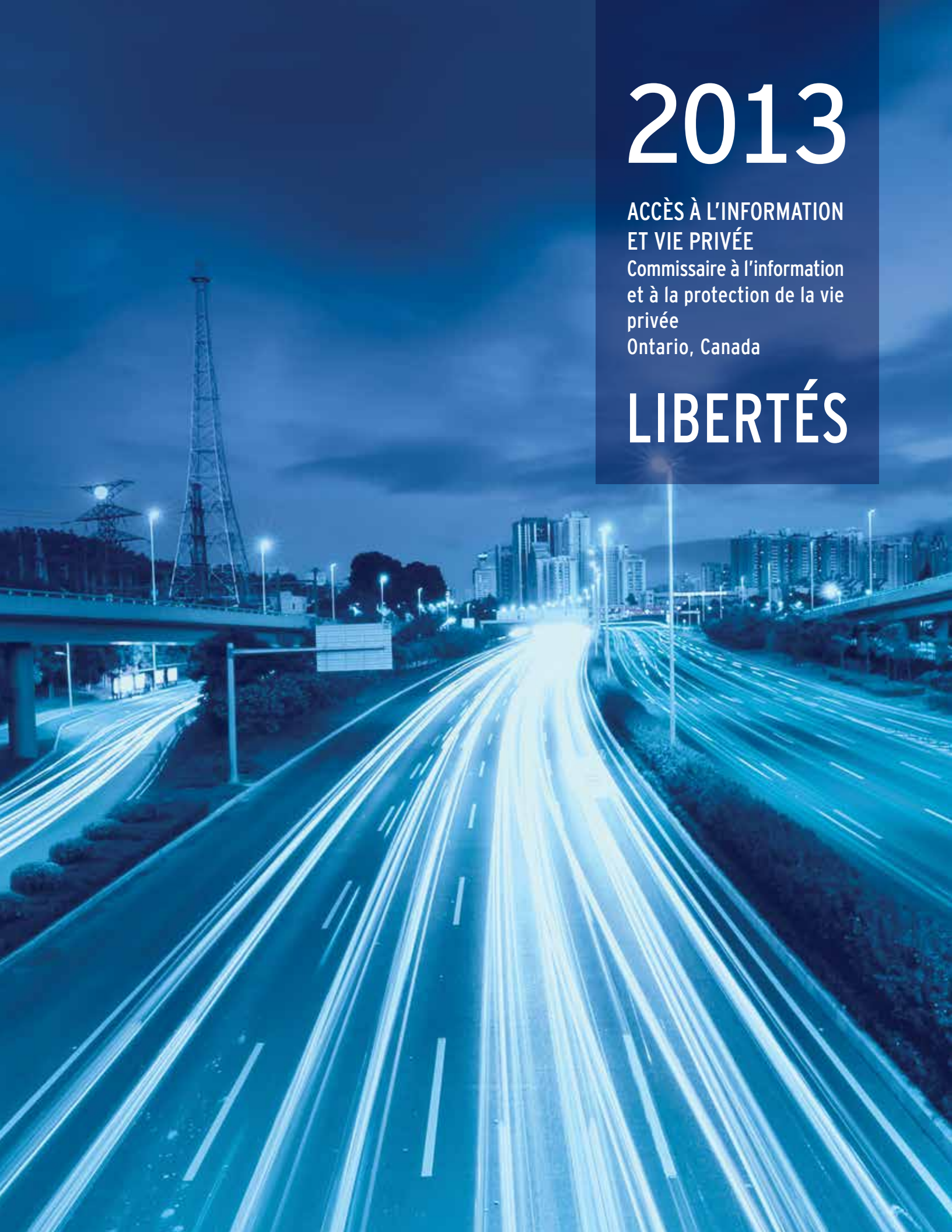


2013

ACCÈS À L'INFORMATION ET VIE PRIVÉE

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

LIBERTÉS

En tant que commissaire, je considère que l'un des éléments les plus importants de mon mandat consiste à informer les citoyens afin de les encourager à faire respecter sans équivoque leur vie privée et leurs libertés.

MESSAGE DE LA COMMISSAIRE

AU DÉBUT DE MON PREMIER MANDAT À TITRE DE COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, EN 1997, IL M'AURAIT ÉTÉ IMPOSSIBLE D'IMAGINER À QUEL POINT LE MONDE CHANGERAIT!

C'est essentiellement à la maison et au bureau que les gens se servaient d'un ordinateur et d'Internet. Les ordinateurs portables n'étaient pas encore très pratiques, et les téléphones cellulaires n'avaient rien d'intelligent.

Aujourd'hui, la technologie de l'information est compacte, mobile et omniprésente. Impossible de se promener dans la rue sans voir quelqu'un se servir d'un appareil mobile doté d'une puissance de calcul supérieure à celle qu'aurait eu tout un étage d'ordinateurs il y a une génération à peine. La technologie de l'information et des communications touche presque tous les aspects de notre vie.

Après ma première reconduction en 2004, j'avais déclaré que nous vivions des bouleversements au chapitre de la protection de la vie privée et de l'accès aux renseignements gouvernementaux. Cependant, comme je l'ai toujours affirmé, la technologie, qui nous oblige à relever bien des défis, représente aussi une source de solutions novatrices, particulièrement du côté de la protection de la vie privée et de l'accès à l'information.

J'ai été très honorée que l'Assemblée législative de l'Ontario renouvelle une autre fois, en 2009, mon mandat de commissaire, ce qui représentait une mesure sans précédent. C'est un jour que je n'oublierai jamais, et je demeure très reconnaissante aux députés provinciaux de m'avoir accordé leur appui et leur confiance. Je me suis engagée alors à me concentrer sur la *protection intégrée de la vie privée* et de promouvoir la transparence et la reddition de comptes de la part du gouvernement par l'entremise de notre nouveau concept d'*accès à l'information intégré*.

Comme le montre la chronologie suivante, je crois que nous comptons de nombreuses réalisations à notre actif, non seulement pour la population ontarienne, mais également pour les générations futures au pays et dans le monde.

2009

En 2009, j'ai continué de promouvoir la *protection intégrée de la vie privée* sur la scène mondiale en lançant *Les sept principes fondamentaux de la protection intégrée de la vie privée*. Je suis fière d'annoncer que ce document a été traduit en 35 langues jusqu'à présent. Pour maintenir l'élan de la *protection intégrée de la vie privée* à l'échelle mondiale, j'ai également lancé le site **www.vieprivee-integree.ca**, qui regroupe actualités, renseignements et études.

Dans un autre ordre d'idées, à l'issue d'une enquête approfondie, j'ai publié un rapport spécial intitulé *Excessive Background Checks Conducted on Prospective Jurors: A Special Investigation Report*. J'ai recommandé notamment que les procureurs de la Couronne cessent de recueillir des renseignements personnels sur les candidats jurés autres que ceux requis aux termes de la *Loi sur les jurys* et du *Code criminel*. J'ai aussi proposé une modification majeure de la méthode de sélection préliminaire des candidats jurés, afin de donner plus de cohérence aux pratiques disparates des bureaux des procureurs de la Couronne et des services policiers.

2010

J'ai lancé une campagne appelée *Attention! Pensez-y. Protégez la vie privée de vos patients* qui demandait au secteur de la santé de l'Ontario de lutter contre les cas croissants d'atteinte évitable à la vie privée mettant en cause des renseignements personnels sur la santé. Plus précisément, j'ai demandé aux groupes de ce secteur de renseigner leur personnel sur les étapes simples à suivre pour éviter la divulgation de données non chiffrées en raison de la perte ou du vol d'appareils électroniques portatifs, qui se produit bien trop souvent.

Une résolution marquante a été adoptée à l'unanimité à Jérusalem lors d'une assemblée internationale de commissaires à la vie privée et d'organismes de protection des données, reconnaissant la *protection intégrée de la vie privée* comme un élément fondamental de la protection de la vie privée, ce qui en a fait aussitôt une norme internationale.

J'ai fait connaître mon concept d'*accès à l'information intégré*. Celui-ci repose sur sept principes fondamentaux qui encouragent les institutions publiques à envisager la publication de renseignements de façon proactive, afin que la divulgation de l'information que détient le gouvernement soit systématique dans la mesure du possible. Ainsi, l'information devient implicitement accessible.

2011

J'ai déclaré que l'année 2011 était celle de l'ingénieur, afin de joindre tous ces experts en conception et en développement de systèmes et de technologies sur qui nous nous appuyons. Je voulais mettre aux défis les innovateurs et ingénieurs d'opérationnaliser la *protection intégrée de la vie privée* et d'en faire une réalité dans la vie de tous les jours. J'ai été ravie de leur réponse à mon invitation, et de leur empressement à relever le défi de faire de la protection de la vie privée une caractéristique de base. Il est devenu évident que mon objectif était tout à fait réalisable!

La Société des loteries et des jeux de l'Ontario (OLG) a lancé son programme volontaire d'autoexclusion à l'issue d'une collaboration fructueuse avec mon bureau et l'Université de Toronto. Ce programme visait à intégrer un protocole de conception fondé sur la *protection intégrée de la vi*e privée et appelé « chiffrement biométrique ». Cette fonctionnalité a permis à l'OLG de mieux soutenir ses clients inscrits à son programme pleinement volontaire d'autoexclusion, tout en protégeant les

renseignements personnels relatifs à tous les clients de l'OLG.

2012

J'ai tenu un symposium public intitulé « Attention à la "surveillance intégrée" : défendons les libertés et le droit à la vie privée », qui a réuni un groupe de leaders éclairés et hautement respectés pour connaître leurs points de vue et accroître la sensibilisation au sujet des répercussions graves sur la vie privée de la surveillance en ligne prévue dans le projet de loi fédéral sur l'« accès légal » [il n'y avait rien de légal dans ce projet]. J'ai été heureuse de voir des gens de tous horizons politiques et sociaux se porter à la défense de la vie privée à la suite du dépôt du projet de loi C-30, qui portait gravement atteinte à la vie privée. Nos efforts ont été couronnés de succès, le projet de loi ayant été retiré.

Après une longue campagne, la *Loi sur la responsabilisation du secteur parapublic* est entrée en vigueur, et a assujetti les hôpitaux de l'Ontario à la *Loi sur l'accès à l'information et la protection de la vie privée*. Ce fut un jalon historique dans l'évolution de l'accès à l'information en Ontario, car les citoyens peuvent désormais demander l'accès à un éventail de renseignements consignés.

Lors de mon enquête sur la perte par Élections Ontario de deux clés USB contenant des renseignements personnels non chiffrés concernant jusqu'à 2,4 millions d'électeurs, j'ai conclu que ce problème avait résulté du fait que cet organisme avait omis de tenir compte de façon systémique des questions de protection de la vie privée et de sécurité de l'information. J'ai recommandé à Élections Ontario de prendre des mesures concrètes afin d'améliorer la protection des renseignements personnels dans trois secteurs : les politiques, pratiques et procédures; la formation et la conformité; ainsi que la reddition de comptes. Le directeur général des élections a accepté sans réserve mes recommandations. Parallèlement à mon rapport, j'ai publié un document d'orientation intitulé *A Policy is Not Enough: It Must be Reflected in Concrete Practices* sur la façon d'instaurer efficacement une politique de protection de la vie privée et de l'intégrer dans les pratiques concrètes d'une organisation.

