveau à ces renseignements. À la suite de son enquête, la commissaire a conclu que l'infirmière avait accédé sans autorisation aux DSE de la patiente à trois reprises après que la plainte eut été déposée.

La commissaire a conclu que l'infirmière, en tant qu'employée de l'hôpital, avait « utilisé » les renseignements en contravention de la *LPRPS*. L'hôpital a lui-même violé la *Loi* en ne respectant pas ses politiques internes concernant la protection de la vie privée des patients, et a négligé de prendre des mesures immédiates pour éviter que les renseignements personnels sur la santé de la patiente ne continuent d'être utilisés de façon non autorisée.

Dans son ordonnance HO-002, la commissaire a ordonné ce qui suit :

- L'hôpital doit examiner et revoir ses pratiques, procédures et protocoles concernant l'accès aux renseignements sur la santé des patients et la protection de ces renseignements, et

concernant ses ressources humaines, pour veiller à se conformer aux exigences de la *Loi* et de ses règlements d'application, en tenant compte des préoccupations soulevées dans cette ordonnance concernant l'importance capitale de protéger les renseignements personnels sur la santé des patients;

- L'hôpital, dans le cadre de l'examen prévu dans l'ordonnance, doit mettre en œuvre un protocole pour veiller à prendre des mesures raisonnables et immédiates, après avoir été informé d'une atteinte réelle ou potentielle à la vie privée d'un particulier, pour s'assurer de ne permettre aucune autre utilisation ou divulgation non autorisée de documents contenant des renseignements personnels sur la santé;
- Après l'examen, l'hôpital doit s'assurer que tous les employés ou représentants sont renseignés au sujet :
 - a) de leurs obligations aux termes de l'alinéa 15 (3) b) de la *Loi*;
 - b) de leur obligation de se conformer aux nouvelles pratiques en matière de renseignements de l'hôpital, conformément au paragraphe 10 (2) de la *Loi*.

La commissaire a également invité l'hôpital à présenter des excuses officielles à la plaignante.

En conclusion, la commissaire a ajouté :

« L'hôpital a été informé du risque de préjudice, mais ce préjudice s'est quand même produit. L'hôpital avait adopté des politiques pour protéger les renseignements sur la santé, mais elles n'ont pas été suivies intégralement, ou elles n'étaient pas suffisantes pour empêcher que se produise une telle atteinte à la vie privée. En outre, il est particulièrement troublant que l'infirmière ait décidé de négliger non seulement les politiques de l'hôpital, mais également ses obligations déontologiques en tant qu'infirmière autorisée, pour continuer d'accéder sans autorisation au dossier de santé électronique d'une patiente, faisant fi de trois avertissements l'informant de la gravité de cet accès non autorisé. Les établissements de santé doivent



Étudiants,
pensez à
votre vie
privée dans
les sites de
réseautage
personnel

SUITE DE
LA PAGE 6

de vie privée et les a appelés à faire part de leurs préoccupations en matière de protection de la vie privée et d'autres sujets connexes. « Ce fut une réunion très productive, a dit la commissaire, ils étaient tous très intelligents, et vraiment disposés à aborder la question... mais ils n'étaient pas très préoccupés par leur vie privée, et n'avaient pas pris le temps d'envisager toutes leurs options avant d'afficher des renseignements personnels dans ces sites Web. »

En octobre, la commissaire et Facebook.com, un grand site de réseautage personnel, ont publié conjointement la brochure *Naviguez sans perdre le nord – Protection de la vie privée : Faites des choix éclairés*. Cette brochure renseigne les étudiants sur les conséquences que pourrait avoir l'affichage des renseignements personnels dans un site de réseautage personnel; ainsi, il pourrait nuire à leurs chances d'emploi, à leur éducation ou à leur réputation, ou même entraîner du harcèlement. Cette brochure invite tous les usagers des sites de réseautage personnel à se renseigner sur les réglages de protection de la vie privée dans tous les sites Web qu'ils fréquentent, à les utiliser et à examiner régulièrement la politique du site Web en matière de vie privée.

Dans cette brochure, de même que dans ses exposés et dans les entrevues, la commissaire insiste sur l'importance du contrôle. Seul l'utilisateur peut contrôler les réglages de protection de la vie privée dans un site Web de réseautage personnel, et déterminer les renseignements qu'il affiche ou

n'affiche pas en ligne. Surtout, la brochure souligne qu'il revient à chaque personne de décider d'afficher ou non des renseignements personnels en ligne, mais qu'elle devrait le faire de façon éclairée.