Conférence Think d'ORION – L'hon. Reza Moridi, ministre de la Recherche et de l'Innovation; Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario; Darin Graham, président et chef de la direction, ORION

Forum des utilisateurs de la *protection intégrée de la vie privée*

Afin d'aider les organisations qui cherchent à mettre en œuvre la *protection intégrée de la vie privée*, j'ai publié le document marquant *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. Ce document recense les expériences d'organismes d'un éventail de secteurs, notamment les télécommunications, la technologie, les soins de santé, le transport et l'énergie. Il propose une vue d'ensemble détaillée des partenariats et projets conjoints auxquels je participe pour implanter la protection intégrée de la vie privée en appliquant ses principes de façon concrète.

2013

Dans mon rapport annuel 2012, j'ai affirmé que le principal enjeu en 2013 serait de savoir si le projet de loi C-30, sur le soi-disant « accès légal », serait modifié afin d'inclure des mesures de protection de la vie privée. J'ai eu une réponse à cette question dès le début de l'année : le 11 février 2013, le gouvernement fédéral a annoncé qu'il n'irait pas de l'avant avec le projet de loi C-30, et que dans toute modernisation éventuelle du *Code criminel*, il n'y aurait aucune des mesures prévues dans le projet de loi, comme la divulgation obligatoire sans mandat de renseignements de base sur les abonnés ou l'obligation pour les fournisseurs de services de télécommunications d'intégrer une capacité d'interception dans leurs systèmes. La vie privée et la liberté étaient saines et sauves!

Toutefois, cette victoire à la suite du retrait du projet de loi C-30 a été de courte durée. En novembre, le gouvernement fédéral a déposé le projet de loi C-13, qui prévoyait de nouveaux pouvoirs en matière de surveillance en vue de protéger les enfants. Moins sévère que son prédécesseur, ce nouveau projet de loi s'appuie toutefois sur des technologies de surveillance nouvelles et en développement qui menacent le droit à la vie privée de tous les Canadiens. En tant que commissaire, je considère que l'un des éléments les plus importants de mon mandat consiste à informer les citoyens afin de les encourager à faire respecter sans équivoque leur vie privée et leurs libertés.

Autre événement au cours d'une année déjà troublante pour le respect de la vie privée, Edward Snowden, ancien analyste à la National Security

Agency (NSA) des États-Unis, a fait des révélations montrant à quel point les gouvernements surveillent leurs citoyens de façon soutenue et systématique. Plus tard, on a découvert que la NSA n'agissait pas seule. Ces révélations ont mis en lumière la participation de grandes entreprises du domaine de l'information et de la technologie ainsi que des autres pays du Groupe des cinq, qui se compose du Royaume-Uni, de l'Australie, de la Nouvelle-Zélande et du Centre de la sécurité des télécommunications Canada (CSTC). Motivée par ce qui m'apparaissait comme une attaque mondiale contre la vie privée lancée impunément par les gouvernements, j'ai rédigé un article d'opinion conjointement avec Ron Deibert, Andrew Clement et Nathalie Des Rosiers qui a paru dans le *Globe and Mail* sous le titre *Real Privacy Means Real Oversight*. Notre argument était que dans une société libre et démocratique, l'État doit être accessible et transparent pour ses citoyens. En outre, il ne devrait pouvoir accéder à des renseignements personnels que lorsqu'une loi le lui permet. Pour ce qui est des pouvoirs de l'État en matière de surveillance, les mesures essentielles de protection de la vie privée doivent comprendre l'autorisation judiciaire et la surveillance indépendante.

En juin, j'ai publié les conclusions de mon enquête sur une plainte du député provincial Peter Tabuns, qui avait allégué que le chef de cabinet de l'ancien ministre de l'Énergie avait supprimé abusivement tous les courriels concernant l'annulation des centrales au gaz de Mississauga et d'Oakville. Comme je l'ai indiqué dans mon rapport d'enquête spécial, *Deleting Accountability: Records Management Practices of Political Staff*, j'ai constaté que la cause fondamentale de ce problème était la pratique consistant à supprimer systématiquement tous les courriels envoyés et reçus par les membres du personnel des cabinets ministériels. Cette pratique allait à l'encontre de la *Loi sur les Archives publiques et la conservation des documents* ainsi que des objets de la *Loi sur l'accès à l'information et la protection de la vie privée* en matière de transparence et de reddition de comptes. Dans mon rapport, j'ai recommandé que le gouvernement prenne trois mesures concrètes, c'est-à-dire modifier les procédures du Bureau du premier ministre et les bureaux des ministres, apporter des changements législatifs et modifier les politiques de conservation des documents. Je constate avec plaisir que la première ministre et le gouvernement ont réalisé des progrès importants en vue de mettre en œuvre chacune de ces recommandations. Mon bureau continue de collaborer étroitement avec eux.

La présidente de la Federal Trade Commission des États-Unis, Edith Ramirez, a déclaré que les principes de la *protection intégrée de la vie privée* devraient être adaptés au nouveau domaine que constituent les appareils ménagers et autres reliés à Internet, étant donné le risque d'une nouvelle explosion dans la quantité de données recueillies sur les consommateurs. M^{me} Ramirez a également affirmé que les entreprises devraient souscrire aux trois principes de base adoptés par la FTC : intégrer des caractéristiques de protection de la vie privée dans les nouveaux produits dès leur conception, concept connu sous le nom de *protection intégrée de la vie privée*; divulguer aux consommateurs les renseignements que les appareils recueillent et la façon dont ils sont utilisés ou partagés; permettre aux consommateurs d'avoir le contrôle de leurs données.

2014

Le 28 janvier 2014, à l'occasion de la Journée internationale de la vie privée, j'ai tenu un symposium public qui a affiché complet, intitulé *Big Surveillance Demands Big Privacy – Enter Privacy-Protective Surveillance*. Plus de 400 personnes y ont participé en personne ou par webdiffusion pour entendre des conférenciers très réputés du monde universitaire, de la communauté juridique et de la société civile, qui ont abordé les nombreuses questions touchant la surveillance exercée par l'État et le besoin urgent des assemblées législatives d'assurer une surveillance indépendante.

Le jour de ce symposium, qui a été couronné de succès, j'ai été troublée d'apprendre que le CSTC avait

utilisé des renseignements recueillis par l'entremise des réseaux Wi-Fi gratuits dans un grand aéroport canadien pour assurer le repérage des appareils sans fil de milliers de passagers de lignes aériennes, pendant des jours après leur départ de l'aérogare. Le CSTC a prétendu que cette activité était légale car il ne recueillait que des métadonnées. J'ai remis fortement en cause cette affirmation. Un tel geste n'est pas digne d'une société libre et démocratique.

Conclusion

J'ai peine à croire parfois que 25 ans se sont écoulés depuis mon arrivée au Bureau du commissaire à l'information et à la protection de la vie privée (CIPVP), que j'ai l'honneur de servir comme commissaire depuis 16 ans. Pendant cette période, j'ai eu de nombreuses occasions de défendre la protection de la vie privée et l'accès à l'information. Je me suis également trouvée dans une position unique en tant que commissaire pour voir comment l'avènement d'Internet a totalement bouleversé les concepts d'accès à l'information et de vie privée. Comme je l'ai déjà dit, dans un monde idéal, nous n'aurions pas besoin du CIPVP. Or, nous vivons dans un monde imparfait, et malgré les grandes avancées réalisées dans les domaines de l'accès à l'information et de la protection de la vie privée, je demeure fermement convaincue que notre travail est plus nécessaire que jamais. Quand je repense à toutes ses années d'activités du CIPVP, il m'apparaît évident que les Ontariennes et les Ontariens peuvent avoir l'assurance que notre bureau est devenu un organisme de premier ordre, reconnu pour son esprit novateur et son leadership dans les domaines de l'accès à l'information et de la protection de la vie privée. Mes efforts et ceux de notre bureau visent toujours à promouvoir une cause noble : l'ouverture et la transparence du gouvernement et la protection de notre vie privée, qui sont essentielles dans notre société libre et démocratique. J'espère que nous continuerons dans cette voie.

Ann Cavoukian, Ph.D.
Commissaire à l'information et à la protection de la vie privée, Ontario, Canada

Comme je l'ai déjà dit, dans un monde idéal, nous n'aurions pas besoin du CIPVP. Or, nous vivons dans un monde imparfait, et malgré les grandes avancées réalisées dans les domaines de l'accès à l'information et de la protection de la vie privée, je demeure fermement convaincue que notre travail est plus nécessaire que jamais.


Dans une société libre et
démocratique, l'État doit être
accessible et transparent
pour ses citoyens.

TABLE DES MATIÈRES

Dans le monde entier, des gouvernements renforcent leurs textes de loi pour s'adapter aux réalités du XXIe siècle. Nous devons faire de même pour que l'Ontario reste un chef de file de l'accès à l'information et de la protection de la vie privée.

RECOMMANDATIONS DE LA COMMISSAIRE

Modernisation de la *LAIPVP* et de la *LAIMPVP*

La *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (*LAIMPVP*) sont entrées en vigueur il y a plus de 20 ans; on peut donc affirmer que ces textes de loi sont parvenus à maturité. Lors des débats qui ont précédé leur adoption, les législateurs n'auraient pu prévoir tout l'éventail de possibilités et de défis qui est apparu à la suite de la croissance explosive d'Internet, du Web et, de nos jours, du monde des mégadonnées. Les *Lois* ne reflètent donc plus les réalités de l'ère de l'information avec lesquelles doivent composer les institutions publiques en matière d'accès à l'information et de protection de la vie privée. Par ailleurs, les révélations d'Edward Snowden au sujet des programmes de surveillance des États ont sensibilisé à l'érosion de leur vie privée les Canadiennes et Canadiens, qui réclament une transparence accrue et un meilleur encadrement de ces programmes. Dans le monde entier, des gouvernements renforcent leurs textes de loi pour s'adapter aux réalités du XXIe siècle. Nous devons faire de même pour que l'Ontario reste un chef de file de l'accès à l'information et de la protection de la vie privée.

En octobre dernier, j'ai appuyé une résolution conjointe des commissaires fédéral, provinciaux et territoriaux de l'accès à l'information et de la protection de la vie privée réclamant des ordres de gouvernement du pays qu'ils mettent à jour leurs lois sur l'accès à l'information et la protection de la vie privée. Il me semblait essentiel pour le gouvernement de l'Ontario d'entamer un examen exhaustif des *Lois* en vue de les moderniser. Je crois fermement qu'il y a lieu d'envisager notamment les réformes suivantes :

- Prévoir d'importants pouvoirs de contrainte et des sanctions sévères en cas de non-respect des dispositions des *Lois* en matière de protection de la vie privée;
- Renforcer les exigences touchant les rapports publics quant à la divulgation de renseignements personnels entre des entités publiques et privées;
- Créer de nouveaux mécanismes assortis d'incitatifs afin d'assurer l'intégration proactive de mesures de protection de la vie privée au stade de la conception des technologies de l'information et des procédés opérationnels;
- Établir des mécanismes supplémentaires de divulgation proactive de l'information.

Sociétés d'aide à l'enfance

Dans mes rapports annuels de 2004, 2009 et 2012, j'ai recommandé que les sociétés d'aide à l'enfance, qui fournissent des services destinés à des citoyens comptant parmi les plus vulnérables, c'est-à-dire les enfants et les adolescents qui sont sous la tutelle de l'État, soient assujetties à la *LAIPVP*. Je suis déçue que rien ne soit fait pour que ces organismes, qui reçoivent beaucoup de fonds publics, fassent preuve de transparence et rendent des comptes. J'invite le gouvernement, dans le cadre de la modernisation des *Lois*, à combler enfin cette lacune flagrante et à faire en sorte que les sociétés d'aide à l'enfance soient ajoutées à la liste des institutions visées par la *Loi*.

Documents des conseillers municipaux

En ce qui concerne les demandes d'accès à des documents que possèdent des conseillers municipaux, on distingue généralement les documents de circonscription des documents créés dans le cadre des activités des conseillers de la part de la municipalité. Concrètement, cette démarche comporte des lacunes. L'expérience a démontré qu'une bonne partie des documents considérés comme politiques ou relevant du travail dans la circonscription ont trait en fait à des activités menées pour la municipalité et devraient être assujettis aux dispositions de la *LAIMPVP.*

Cette question a suscité beaucoup d'intérêt en raison de la présentation de demandes d'accès à des documents dont des conseillers de Toronto avaient la garde. Dans plusieurs ordonnances récentes, nous avons établi que compte tenu du libellé actuel de la *Loi*, la ville n'avait pas la garde ou le contrôle des documents demandés, de sorte que ceux-ci ne pouvaient faire l'objet d'une demande d'accès à l'information. Malheureusement, cela ne permet pas de satisfaire le public, qui exige la transparence et la reddition de comptes. Lorsqu'il s'agit de l'utilisation de l'argent des contribuables, de nombreuses raisons valables peuvent justifier la publication de renseignements sur les dépenses de déplacement, de réception et autres des conseillers municipaux.

Au cours de l'année, j'ai écrit au ministre des Services gouvernementaux et au ministre des Affaires municipales et du Logement pour demander au gouvernement provincial d'envisager des modifications possibles à la *LAIMPVP* afin de préciser le statut des documents des conseillers municipaux. On m'a assuré que des travaux sont en cours dans ce sens. Je suis persuadée qu'il est nécessaire d'apporter de telles modifications afin de rendre les documents gouvernementaux plus accessibles au public pour susciter une plus grande confiance.

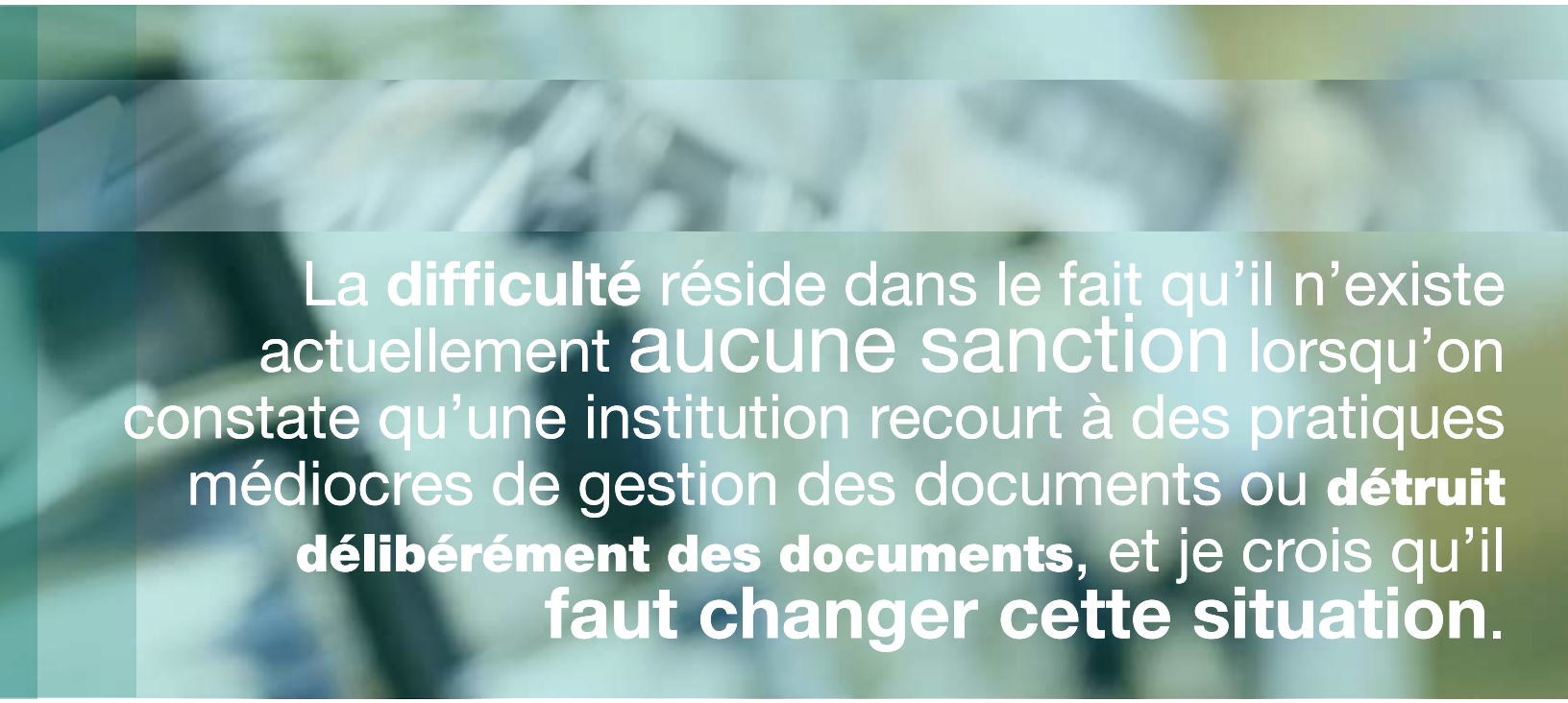
Contrats conclus par le gouvernement

Chaque année, nous recevons un certain nombre d'appels concernant des demandes d'accès à des contrats accordés par des institutions publiques. Ces contrats peuvent porter notamment sur des projets de construction d'infrastructures ou sur l'acquisition de services de sous-traitants, notamment en gestion des déchets, en déneigement et en entretien. Les contrats signés par les institutions représentent des dépenses importantes de fonds publics; il est donc essentiel de faire preuve de transparence. La population ontarienne a le droit de savoir comment son argent est dépensé.

J'ai réclamé à plusieurs reprises la divulgation systématique et proactive des contrats publics. Une telle divulgation renforcerait la transparence et la reddition de comptes relativement aux dépenses gouvernementales et favoriserait la confiance du public. Elle permettrait aussi de réduire considérablement le nombre de demandes d'accès à l'information qui sont présentées au gouvernement et d'appels interjetés devant mon bureau. Je suis ravie de constater que certaines institutions ont tenu compte de mes préoccupations. Ainsi, je crois que la ville de Toronto montre l'exemple, et que d'autres institutions pourraient s'en inspirer.

Malheureusement, de nombreux auteurs de demande ont toujours de la difficulté à accéder aux contrats du gouvernement. Certaines institutions refusent les demandes d'accès à des contrats en invoquant les dispositions de la *LAIPVP* et de la *LAIMPVP* concernant les renseignements de tiers. Les parties contractantes invoquent aussi couramment ces dispositions de sorte que les décisions sont portées en appel devant mon bureau, ce qui retarde inutilement la divulgation des contrats.

J'invite le gouvernement à modifier les *Lois* afin d'éclaircir les clauses invoquées pour refuser l'accès à ces documents et signifier clairement que ces renseignements devraient être publiés de façon proactive, sans qu'il soit nécessaire de faire appel au processus d'accès à l'information.



Nouvelles sanctions en cas d'inobservation des règles de conservation des documents

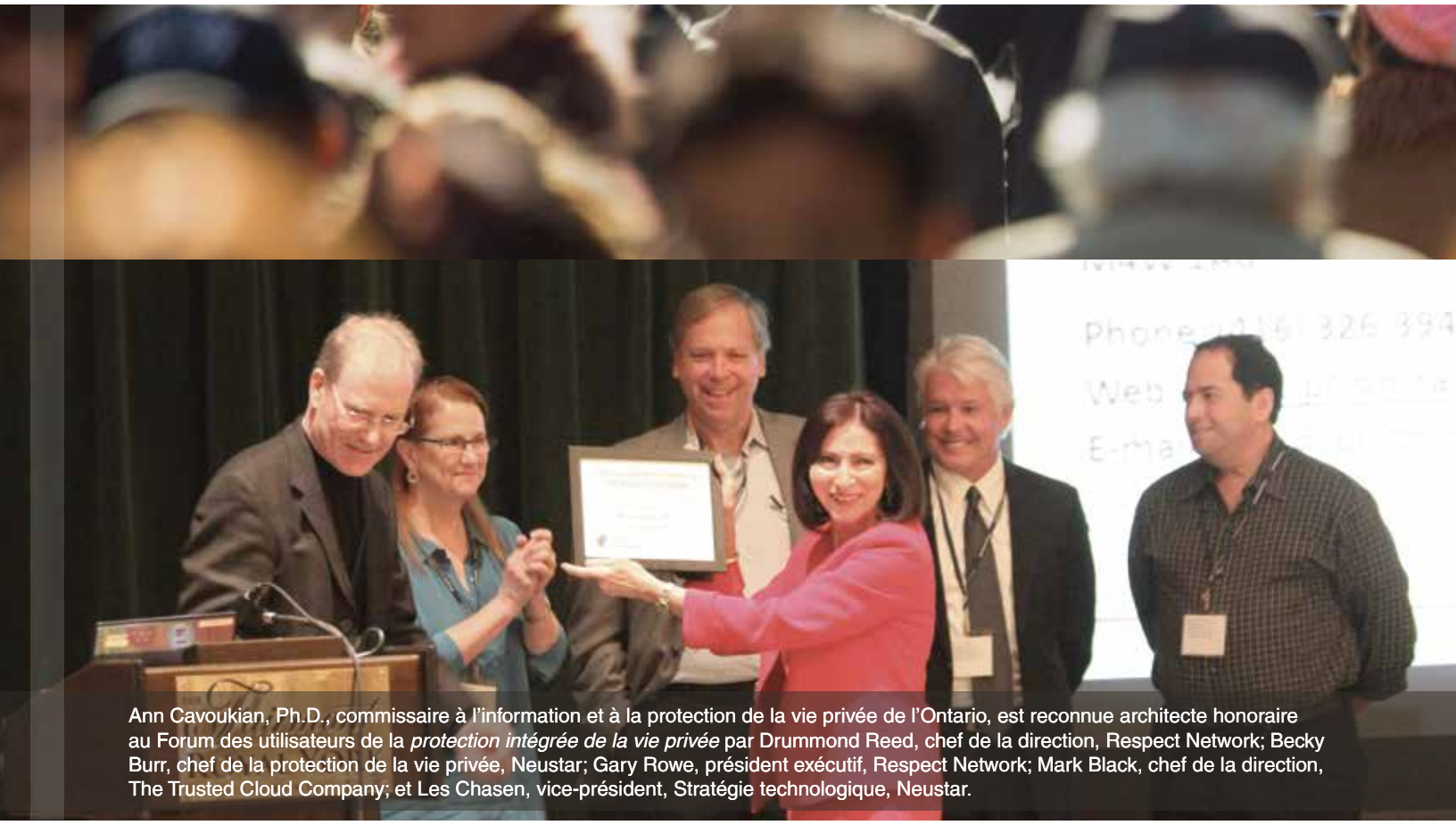
Dans mon rapport d'enquête spécial intitulé *Deleting Accountability: Record Management Practices of Political Staff*, j'ai expliqué qu'au sein du gouvernement, on se préoccupait peu de la nécessité de conserver les documents importants. Mon bureau et les lois sur l'accès à l'information ne peuvent servir efficacement le public que si les institutions conservent des documents et documentent de façon complète leurs décisions importantes. La difficulté réside dans le fait qu'il n'existe actuellement **aucune** sanction lorsqu'on constate qu'une institution recourt à des pratiques médiocres de gestion des documents ou détruit délibérément des documents, et je crois qu'il faut changer cette situation. Pour que le gouvernement demeure transparent et responsable, il faut établir des attentes plus élevées quant à la conservation des documents, renseigner le personnel à l'échelle du gouvernement sur l'obligation de documenter ses activités et prévoir des sanctions plus sévères en cas de tenue inappropriée de registres. Surtout, la destruction délibérée de documents devrait représenter une infraction.