La commissaire a lancé son initiative sur le réseautage personnel en ligne ainsi que la brochure à la série de conférences sur l'éthique de l'Université Ryerson, le 12 octobre, en compagnie de gens d'affaires, de professeurs d'université et d'étudiants d'université et de collèges. Des milliers d'exemplaires de cette brochure du CIPVP ont été distribués dans les universités et collèges de l'Ontario, et d'autres commissaires provinciaux à la vie privée l'ont employée dans le cadre de campagnes de sensibilisation au réseautage personnel en ligne.

La commissaire Cavoukian a également fait part de cette initiative aux élèves du secondaire; ainsi, elle a fait un exposé devant les élèves de l'école Bishop Strachan de Toronto, au début de décembre, concernant le harcèlement en ligne. La commissaire a décrit les conséquences potentielles des activités sur Internet, y compris les répercussions à long terme. Comme elle l'a précisé, tout ce qu'on affiche en ligne peut y demeurer en permanence, et être localisé par le personnel enseignant, les administrateurs d'universités ou des employeurs éventuels. Ces renseignements représentent un « curriculum vitae en ligne » qu'il est impossible de contrôler. Comme l'a dit la commissaire, avant d'afficher quoi que ce soit sur Internet, pensez avant de cliquer.

« Indifférence
totale » à l'égard
de la vie privée
d'une patiente,
selon une
ordonnance
fondée sur la

LPRPS
SUITE DE
LA PAGE 8

intégrer dans leurs politiques et pratiques des mesures de protection contre une telle indifférence totale à l'égard de la vie privée d'un patient de la part d'un employé de l'hôpital.

Ce cas démontre qu'il faut bâtir une culture de la vie privée dans les établissements de soins de santé de la province. À moins que des politiques à cet égard ne soient intégrées dans les activités quotidiennes de l'hôpital, elles seront inefficaces. Les hôpitaux

doivent s'assurer non seulement de renseigner leur personnel sur la *Loi* ainsi que sur leurs politiques et pratiques en matière de renseignements, mais ils doivent également intégrer le respect de la vie privée dans leur culture institutionnelle. »



Sommaires

«Sommaires»
est une rubrique
régulière où
sont exposées
les principales
ordonnances
et enquêtes
sur la vie privée.

Ordonnance MO-2072

Appel MA-040138-2

Toronto District School Board

Cet appel portait sur une demande présentée en vertu de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (la « Loi ») au Toronto District School Board pour obtenir une copie du rapport d'évaluation préparé par le conseil scolaire concernant sa demande de propositions pour obtenir du personnel contractuel spécialisé en technologie de l'information.

Le conseil scolaire a localisé un document pertinent, à savoir une feuille de calcul qui était une « évaluation des soumissions », soit un rapport contenant une évaluation des soumissions que le conseil avait reçues et envisagées. Cette évaluation comportait plusieurs catégories de renseignements sur les prix, notamment le salaire du personnel occupant différents postes, les marges, les taux pour les heures supplémentaires, les rabais et d'autres frais extraits des propositions présentées par les 24 parties concernées en réponse à la demande de propositions. L'évaluation des soumissions contenait également des renseignements sous le titre « motifs de disqualification ».

Le conseil scolaire a invoqué l'exception fondée sur les renseignements de tiers figurant au paragraphe 10 (1) de la *Loi* pour refuser l'accès à ce document. L'auteur de la demande a interjeté appel de cette décision devant le CIPVP, et le conseil ainsi que 10 des parties touchées ont présenté des observations selon lesquelles il était raisonnable de s'attendre à ce que la divulgation des renseignements en cause entraîne l'un des préjudices énumérés aux alinéas 10 (1) a) et 10 (1) c) de la *Loi*. Pour étayer leur point de vue, le conseil scolaire et les parties concernées ont fourni des indications sur les avantages que leurs concurrents pourraient tirer de cette divulgation, y compris l'accès à des renseignements internes sur les prix et les coûts, et la capacité de présenter des soumissions inférieures à leurs concurrents. Bernard Morrow, arbitre, a jugé que ces dispositions ne s'appliquaient pas, du fait que le conseil scolaire et les parties concernées n'avaient pas répondu au critère sur les préjudices, et il a ordonné la divulgation de la totalité des documents.