J'ai donc formulé quatre recommandations :

1. Prévoir dans la *LAIPVP* et la *LAIMPVP* l'obligation pour les institutions de documenter leurs activités et de consigner avec exactitude leurs décisions;
2. Obliger toutes les institutions assujetties à la *LAIPVP* et à la *LAIMPVP* à prendre des mesures raisonnables pour conserver de façon sécurisée les documents qui font ou pourraient raisonnablement faire l'objet d'une demande d'accès à l'information en vertu de la *LAIPVP* et de la *LAIMPVP*;
3. Interdire la destruction ou la modification délibérée de documents qui font ou pourraient raisonnablement faire l'objet d'une demande d'accès à l'information en vertu de la *LAIPVP* et de la *LAIMPVP*;
4. Prévoir que toute personne qui détruit ou modifie délibérément des documents qui font ou pourraient raisonnablement faire l'objet d'une demande d'accès à l'information en vertu de la *LAIPVP* et de la *LAIMPVP* se rend coupable d'une infraction en vertu de l'une ou l'autre de ces lois.

La protection de la vie privée doit être intégrée dans les technologies, les pratiques des organisations et la conception matérielle – ce que l'on appelle la *protection intégrée de la vie privée*, qu'il revient à vous et à votre organisation de mettre en œuvre.

PROTECTION INTÉGRÉE DE LA VIE PRIVÉE



Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario, est reconnue architecte honoraire au Forum des utilisateurs de la *protection intégrée de la vie privée* par Drummond Reed, chef de la direction, Respect Network; Becky Burr, chef de la protection de la vie privée, Neustar; Gary Rowe, président exécutif, Respect Network; Mark Black, chef de la direction, The Trusted Cloud Company; et Les Chasen, vice-président, Stratégie technologique, Neustar.

Ambassadeurs de la *protection intégrée de la vie privée*

En 2013, nous avons constaté une hausse considérable du nombre d'ambassadeurs de la *protection intégrée de la vie privée* (*PIVP*). On en compte maintenant plus de 200 dans le monde. Ce sont des gens qui préconisent l'intégration de mesures de protection de la vie privée dans les technologies, les procédés et les infrastructures réseautées. Ce groupe exclusif mais croissant de chefs de file en matière de vie privée se compose d'experts de l'industrie, d'entrepreneurs, d'universitaires, d'ingénieurs, d'innovateurs, d'avocats et de cadres supérieurs.

La même tendance se constate du côté des organisations ambassadrices de la *PIVP*. Nous avons doublé le nombre de ces organisations qui incarnent les sept principes fondamentaux de la *protection intégrée de la vie privée* non seulement dans le cadre de certains projets, mais dans l'essence même de leurs activités. Comme les ambassadeurs individuels, on les retrouve dans le monde entier et dans une foule de domaines. Les organisations ambassadrices procurent des produits et services dans un éventail de secteurs tels que les soins de santé, la technologie, l'infonuagique, l'énergie et la biométrie. Je suis ravie de constater cette croissance de la communauté des ambassadeurs de la *PIVP*. Elle témoigne du fait que la *protection intégrée de la vie privée* est la règle d'or à respecter quand on s'engage à protéger les renseignements personnels.

www.privacybydesign.ca

Le Centre d'excellence en *PIVP* mobilise un **large éventail** de professionnels en vue **d'améliorer** les pratiques de protection de la vie privée...

Centre d'excellence en *protection intégrée de la vie privée*

Privacy by Design Centre of Excellence

PbD Ontario

Le 15 avril 2013, nous avons lancé le Centre d'excellence en *protection intégrée de la vie privée*, une initiative conjointe du ministère des Services gouvernementaux et du Bureau du commissaire à l'information et à la protection de la vie privée (CIPVP). Le Centre d'excellence en *PIVP* a été créé en vue de fournir des ressources et une orientation aux plus de 65 000 membres de la fonction publique de l'Ontario. Depuis avril, il a étendu ses activités au secteur parapublic, et notamment aux hôpitaux, aux municipalités et aux établissements d'enseignement.

Le Centre d'excellence en *PIVP* mobilise un large éventail de professionnels en vue d'améliorer les pratiques de protection de la vie privée pour qu'il soit possible de mieux repérer les nouveaux enjeux, d'améliorer la compréhension générale des pratiques courantes et de renseigner la collectivité. Nous pourrons ainsi faire en sorte que la protection de la vie privée demeure intégrée dans les programmes nouveaux et existants du gouvernement de l'Ontario. L'adoption officielle de la *PIVP* dans l'ensemble du gouvernement permettra sans doute à l'Ontario de maintenir pendant de longues années son rôle de chef de file mondial en protection de la vie privée, et je suis impatiente de prendre connaissance de nouveaux moyens novateurs d'intégrer la *PIVP* dans la technologie, les pratiques et la conception matérielle de nos collectivités.

Nouveaux documents sur la protection *intégrée de la vie privée*

Privacy and Security by Design: A Convergence of Paradigms **:** Ce document décrit la convergence d'une perspective commune en matière de conception pour la protection de la vie privée et la sécurité. Il décrit les similitudes entre les notions de sécurité et de protection de la vie privée, qui se complètent et se renforcent mutuellement.

Privacy by Design and Third Party Access to Customer Energy Usage Data : Ce document porte sur l'accès par des tiers à des données sur la consommation énergétique des abonnés et sur ses avantages de même que sur les risques possibles qu'il pose pour la vie privée. Il passe en revue des produits et services qui pourraient recourir à l'accès par des tiers, et qui pourraient favoriser la conservation d'énergie et ouvrir de nouveaux débouchés.

Looking Forward: De-identification Developments – New Tools, New Challenges : Ce document fait le point sur les derniers développements en matière d'anonymisation et aborde de nouveaux enjeux sur ce sujet.

Surveillance, Then and Now: Securing Privacy in Public Spaces **:** Une approche proactive axée sur la *protection intégrée de la vie privée* est essentielle pour élaborer et mettre en œuvre le cadre réglementaire requis afin d'assurer une supervision appropriée des activités de surveillance que mène l'État au moyen de nouvelles technologies. Ce document propose des ressources aux services policiers, aux législateurs et au grand public pour les aider à comprendre le droit fondamental à la vie privée et à le protéger contre la surveillance des activités auxquelles les citoyens se livrent dans les endroits publics.

A Primer on Metadata: Separating Fact from Fiction **:** Ce document réfute la croyance populaire selon laquelle les renseignements sur les communications personnelles saisis par des organismes gouvernementaux, dont la National Security Agency (NSA) des États-Unis, ne sont pas délicats et ne représentent pas une menace à la vie privée car ils ne sont « que des métadonnées ». Il propose des mesures proactives visant à permettre à la fois la protection de la vie privée et la sécurité et à renforcer la reddition de comptes, l'encadrement et la transparence des organismes gouvernementaux.

Privacy by Design: Fundamentals for Smart Grid App Developers **:** Dans ce document, nous adressons aux réalisateurs d'applications pour le réseau intelligent de transport d'électricité un document de base sur la *protection intégrée de la vie privée.* S'ils utilisent ses principes, non seulement les clients auront confiance en leurs applications, mais ils

se démarqueront en tant qu'adopteurs précoces et chefs de file de l'intégration de mesures de protection de la vie privée dans les applications pour le réseau intelligent de transport d'électricité.

Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism **:** En illustrant la méthodologie sur laquelle s'appuie la surveillance sans atteinte à la vie privée, nous cherchons à démontrer dans ce document que contrairement aux apparences, il est possible de respecter la vie privée tout en luttant efficacement contre le terrorisme. En effet, nous disposons des technologies de pointe nécessaires, et nous pouvons élaborer un système pour atteindre cet objectif qui est avantageux pour tout le monde.

Privacy and Security by Design: An Enterprise Architecture Approach **:** Les données étant de plus en plus menacées, les moyens employés autrefois pour les protéger, qui consistaient simplement à ériger un « périmètre » défensif autour d'une ressource, ne suffiront plus. Ce document montre que l'on doit passer à l'offensive en matière de sécurité, et que les entreprises et organisations se doivent de tenir compte systématiquement des préoccupations touchant à la fois la sécurité et la protection de la vie privée.

Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control **:** L'écosystème de données personnelles (EDP) est un concept qu'adopte un nombre croissant d'entreprises et d'organisations qui sont convaincues que les particuliers doivent assumer le contrôle de leurs données personnelles, et qui mettent pour ce faire de plus en plus d'outils et de technologies à leur disposition.

Privacy Exposures and Risk Reduction Strategies for Small Organizations : Une organisation s'exposera toujours à des risques à moins de prévoir une stratégie pour assurer la mise en œuvre concrète de ses politiques et procédures de protection de la vie privée. Dans les petites entreprises, il est essentiel d'appliquer les concepts fondamentaux de la *protection intégrée de la vie privée* pour éviter les écueils des fuites de données.

Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design **:** Ce document définit les sept éléments de base des mesures strictes de protection de la vie privée et illustre comment elles s'appliquent aux défis uniques que présentent les mégadonnées dans le contexte de l'écosystème de données personnelles.

(Bring Your Own Device) Is Your Organization Ready? **:** Fidèle au principe de sécurité de bout en bout de la *protection intégrée de la vie privée*, ce document décrit les risques liés à la gestion de l'information et propose des conseils pratiques afin de les atténuer. Bien qu'il n'existe aucune solution toute faite, ce document énonce un processus complet à cinq étapes permettant aux organisations de mettre en œuvre un programme « prenez vos appareils personnels » qui permet d'assurer à la fois la protection de la vie privée et la sécurité.

Nous pouvons, et nous devons, faire en sorte que la sécurité et la protection de la vie privée aillent de pair. L'une ne doit pas être privilégiée au détriment de l'autre.

QUESTIONS CLÉS

Enquête du CIPVP – Deleting Accountability: Record Management Practices of Political Staff

L'accès à l'information est essentiel dans une société libre et démocratique. Il permet de se renseigner sur les activités du gouvernement et de savoir à quoi est consacré l'argent des contribuables. L'absence de documents sur les principales décisions du gouvernement porte atteinte à la transparence, et peut soustraire à l'examen public le fondement des politiques établies.

Au cours du dernier exercice, mon bureau a eu la tâche peu enviable de faire enquête sur les pratiques de tenue de dossiers de membres clés du personnel de l'ancien premier ministre et de l'ancien ministre de l'Énergie. Nous avons entamé notre enquête en avril aussitôt après avoir reçu une plainte d'un député provincial. D'après les allégations, l'ancien chef de cabinet du ministre de l'Énergie avait supprimé abusivement tous les courriels concernant l'annulation et la relocalisation des centrales au gaz d'Oakville et de Mississauga. Il était remarquable que le ministère de l'Énergie et l'Office de l'électricité de l'Ontario (OEO) aient déposé plus de 56 500 pages de documents auprès d'un comité législatif chargé de la question des centrales au gaz, et que le personnel politique du bureau du ministre de l'Énergie n'en ait déposé aucun.

Lors d'une entrevue, l'ancien chef de cabinet nous a dit qu'il supprimait systématiquement tous les courriels pour que sa boîte de réception soit toujours « propre ». Il était difficile d'accepter que cette suppression systématique de courriels n'était pas en réalité une façon d'éviter de faire preuve de transparence et de rendre compte de son travail, et que cette pratique n'était qu'une façon banale de gérer efficacement son compte de courriel.

Pendant les entrevues que nous avons menées dans le cadre de notre enquête, nous avons rencontré le secrétaire du Conseil des ministres. Nous avons appris qu'au début de 2013, lorsque le personnel de l'ancien premier ministre se préparait à l'entrée en fonction de la nouvelle première ministre, le chef de cabinet de l'ancien premier ministre a posé au secrétaire

du Conseil des ministres des questions sur la façon de « nettoyer les disques durs du Cabinet du Premier ministre ». Le secrétaire l'a informé de ses obligations, mais je redoutais que des documents électroniques n'eussent été supprimés par des membres du personnel de l'ancien premier ministre. J'ai donc décidé d'élargir la portée de mon enquête.

Le chef de cabinet de l'ancien premier ministre m'a appris, lors de nos discussions, qu'il appliquait une politique semblable consistant à supprimer ses courriels tous les jours. Je ne suis pas en mesure d'affirmer avec certitude que les membres du personnel de l'ancien premier ministre ont supprimé de façon abusive des documents électroniques sauvegardés sur disque dur lors de la transition en vue de l'entrée en fonction de la nouvelle première ministre, mais compte tenu de leurs pratiques de gestion des courriels, j'ai pu constater à tout le moins qu'ils ne remplissaient pas leurs obligations en matière de conservation des documents.

Pendant l'enquête, nous avons tenu des discussions approfondies avec le ministère des Services gouvernementaux (MSG) sur la façon dont étaient stockés et sauvegardés les fichiers électroniques et les courriels. Nous espérions pouvoir récupérer les courriels supprimés; or, on nous a dit qu'ils avaient été supprimés définitivement et qu'il était essentiellement impossible de les récupérer.

Après mon examen des enjeux soulevés lors de cette enquête et des indications que nous avons recueillies, j'ai constaté avec inquiétude une absence apparente de responsabilité et de reddition de comptes en matière de gestion des documents dans les bureaux des principaux dirigeants politiques de la province. Il ne fait aucun doute que les pratiques de gestion des courriels du bureau de l'ancien ministre et du cabinet de l'ancien premier ministre allaient à l'encontre de la *Loi de 2006 sur les Archives publiques et la conservation des documents* (*LAPCD*) et du calendrier de conservation des documents que les Archives publiques de l'Ontario avaient dressé pour les bureaux des ministres.

Cette pratique était également contraire au droit d'accès aux documents gouvernementaux dont jouit le public en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) ainsi qu'aux principes de transparence et de reddition de comptes sur lesquels s'appuient les deux *Lois*. J'estimais qu'il fallait apporter des changements aux politiques et aux processus de formation du personnel des bureaux des ministres. J'étais également préoccupée par l'absence, dans le cabinet de l'ancien premier ministre et le bureau de l'ancien ministre de l'Énergie, d'une

personne responsable des pratiques de gestion des documents qui rappellerait au personnel politique de ces bureaux ses obligations.

Dans mon rapport intitulé *Deleting Accountability: Records Management Practices of Political Staff*, qui a été publié en juin, j'ai recommandé que le gouvernement prenne des mesures concrètes dans trois domaines spécifiques afin de veiller à ce que les dossiers susceptibles de faire l'objet d'une demande d'accès en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) et de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (*LAIMPVP*) soient conservés:

- Cabinet du Premier ministre – Prendre une directive prévoyant qu'au bureau de tous les ministres et au Cabinet du Premier ministre, un haut fonctionnaire soit désigné responsable des politiques et des pratiques de conservation des documents et veille à ce que les employés des ministres reçoivent une formation sur leurs obligations en matière de gestion des dossiers.
- Modifications législatives – Modifier la *LAIPVP* et la *LAIMPVP* afin d'imposer aux institutions la responsabilité de s'assurer que toutes les décisions clés sont documentées et que les documents sont conservés de façon sécurisée, et de faire en sorte que la destruction délibérée ou inappropriée de documents constitue une infraction grave.
- Politiques de conservation des documents – Effectuer un examen des politiques et des pratiques de conservation des dossiers des Archives publiques de l'Ontario applicables aux processus de gestion des dossiers des bureaux des ministres et du Cabinet du Premier ministre, afin d'établir clairement l'obligation de conserver les documents officiels ou internes.

Après la publication de mon rapport, j'ai reçu de nouveaux renseignements sur le système de courrier électronique de la fonction publique de l'Ontario qui auraient dû m'avoir été fournis pendant mon enquête. J'ai également appris que les membres du personnel du MSG avaient négligé de mener une enquête approfondie lorsque j'ai abordé la possibilité de récupérer les courriels supprimés. Ils étaient persuadés que leur processus de gestion de l'information avait fonctionné correctement et que les courriels avaient été définitivement supprimés. Je croyais que le MSG avait fait le travail qui s'imposait avant de tirer cette conclusion, et j'ai donc accepté sa réponse. Or, ce n'est qu'en réponse aux motions déposées devant le Comité permanent de la justice que le personnel du ministère a fait preuve d'une dil-

igence raisonnable et a cessé de s'en remettre simplement aux politiques établies. J'ai été atterrée d'apprendre qu'on nous avait fourni des renseignements inexacts, tout en étant satisfaite que d'autres documents aient été localisés. J'ai donc publié en août un addenda en complément de mon rapport décrivant les circonstances entourant la divulgation de ces nouveaux renseignements. J'y ai souligné que le sous-ministre des Services gouvernementaux m'avait présenté ses excuses et avait assumé l'entière responsabilité de cette situation. Ces événements et les nouveaux renseignements recueillis n'ont eu aucune incidence sur les recommandations énoncées dans mon rapport initial, qui demeuraient valables et n'ont pas été modifiées.

Depuis la conclusion de mon enquête, j'ai apprécié la coopération dont la première ministre Kathleen Wynne et le ministre des Services gouvernementaux ont fait preuve en vue d'appliquer les recommandations que j'ai formulées dans mon rapport. Au début de septembre, la première ministre a publié une directive conforme à mes recommandations et a engagé le gouvernement à rehausser la transparence et la reddition de comptes grâce à des pratiques de tenues de dossiers considérablement améliorées. En outre, le personnel des cabinets ministériels a reçu une formation approfondie sur ses responsabilités en matière de conservation des documents. Je suis ravie de ces mesures et je suis impatiente de passer en revue le fruit des recherches du gouvernement sur les modifications législatives que j'ai recommandées.

Faute de documents sur les fondements des décisions gouvernementales importantes, le gouvernement peut éviter toute divulgation, transparence et examen public quant aux motifs de ses actes. Sans examen public, il y a peu de reddition de comptes, ce qui met en péril la liberté et la démocratie. Ces actes empêchent également le public de participer de façon éclairée et significative au processus démocratique et mine sa confiance dans le gouvernement. J'espère qu'après la mise en œuvre de ces recommandations, les documents concernant les décisions importantes du gouvernement seront bien conservés, et que jamais plus il ne sera nécessaire de mener à nouveau une pareille enquête.

La surveillance de masse : le combat pour la transparence et les mesures de protection de la vie privée

Cette année, les questions touchant la surveillance et la collecte de métadonnées ont occupé l'avant-plan de l'actualité. D'après les révélations d'Edward Snowden, les Canadiens, encore plus que les Américains, sont laissés dans l'ignorance quant aux activités de leur gouvernement. En effet, nous en savons étonnamment peu sur ce que notre gouvernement, et les agences de renseignement étranger, font de nos renseignements personnels. Il est troublant que cette question importante ait suscité si peu de débats, particulièrement au Parlement. Ces révélations auraient dû donner lieu à des initiatives d'information du public et à des mesures décisives. Mon bureau a relevé ce défi, et a préconisé un débat national franc, approfondi et immédiat à ce sujet.

Pourtant, l'année s'était ouverte sur une véritable victoire pour la protection de la vie privée et la liberté. Le gouvernement fédéral avait confirmé le retrait du projet de loi C-30, qui aurait permis à la police d'accéder sans mandat à des renseignements sur les abonnés. Ces dernières années, j'ai dénoncé à maintes reprises le fait que ce projet de loi aurait porté atteinte au droit à la vie privée des Canadiennes et des Canadiens, notamment en ligne et lors de l'utilisation d'appareils mobiles.

Je me suis ensuite attardée à la question importante de la surveillance accrue du public grâce à de nouvelles technologies. La surveillance constante de gens qui se livrent à leurs activités quotidiennes dans les lieux publics représente, comme l'a dit de façon mémorable le juge Gérard La Forest, « une perspective impensable dans une société libre et ouverte comme la nôtre ». Quelques jours avant les révélations de Snowden, nous avons publié un nouveau libre blanc, *Surveillance, Then and Now: Securing Privacy in Public Spaces*. Ce document vise à aider la police, les législateurs et le grand public à comprendre et à protéger notre droit fondamental à la vie privée dans le cadre de la surveillance par l'État de nos activités publiques et en ligne au moyen de nouvelles technologies de plus en plus répandues. Il explique qu'une approche proactive fondée sur la *protection intégrée de la vie privée* est essentielle pour concevoir et mettre en œuvre la réglementation requise pour bien encadrer cette surveillance.

Au cours des semaines et des mois qui ont suivi, grâce à Edward Snowden, il est devenu évident que ces menaces à la vie privée étaient beaucoup plus sérieuses qu'on aurait pu l'imaginer. La surveillance généralisée du public et la collecte

systématique de données de communication représentent une grave menace à la vie privée et aux libertés civiles. Or, des journalistes et le gouvernement ont minimisé cette situation en affirmant que l'on ne recueillait « que des métadonnées », sans décrire précisément de quoi il s'agit. J'ai donc publié le document *A Primer on Metadata: Separating Fact from Fiction* qui explique clairement que les métadonnées peuvent être en fait plus révélatrices que le contenu des communications en tant que tel. Ce document décrit clairement ce que sont les métadonnées et remet en question les affirmations selon lesquelles les renseignements recueillis ne sont pas délicats et ne portent pas atteinte à la vie privée car ils ne permettent pas d'accéder au contenu. Le jour de sa publication, en juillet, j'ai publié un article d'opinion dans le *Toronto Star* pour en décrire les points saillants.

À mesure que les révélations se sont poursuivies, jetant un éclairage sur le rôle du Centre de la sécurité des télécommunications Canada (CSTC), mon bureau a cherché à sensibiliser la population au besoin urgent d'assurer un encadrement adéquat. Moi et les coauteurs Ron Deibert, Andrew Clement et Nathalie Des Rosiers avons rédigé un article d'opinion qui a paru dans le *Globe and Mail* sous le titre *Real Privacy Means Real Oversight* dans lequel nous réclamions un débat approprié à la Chambre des communes et annoncions un symposium public qui a eu lieu à l'occasion de la Journée internationale de la vie privée, le 28 janvier 2014. Ce symposium avait pour but d'ouvrir de nouvelles voies et d'entamer un dialogue plus ouvert avec tous les organismes de sécurité et de renseignement et, surtout, le public.

Pour trouver une solution à ce problème complexe, j'ai collaboré avec le professeur Khaled El Emam à un nouveau concept de surveillance, la surveillance sans atteinte à la vie privée. Présentée au début de septembre, cette méthodologie propose une solution de rechange à somme positive (et non à somme nulle) aux systèmes actuels de surveillance antiterroriste. La plupart des mesures de lutte au terrorisme cherchent à parvenir à un « équilibre » entre la sécurité publique et la protection de la vie privée. Or, cela aboutit souvent à un paradigme à somme nulle qui consiste à abandonner ce que l'on considère comme étant le « moins important », c'est-à-dire la protection de la vie privée, au profit de ce qui compte le plus, soit la sécurité publique. Ce compromis à somme nulle est toujours destructeur dans une société libre et ouverte. Non seulement il n'est pas approprié, mais il est inutile. La protection de la vie privée et la lutte au terrorisme peuvent coexister dans le respect de leurs valeurs respectives. Nous savons que cet objectif est réalisable.