Dans sa décision, l'arbitre a convenu qu'il faut envisager avec prudence la question de la divulgation de renseignements précis sur les soumissions, en tenant compte des critères qui ont été élaborés par le CIPVP, de même que des réalités commerciales du processus de demande de propositions et de la nature de l'industrie en cause [voir l'ordonnance MO-1888].

Cette décision revêt de l'importance car elle souligne que la divulgation de renseignements sur les prix ne signifie pas nécessairement qu'il serait raisonnable de s'attendre à ce qu'il y ait préjudice.

Dans sa décision selon laquelle les critères de préjudice relativement au paragraphe 10 (1) n'étaient pas respectés, l'arbitre Morrow a tenu compte des facteurs suivants :

- huit des 24 parties concernées ont consenti à la divulgation des renseignements qui les concernaient;
- les renseignements en cause ont été présentés par les parties concernées il y a plus de deux ans et demi, et peu d'indications donnent à penser que ces renseignements seraient d'une valeur quelconque pour leurs concurrents de nos jours;
- le prix joue un rôle important pour déterminer si une soumission sera acceptée ou non, mais il ne s'agissait pas du seul critère d'évaluation qui se trouvait dans l'évaluation des soumissions, car ce document établit également les politiques des parties concernées relativement aux heures supplémentaires, une date de garantie de prix, des critères de rabais ainsi que des notes supplémentaires sur des éléments particuliers de chaque proposition.

Ordonnance PO-2494

PA-040327-1

Ministère de la Sécurité communautaire et des Services correctionnels

Cet appel portait sur une demande présentée au ministère de la Sécurité communautaire et des Services correctionnels en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* pour obtenir des documents concernant le permis de



Sommaires

SUITE DE
LA PAGE 10

possession d'armes à feu de l'appelante. Celle-ci avait présenté sa demande à la suite de l'exécution d'un mandat de perquisition à sa résidence par la Police provinciale de l'Ontario pour une question touchant l'application de la loi qui n'avait pas trait à sa demande.

Les documents pertinents comprenaient des photographies et des enregistrements vidéo faits pendant la perquisition, des notes des agents de la Police provinciale et des courriels internes de la Police provinciale concernant la perquisition et les accusations qui ont été portées par la suite.

Le ministère s'est appuyé sur l'alinéa 49 a) (limites au droit d'un particulier d'obtenir les renseignements personnels qui le concernent), de même que sur l'article 19 (secret professionnel de l'avocat) de la *Loi*, pour refuser la divulgation de la totalité des documents en cause. Le ministère a également invoqué l'alinéa 49 b) de même que l'article 21 (vie privée) pour refuser la divulgation de certains autres renseignements.

Le ministère a déclaré qu'étant donné que des exemplaires des documents dont la divulgation avait été refusée étaient inclus dans le dossier du procureur de la Couronne utilisé aux fins d'une instance criminelle, l'article 19 s'appliquait aux documents. Le ministère a soutenu que tous les documents qu'il avait en sa possession et qui se retrouveraient dans le dossier de la Couronne seraient nécessairement considérés comme des renseignements élaborés pour le compte du procureur de la Couronne à l'occasion ou en prévision d'une instance, conformément à l'article 19.

Brian Beamish, commissaire adjoint (accès à l'information), a rejeté l'argument du ministère, car il était d'avis que les documents avaient été préparés à des fins d'enquête pour permettre au ministère de déterminer s'il devait porter ou non des accusations criminelles pour possession d'armes à feu. Il a soutenu que cette fin ne revenait pas à utiliser des copies des documents pour déterminer s'il fallait ou non porter des accusations criminelles et utiliser ces documents dans le cadre de l'instance. D'après le commissaire adjoint, le fait que des copies des documents se soient retrouvées dans le dossier de la Couronne ne vient pas modifier les fins auxquelles ces documents ont été préparés et sont maintenant conservés par le ministère.

Dans sa décision, le commissaire adjoint a tenu compte du fait que les dossiers d'enquête sont protégés par les dispositions de l'article 14 de la

Loi portant sur l'application de la loi. Il a soutenu également que si l'on acceptait l'argument du ministère, l'article 19 s'appliquerait à presque tout document d'enquête créé par la police. Le commissaire adjoint était d'avis que cette interprétation minerait l'objet de la *Loi* d'assurer l'accès à l'information. Selon lui, s'il appliquait l'exception fondée sur le secret professionnel de l'avocat en l'espèce, tous les documents que les services de police de l'Ontario divulguent systématiquement de nos jours ne seraient plus divulgués à l'avenir, ce qui changerait totalement une pratique de longue date.