Malheureusement, à la fin de 2013, le gouvernement fédéral a décidé de se servir de la cyberintimidation come prétexte pour déposer à nouveau une bonne partie des dispositions du projet de loi C-30 sur la surveillance. Par contre, le projet de loi C-13 ne donne pas à la police la possibilité d'accéder sans mandat aux renseignements sur les abonnés ni n'établit de capacité minimum obligatoire d'interception comme l'ancien projet de loi. En outre, la plupart des pouvoirs proposés seront assujettis à une forme de surveillance judiciaire. Cependant, les pouvoirs de surveillance que prévoit le projet de loi C-13 misent sur des technologies qui sont nouvelles ou encore en développement. Par conséquent, ils ont pour effet d'accroître considérablement la capacité de surveillance de l'État et non simplement de la maintenir. J'ai donc renouvelé mon invitation à créer un organisme indépendant de surveillance et d'examen doté d'un mandat législatif fort, qui superviserait et examinerait l'accès de l'État à des renseignements personnels très délicats associés aux communications numériques et qui rendrait compte chaque année au Parlement et au public de l'utilisation de ces pouvoirs de surveillance et d'accès.

Les propositions visant à accroître la surveillance doivent être doublées de garanties législatives. Ainsi, les tribunaux, les personnes touchées, les législatures futures et le public doivent être bien informés de la portée, de l'efficacité et des torts éventuels de ces pouvoirs. Supervisés adéquatement, les pouvoirs de surveillance intérieure peuvent se révéler précieux pour les organismes de sécurité. Cependant, il est vrai aussi que les personnes innocentes qui font l'objet de soupçons injustifiés, ou à l'égard desquels on invoque abusivement des éléments de preuve ou tire hâtivement des conclusions fausses, peuvent en subir des conséquences désastreuses. Nous pouvons, et nous devons, faire en sorte que la sécurité et la protection de la vie privée aillent de pair. L'une ne doit pas être privilégiée au détriment de l'autre. Il importe de tenir compte de la valeur véritable de la protection de la vie privée et idéalement de l'améliorer au lieu de la diminuer – chaque fois qu'on s'efforce de moderniser les pouvoirs d'application de la loi.

Appel à l'action lancé

En 2013, Edward Snowden a fait une série presque interminable de révélations sur la National Security Agency (NSA) des États-Unis. Cependant, cette affaire au départ strictement américaine a eu tôt fait de devenir canadienne également, car il est devenu évident que notre propre service de renseignement étranger, le Centre de la sécurité des télécommunications Canada (CSTC), avait participé à de nombreux programmes avec la NSA et ses autres partenaires du Groupe des cinq (le Royaume-Uni, l'Australie et la Nouvelle-Zélande). L'un de ces programmes consistait à aider la NSA à créer une porte dérobée dans les outils de chiffrement approuvés par le gouvernement, nous rendant ainsi tous plus vulnérables à la surveillance de l'État. Le CSTC a également contribué aux activités d'espionnage de la NSA lors du sommet du G8 tenu à Toronto en juin 2010. Au début de 2014, nous apprenions aussi que le CSTC avait élaboré un outil de surveillance « révolutionnaire » faisant appel à des métadonnées associées à des personnes qui utilisaient l'accès Wi-Fi gratuit dans un grand aéroport canadien. Le CSTC a affirmé que cette activité était « légale » car il recueillait uniquement des « métadonnées ». Cette affirmation a été vertement remise en cause et doit continuer de l'être, car les métadonnées sont parfois plus révélatrices que le contenu même des communications.

Il ressort que nous avons laissé le CSTC conduire ses activités avec encore moins d'encadrement que la NSA. Ses pouvoirs en matière d'espionnage représentent une menace au droit à la vie privée dont jouissent les Canadiennes et les Canadiens. Nous méritons et nous exigeons de connaître la portée des programmes d'espionnage du CSTC. Nous devons poser des questions essentielles : Jusqu'où vont nos organismes de sécurité sous prétexte de protéger la sécurité publique? De quoi sont-ils capables? Ces techniques envahissantes sont-elles employées pour espionner les Canadiennes et les Canadiens au pays ou à l'étranger? Le CSTC recueille-t-il souvent des renseignements personnels tels que des métadonnées, et à quels organismes d'exécution de la loi et de renseignement les fournit-il?

Les révélations d'Edward Snowden ont suscité un débat rigoureux au Congrès américain et ont donné lieu à des déclarations de la Maison-Blanche et à plusieurs

poursuites judiciaires. En outre, elles ont poussé quelques-unes des entreprises de technologie les plus importantes au monde à faire équipe pour exiger des changements. Cependant, la réaction au Canada a été très décevante. Presque tous les grands journaux canadiens ont réclamé dans leurs éditoriaux une transparence et un encadrement accrus, mais le gouvernement actuel ainsi que le CSTC ont peu réagi et commenté. C'est tout à fait inacceptable!

Dans une société libre et ouverte, les gouvernements doivent faire preuve de transparence et être accessibles aux citoyens. Chercher à se soustraire à la surveillance du public par souci de sécurité, c'est non seulement faire fausse route, mais c'est aussi choisir la voie de la facilité. Il faut rappeler au gouvernement fédéral qu'il est en poste au gré de la population, et que les citoyens ont le droit d'être bien informés de ses activités. Par contre, les gouvernements ne doivent pas jouir d'un accès systématique aux renseignements concernant leurs citoyens. Ils doivent y accéder uniquement quand des lois l'autorisent, et ces lois doivent être claires et protéger la vie privée. Parmi ces protections essentielles, il doit y avoir un encadrement judiciaire indépendant du pouvoir intrusif de l'état en matière de surveillance. À l'heure actuelle, la seule mesure de reddition de comptes et de transparence à laquelle le CSTC est assujetti consiste en un examen annuel unique et vague, effectué par une seule personne disposant d'un personnel peu nombreux. C'est tout à fait inadéquat pour des programmes qui pourraient porter atteinte à la liberté de toute la population canadienne. Il nous faut au minimum un nouveau mandat législatif pour établir une structure de responsabilité claire.

Les sacrifices d'Edward Snowden nous ont appris que le pouvoir incontrôlé de l'État comporte des risques considérables. Je demande à tous les Canadiens et Canadiennes d'exiger des réponses de nos dirigeants. Nous devons ouvrir une nouvelle voie et entamer un dialogue plus ouvert avec le public afin de préserver la vie privée et les libertés civiles. Nous devons continuer de mobiliser par tous les moyens les citoyens et les élus. Il faut dire haut et fort « respectez notre vie privée, respectez nos libertés ». Nous ne méritons rien de moins dans une société libre et démocratique.

L'anonymisation : un outil efficace pour protéger la vie privée

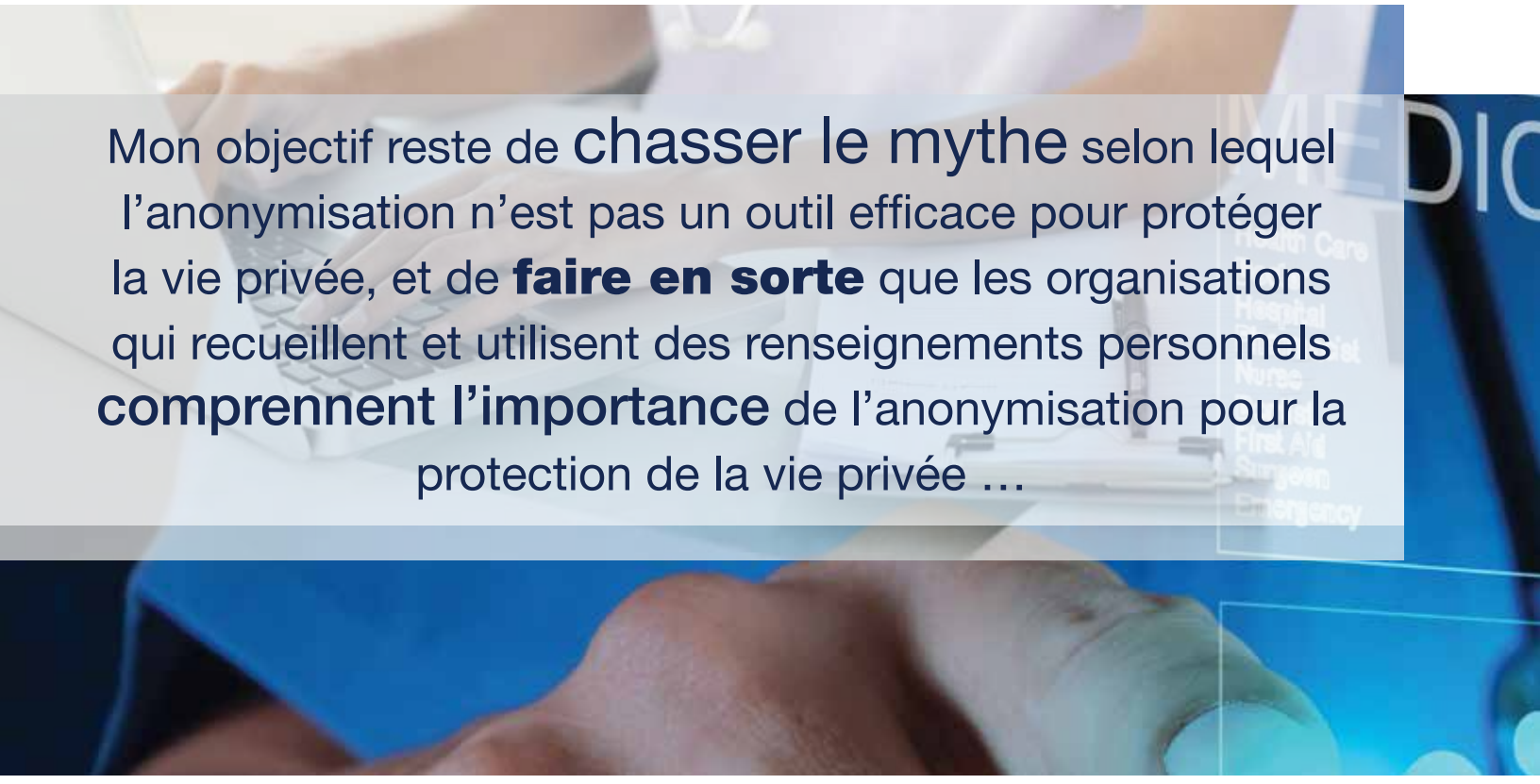
En 2013, j'ai poursuivi ma campagne visant à promouvoir l'anonymisation des données comme outil crucial de protection de la vie privée et à chasser les mythes entourant la désanonymisation en lançant le *Centre d'anonymisation fondée sur la protection intégrée de la vie privée.*

L'anonymisation est un outil précieux qui réduit considérablement le risque que des renseignements personnels ne soient utilisés ou divulgués à des fins non autorisées ou malveillantes tout en permettant l'utilisation de ces renseignements à des fins secondaires autorisées, avantageuses pour les particuliers et l'ensemble de la société. Il est possible d'effectuer cette anonymisation de façon à réduire le risque de désanonymisation et à maintenir la qualité des données. Cela nous permet de passer d'un paradigme à somme nulle à un paradigme à somme positive, une solution avantageuse pour tout le monde qui est à la base de la *protection intégrée de la vie privée.*

Par exemple, l'anonymisation se révèle particulièrement utile du côté des renseignements personnels sur la santé, qui sont très délicats et portent sur les aspects les plus personnels de la vie. Les renseignements personnels sur la santé nécessitent les mesures de protection de la vie privée et de sécurité les plus strictes afin d'éviter leur collecte, leur utilisation et leur divulgation non autorisées. Cependant, dans des circonstances appropriées, il importe aussi de permettre l'accès à des renseignements personnels sur la santé à des fins secondaires qui revêtent un grand intérêt public, notamment pour la recherche sur le cancer.

Chasser les mythes

Contrairement à ce que prétendent certains détracteurs, il n'est ni « facile » ni « trivial » de désanonymiser des renseignements qui ont été correctement anonymisés. Y parvenir nécessite des efforts concertés de la part de techniciens chevronnés. Je l'explique très clairement dans un document que j'ai rédigé avec le professeur Khaled El Emam intitulé *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy,* en réponse à un nombre crois-



sant d'allégations selon lesquelles il est facile de désanonymiser des renseignements. Ce document propose même un outil qui réduit le risque de désanonymisation tout en préservant la qualité des données.

Mon objectif reste de chasser le mythe selon lequel l'anonymisation n'est pas un outil efficace pour protéger la vie privée, et de faire en sorte que les organisations qui recueillent et utilisent des renseignements personnels comprennent l'importance de l'anonymisation pour la protection de la vie privée et continuent de s'en servir dans toute la mesure du possible afin de minimiser les risques éventuels. Bien que je me concentre surtout sur l'importance de l'anonymisation dans le contexte des renseignements personnels sur la santé, les mêmes arguments sont valables dans le contexte plus général des renseignements personnels employés par les gouvernements, les entreprises et d'autres organisations.

Cependant, comme les techniques de désanonymisation deviennent plus perfectionnées et que de plus en plus de renseignements personnels sont accessibles, ce qui facilite la désanonymisation, il est important de réévaluer et de renforcer l'anonymisation et les techniques de gestion des risques de désanonymisation. Dans la grande majorité des cas, l'anonymisation protège la vie privée des particuliers, dans la mesure où des précautions appropriées sont prises. L'anonymisation n'est pas nécessairement une solution parfaite pour réduire tous les risques d'atteinte à la vie privée lorsqu'on envisage d'utiliser des renseignements personnels à des fins secondaires, mais elle représente une première mesure importante à employer dans le cadre d'un régime global d'évaluation des risques.

Centre d'anonymisation fondée sur la protection intégrée de la vie privée

Pour promouvoir le concept d'anonymisation et favoriser l'adoption de techniques appropriées et de pratiques exemplaires, j'ai lancé, à l'été 2013, le *Centre d'anonymisation fondée sur la PIVP*. Je voulais démontrer la nécessité de l'anonymisation et sensibiliser les gens à son importance vitale comme mécanisme clé de protection de la vie privée. Je voulais aussi créer une tribune où les participants pourraient débattre d'idées et d'études afin que la communauté de la protection de la vie privée reste à l'avant-garde des dernières techniques d'anonymisation et procédures de gestion des risques de désanonymisation. Enfin, je souhaitais aussi favoriser l'innovation et l'échange de connaissances afin d'assurer la protection de la vie privée aujourd'hui et dans l'avenir. J'invite donc tous les intéressés à participer activement au *Centre d'anonymisation fondée sur la PIVP.* Si vous avez une idée ou une question, vous pouvez soumettre un billet de blogue de 350 à 500 mots à **pbd@ipc.on.ca** pour amorcer un débat ou aborder un sujet particulier.


Medical and Surgical History of the Civil War
Index
4-E
L-Z
Civil War Eyewitnesses Books and Articles, 1957-1959
1
2
3
Military Order of the Loyal Legion of the United States

L'absence de documents sur les principales décisions du gouvernement porte atteinte à la transparence, et peut soustraire à l'examen public le fondement des politiques établies.

ACCÈS À L'INFORMATION

Les avantages économiques et sociaux des données ouvertes

Le mouvement mondial des données ouvertes met gratuitement à la disposition du public de grandes quantités de données lisibles par machine. Il s'agit de l'une des applications les plus fidèles des principes de l'*accès à l'information intégré*, qui encourage les institutions publiques à divulguer des renseignements proactivement dans le cadre d'un processus automatique au lieu d'attendre de recevoir des demandes d'accès à l'information. Ce mouvement préconise une transparence et une reddition de comptes accrue au sein des gouvernements et crée de nouvelles possibilités de mobilisation des citoyens.

En septembre dernier, pour souligner la Semaine du droit à l'information 2013, j'ai tenu un événement au Toronto Region Board of Trade soulignant les réalisations du mouvement des données ouvertes. Cet événement visait à démontrer les énormes retombées économiques d'un gouvernement ouvert et à illustrer les avantages que la divulgation automatique de renseignements au public peuvent rapporter aux gouvernements et aux autres organismes. Des conférenciers ont expliqué comment des gouvernements et des innovateurs ont opérationnalisé les données ouvertes pour mieux servir la collectivité. Ces programmes mobilisent les citoyens, procurent des renseignements utiles aux entreprises et stimulent l'innovation en motivant la création de nouveaux produits et services.

Ron McKerlie, sous-ministre, gouvernement ouvert au ministère des Services gouvernementaux, a fait part de la vision de l'Ontario concernant les données et renseignements ouverts et le dialogue avec le public. Au cours des prochaines années, le gouvernement cherchera à mobiliser le public en instaurant de nouveaux outils à des fins de consultation, élaborera des politiques, programmes et services mieux adaptés, assurera un accès plus efficace aux services, données et renseignements du gouvernement et favorisera la croissance économique en veillant à ce que les données et les renseignements soient accessibles sous une forme utile. Je félicite le gouvernement de souscrire aux principes du gouvernement ouvert et je l'invite à faire de l'Ontario un chef de file et non un suiveur en la matière.

Nancy Isozaki, de la ville de Toronto, a décrit les nombreuses initiatives de diffusion d'information qui ont fait de Toronto un chef de file en la matière au Canada. Ainsi, la ville affiche en ligne tous les ordres du jour et rapports du conseil municipal, permettant aux citoy-

Ron McKerlie, sous-ministre, gouvernement ouvert, ministère des Services gouvernementaux

Nancy Isozaki, directrice des politiques municipales en matière d'information, ville de Toronto

Stéphane Guidoin, directeur en solutions de transport, Nord Ouvert

ens de faire le suivi des enjeux, de se renseigner sur la façon dont les conseillers ont voté et de s'inscrire pour prendre la parole sur un point porté à l'ordre du jour.

Rob Giggey a montré comment les concours Apps pour Ottawa de la ville d'Ottawa ont mené à la création de 39 applis pour le public au moyen des données ouvertes de la ville. L'une des applications primées permet de sélectionner les meilleures activités récréatives, et une autre permet de surveiller les activités des lobbyistes.

Joe Greenwood, du District de la découverte MaRS, a montré comment les données ouvertes peuvent favoriser l'efficacité et réaliser des économies dans les domaines des soins de santé, du transport et de l'énergie. L'Initiative ontarienne du bouton vert, dans le cadre de laquelle 20 entreprises élaborent des solutions de contrôle de la consommation d'énergie pour les consommateurs en se fondant sur des données anonymisées provenant de 2,7 millions de foyers et d'entreprises, a suscité beaucoup d'intérêt.

Dennis Brink, directeur général de l'Institut des données ouvertes du Canada, a abordé le succès de Propertize.ca, un site Web qui permet au public de comparer l'évaluation foncière de différentes propriétés à partir de renseignements ouverts.

Stéphane Guidoin de Nord Ouvert a abordé l'importance sociale considérable que revêtent les programmes de données ouvertes. Son organisme a contribué à implanter le *Budget Citoyen,* un simulateur budgétaire interactif qui fait participer les citoyens au processus budgétaire, dans les sites Web de diverses municipalités d'Amérique du Nord.

Il était encourageant de constater l'essor continu du mouvement des données ouvertes, et de voir tant d'organisations adopter mon concept d'*accès à l'information intégré.* Je continuerai d'inviter les institutions publiques à faire preuve de plus de transparence et à divulguer au public le plus possible de renseignements.

Faits saillants sur des ordonnances de 2013

Loi municipale

MO-2848
Ville de Toronto

Deux auteurs de demande des médias ont demandé l'accès au registre d'utilisation du laissez-passer dont se sert le maire de Toronto pour se stationner à l'hôtel de ville. La ville a refusé l'accès à ce document, affirmant que sa divulgation représenterait une atteinte injustifiée à la vie privée, ferait obstacle à des questions touchant l'exécution de la loi et constituerait une menace à la santé ou à la sécurité. Dans cette ordonnance, l'arbitre a établi que ce document n'est pas visé par ces exceptions et a ordonné sa divulgation aux auteurs de demande. L'arbitre a notamment établi que les renseignements contenus dans le registre ne sont pas des renseignements personnels.

MO-2964-I
Ville du Grand Sudbury

La ville a reçu six demandes d'accès aux contrats d'emploi « actuels et antérieurs » de six employés nommés de la ville. Celle-ci a rendu une décision qui a soulevé un certain nombre de questions. Cette ordonnance portait sur les questions relatives à l'accès aux contrats d'emploi actuels des six employés nommés qui, selon la ville, ne pouvaient être divulgués car ils révéleraient l'essentiel de délibérations tenues à huis clos. L'arbitre a établi que ces contrats d'emploi n'étaient pas visés par cette exception. Bien que les contrats signés représentent le *produit* de délibérations tenues à huis clos, ils ne révèlent pas la *substance* de ces délibérations. L'arbitre a également établi que les parties de ces documents qui décrivent les avantages sociaux devaient être divulguées. Il a pris en délibéré la question de l'accès aux autres parties des documents.

Loi provinciale

PO-3233
Université Carleton

Un média a présenté une demande d'accès à des renseignements particuliers sur des notes d'étudiants pour la période allant de 1999 à 2011. L'université a refusé l'accès à ces renseignements en affirmant que leur divulgation porterait une atteinte injustifiée à la vie privée des étudiants ou nuirait aux intérêts économiques ou à la situation concurrentielle de l'université. Dans

L'accès à l'information intégré et le mouvement des données ouvertes : des avantages sociaux et économiques tangibles – Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario; Ron McKerlie, sous-ministre, gouvernement ouvert, ministère des Services gouvernementaux; Nancy Isozaki, directrice des politiques municipales en matière d'information, services municipaux de gestion de l'information, ville de Toronto; Rob Giggey, coordonnateur, Soutien stratégique et responsable des données ouvertes, ville d'Ottawa; Stéphane Guidoin, directeur en solutions de transport, Nord Ouvert; Joe Greenwood, directeur des programmes, District de la découverte MaRS; Dennis Brink, directeur général, Open Data Institute of Canada.

cette ordonnance, l'arbitre a établi que les renseignements pertinents sur les notes, qui sont anonymisés, ne sont pas visés par la définition de « renseignements personnels » de la *Loi sur l'accès à l'information et la protection de la vie privée* car ils n'ont pas trait à des particuliers qui peuvent être identifiés. L'exception fondée sur la vie privée ne peut donc être invoquée. L'arbitre a également rejeté l'affirmation de l'université selon laquelle la divulgation nuirait à ses intérêts économiques ou à sa situation concurrentielle. Comme les données sur les notes ne faisaient l'objet d'aucune exception, l'arbitre a ordonné à l'université de divulguer les renseignements demandés.