Le commissaire adjoint a également constaté que certains des renseignements dont le ministère a refusé la divulgation en vertu de l'alinéa 49 b) et de l'article 21 faisaient l'objet d'une exception, mais pas tous.

Par conséquent, le commissaire adjoint Beamish a ordonné au ministère de divulguer les documents pertinents à l'appelante, à l'exception des renseignements personnels qui faisaient l'objet d'une exception.

Ordonnance PO-2500

Appel PA-030106-5

Ministère de l'Environnement

Le ministère de l'Environnement a reçu une demande d'accès à tous les renseignements qu'il avait reçus ou produits au sujet de rapports environnementaux faisant intervenir les installations nucléaires de Bruce à Tiverton (Ontario).

Ils'agit là du cinquième d'une série d'appels devant le CIPVP concernant la même demande. L'historique des quatre premiers appels est décrit en détail dans l'ordonnance PO-2243, qui a réglé l'appel PA-030106-4. En réponse à cette ordonnance, le ministère a décidé de divulguer une partie des documents pertinents et de refuser l'accès à d'autres documents, en totalité ou en partie, en invoquant les exceptions figurant à l'alinéa 14 (1) i) (sécurité d'un immeuble) de l'article 16 (sécurité nationale), des alinéas 17 (1) a) et c) (renseignements de tiers), de l'article 19 (secret professionnel de l'avocat), du paragraphe 21 (1) (vie privée) et de l'alinéa 22 a) (renseignements accessibles au public) de la *Loi sur l'accès à l'information et la protection de la vie privée* (la « *Loi* »).

Dans sa lettre d'appel, l'appelante a soulevé l'application possible de l'exception fondée



Sommaires

SUITE DE
LA PAGE 11

sur l'intérêt public prévue à l'article 23 aux renseignements contenus dans les documents.

Les observations du ministère concernant l'article 16 portent surtout sur ses inquiétudes concernant la possibilité que les installations nucléaires de Bruce fassent l'objet d'attaques violentes. Le ministère a également précisé que ses inquiétudes découlaient du fait qu'une fois les renseignements divulgués, ils seraient du domaine public. Le ministère a inclus dans ses observations des conseils reçus du corps de police local concernant les répercussions de la divulgation des documents au sujet desquels il a invoqué cette exception.

L'arbitre John Higgins a souligné que les gouvernements du Canada et des États-Unis avaient pris des mesures pour réduire le risque d'attaques contre leurs populations dans la foulée des attaques terroristes du 11 septembre 2001, notamment des mesures législatives, par exemple la *Patriot Act*

des États-Unis et la *Loi antiterroriste* du Canada. De toute évidence, de l'avis de l'arbitre, ce risque s'applique aux installations telles que les centrales nucléaires.

L'arbitre, après avoir examiné les documents et les observations des parties, a jugé qu'il était raisonnable de s'attendre à ce que la divulgation de la totalité ou de parties de documents contenant des renseignements techniques détaillés sur les installations nucléaires et autres de Bruce nuise à la défense du Canada ou entrave la détection, la prévention ou la répression de l'espionnage, du sabotage ou du terrorisme, et que les documents faisaient donc l'objet de l'exception prévue à l'article 16.

L'arbitre Higgins a protégé d'autres documents en vertu de l'exception fondée sur le secret professionnel de l'avocat, et il a ordonné la divulgation du reste des documents au sujet desquels d'autres exceptions avaient été invoquées.

Médiations fructueuses

SUITE DE
LA PAGE 7

auteurs des demandes des motifs écrits dans les cas où cette rectification est refusée.

Après d'autres discussions avec le médiateur, la plaignante a convenu, pour résoudre cette plainte, de rédiger une déclaration de désaccord et de la remettre à l'établissement pour étude. L'établissement a confirmé par écrit à la plaignante qu'il avait reçu cette déclaration, qu'il l'avait annexée au dossier de santé au travail et qu'elle serait fournie chaque fois que le dossier serait utilisé.

Conséquences de la panne d'électricité

La plupart des habitants du Sud de l'Ontario se souviendront de l'endroit où ils étaient, à l'été 2003, lorsqu'il y a eu une panne d'électricité à la suite de la défaillance d'un réseau américain relié à un certain nombre d'États ainsi qu'à l'Ontario.

Cette panne généralisée a entraîné certains problèmes persistants et a donné lieu à des demandes d'accès à l'information.

En l'occurrence, l'auteur de la demande voulait savoir si la panne d'électricité avait causé des problèmes environnementaux. Il a présenté au ministère de l'Environnement une demande en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* en vue d'obtenir certains documents.

Le ministère a répondu qu'après des recherches approfondies dans les dossiers de la Direction des enquêtes et de l'application des lois, il n'avait pu

localiser aucun document visé par la demande. L'auteur de la demande (désormais l'appelant) a interjeté appel de cette décision devant le CIPVP.

Pendant le processus de médiation, le médiateur a communiqué d'abord avec l'appelant. Ce dernier a reconnu que la lettre de demande qu'il avait fait parvenir au ministère aurait pu être plus claire. Elle ne contenait pas de détails suffisants qui auraient permis au ministère de mener des recherches fructueuses.

Le médiateur a recommandé d'organiser une conférence téléphonique entre l'appelant, le médiateur et le ministère. Pendant cette conférence, l'appelant a pu éclaircir sa demande et fournir des renseignements supplémentaires. Par la suite, le ministère a accepté de mener des recherches supplémentaires pour localiser les documents, et a élargi cette recherche à d'autres services.

Le ministère a localisé des documents pertinents et a accordé l'accès à ces documents à l'appelant. Après examen, l'appelant a informé le médiateur qu'il était satisfait des documents fournis, et qu'il ne voulait plus procéder à l'appel. L'appelant a apprécié que le ministère lui donne la possibilité, lors de la conférence téléphonique, d'expliquer sa demande.

La conférence téléphonique a duré moins d'une demi-heure et a permis à l'appelant d'obtenir les renseignements dont il avait besoin. L'appel a donc été réglé grâce à une communication directe entre l'appelant et le ministère.



La commissaire Ann Cavoukian prend la parole au déjeuner-causerie « Femmes d'influence » de PowerPoint Group, tenu en septembre à l'hôtel Fairmont Royal York. Son allocution, intitulée « Franchir les obstacles », portait sur les défis qu'elle a dû surmonter. La salle affichait complet.

**Protégez les
renseignements
que vous sortez
du bureau**

SUITE DE
LA PAGE 5

assistant numérique) devrait être doté au moins d'un coupe-feu, d'un logiciel antivirus et d'une protection contre les logiciels espions. En outre, installez les dernières mises à jour et rustines de sécurité dans vos appareils mobiles, y compris votre téléphone cellulaire;

- Lorsque vous utilisez un réseau public sans fil ou un point d'accès sans fil dans un aéroport, un hôtel, un café, etc., n'oubliez pas que ces réseaux ne sont pas sécuritaires. Suivez les conseils suivants :
 - o Assurez-vous que personne ne regarde par-dessus votre épaule ce qui se trouve à l'écran de votre ordinateur portatif;
 - o Ne vous reliez jamais à deux réseaux distincts en même temps (par exemple, un réseau Wi-Fi et un réseau Bluetooth);

- o Ne faites pas d'opérations commerciales confidentielles à moins d'être branché de façon chiffrée au réseau privé virtuel (RPV) de votre entreprise.

Cette brochure propose également des conseils si vous perdez des données confidentielles, que ce soit à votre sujet ou au sujet de votre clientèle (agissez tout de suite!), et fournit un aide-mémoire rapide.

La brochure *Réduisez les risques du travail à distance - Guide élémentaire de protection des renseignements personnels sur votre ordinateur portable (Restez sur vos gardes)* est accessible dans le site Web du CIPVP à www.ipc.on.ca.

PERSPECTIVES

est publié par **le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario**.

Pour nous faire part de vos observations, nous informer d'un changement d'adresse ou pour que votre nom soit ajouté à la liste d'envoi, veuillez communiquer avec :

Le service des communications

*Commissaire à l'information et
à la protection de la vie privée/Ontario*
2, rue Bloor Est, Bureau 1400
Toronto (Ontario) M4W 1A8
Téléphone : 416-326-3333 • 1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca
This newsletter is also available in English.



Papier recyclé
à 30 %

ISSN 1188-3006