PO-3240
Ministère des Richesses naturelles

Une demande d'accès à l'information a été présentée en vue d'obtenir des renseignements concernant un plan de gestion adaptive qu'une entreprise a soumis à l'appui d'une demande de permis pour l'agrandissement d'une carrière. Le ministère a trouvé un courriel pertinent rédigé par un biologiste qui était à son emploi et qui portait sur les stratégies d'atténuation des risques pour l'environnement décrites dans le plan de gestion adaptive. Il a refusé l'accès à la totalité de ce courriel en invoquant l'exception s'appliquant à des renseignements qui révéleraient des conseils ou des recommandations prévue dans la *Loi sur l'accès à l'information et la protection de la vie privée*. L'auteur de la demande a interjeté appel de cette décision, en soutenant que cette exception ne s'appliquait pas, et que même si elle s'appliquait, la disposition de la *Loi* sur la nécessité manifeste de divulguer les renseignements dans l'intérêt public autoriserait la divulgation. L'arbitre a établi que les renseignements en cause se composent de conseils ou de recommandations qui sont soustraits à l'obligation de divulgation, mais que la nécessité manifeste de les divulguer dans l'intérêt public l'emporte sur l'objet de cette exception. L'arbitre a donc ordonné la divulgation du courriel.

La protection de la vie privée ne doit plus servir de prétexte

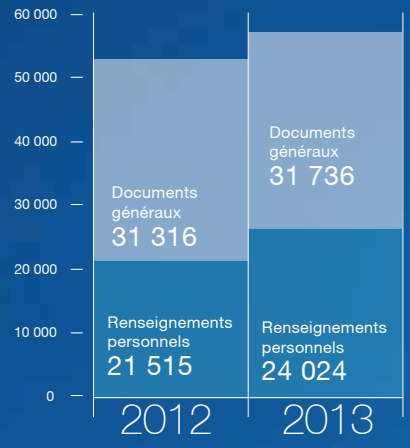
Il arrive que des institutions publiques invoquent la protection de la vie privée et les lois qui la régissent pour justifier leur décision de ne pas divulguer des documents généraux à la demande du public ou des médias. C'est là une malheureuse habitude, car ces lois visent à protéger la vie privée, pas à prévenir la communication de renseignements. La vie privée est un droit fondamental qui nous permet d'exercer les autres droits auxquels nous tenons, comme celui d'être libre. L'invoquer comme obstacle à la divulgation de données dénuées de renseignements personnels dévalue la vie privée et porte atteinte à la confiance du public.

D'après mon expérience, cette excuse reflète la volonté de faire preuve de prudence au lieu de chercher à comprendre les circonstances dans lesquelles il est possible de divulguer des documents ou, dans les pires cas, c'est un moyen pratique de détourner l'attention pour ne rien faire, et éviter ainsi de divulguer des renseignements que le public ou les médias pourraient juger durement.

Il faut toujours faire preuve de jugement avant de divulguer des renseignements, mais sans invoquer la protection de la vie privée comme prétexte. Les organisations gouvernementales doivent établir des méthodes de diffusion systématique de l'information par souci de transparence et de reddition de comptes. Ce serait avantageux pour tout le monde.

Quand je repense à toutes ses années d'activités du CIPVP, il m'apparaît évident que les Ontariennes et les Ontariens peuvent avoir l'assurance que notre bureau est devenu un organisme de premier ordre, reconnu pour son esprit novateur et son leadership dans les domaines de l'accès à l'information et de la protection de la vie privée.

STATISTIQUES



DEMANDES GLOBALES

↑12% Renseignements personnels

↑1% Documents généraux

↑6% Total des demandes

COUP D'OEIL SUR 2013

SOMMAIRE PROVINCIAL

RENSEIGNEMENTS PERSONNELS

DEMANDES
2013 6 825
2012 5 813
↑17%

APPELS OUVERTS
2013 186
2012 163
↑14%

APPELS FERMÉS
2013 143
2012 164
↓13%

COÛT MOYEN
2013 6,04 $
2012 4,98 $
↑21%

DOCUMENTS GÉNÉRAUX

DEMANDES
2013 13 996
2012 14 158
↓1%

APPELS OUVERTS
2013 421
2012 456
↓8%

APPELS FERMÉS
2013 454
2012 395
↑15%

COÛT MOYEN
2013 40,57 $
2012 41,99 $
↓3%

TOTAL DES DEMANDES
2013 20 821
2012 19 971
↑4%

PLAINTES CONCERNANT LA VIE PRIVÉE OUVERTES
2013 120
2012 155
↓23%

PLAINTES CONCERNANT LA VIE PRIVÉE FERMÉES
2013 118
2012 154
↑23%

SOMMAIRE MUNICIPAL

RENSEIGNEMENTS PERSONNELS

DEMANDES
2013 16 726
2012 15 702
↑7%

APPELS OUVERTS
2013 245
2012 265
↓8%

APPELS FERMÉS
2013 255
2012 230
↑11%

COÛT MOYEN
2013 8,24 $
2012 9,67 $
↓15%

DOCUMENTS GÉNÉRAUX

DEMANDES
2013 17 304
2012 17 158
↑1%

APPELS OUVERTS
2013 433
2012 392
↑10%

APPELS FERMÉS
2013 386
2012 369
↑5%

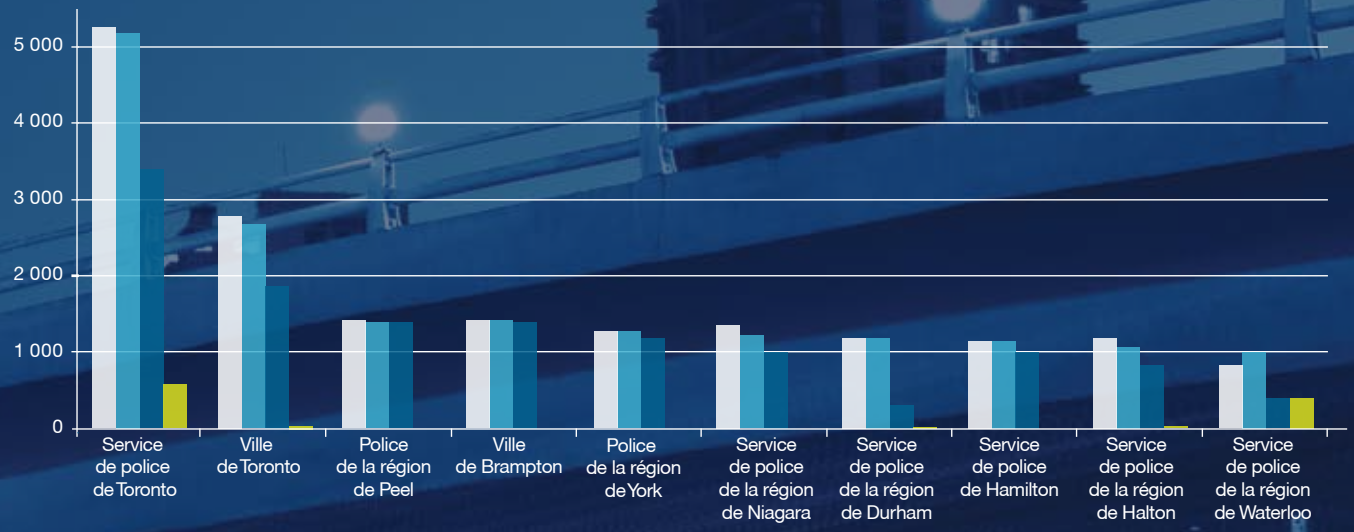
COÛT MOYEN
2013 28,09 $
2012 27,30 $
↑3%

TOTAL DES DEMANDES
2013 34 030
2012 32 860
↑4%

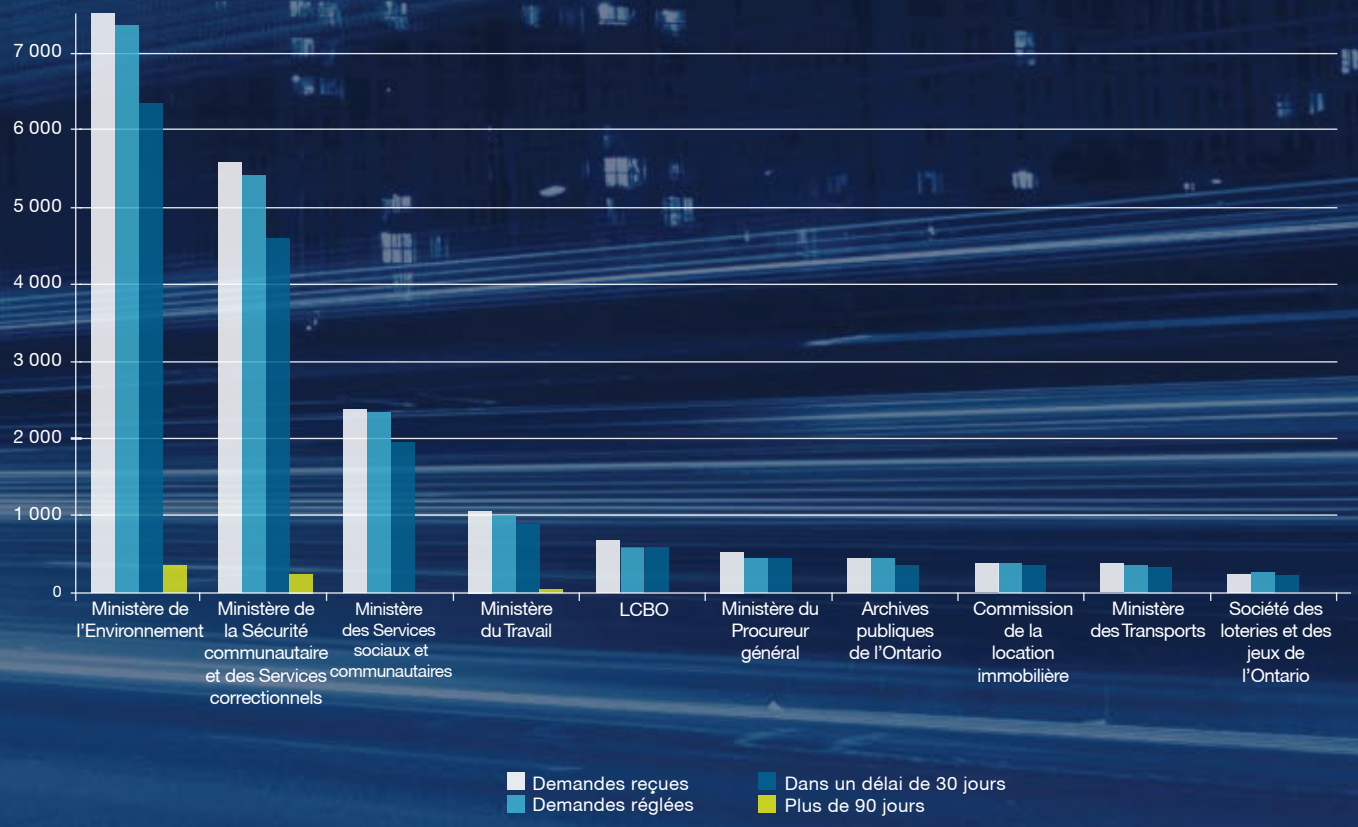
PLAINTES CONCERNANT LA VIE PRIVÉE OUVERTES
2013 136
2012 127
↑7%

PLAINTES CONCERNANT LA VIE PRIVÉE FERMÉES
2013 141
2012 121
↑17%

DIX PREMIÈRES INSTITUTIONS MUNICIPALES



DIX PREMIÈRES INSTITUTIONS PROVINCIALES



Selon le nombre de demandes réglées en 2013.

FAITS SAILLANTS 2013

55 760

Demandes d'accès à l'information présentées en Ontario

34 329

Demandes d'accès à l'information présentées aux organismes du gouvernement municipal

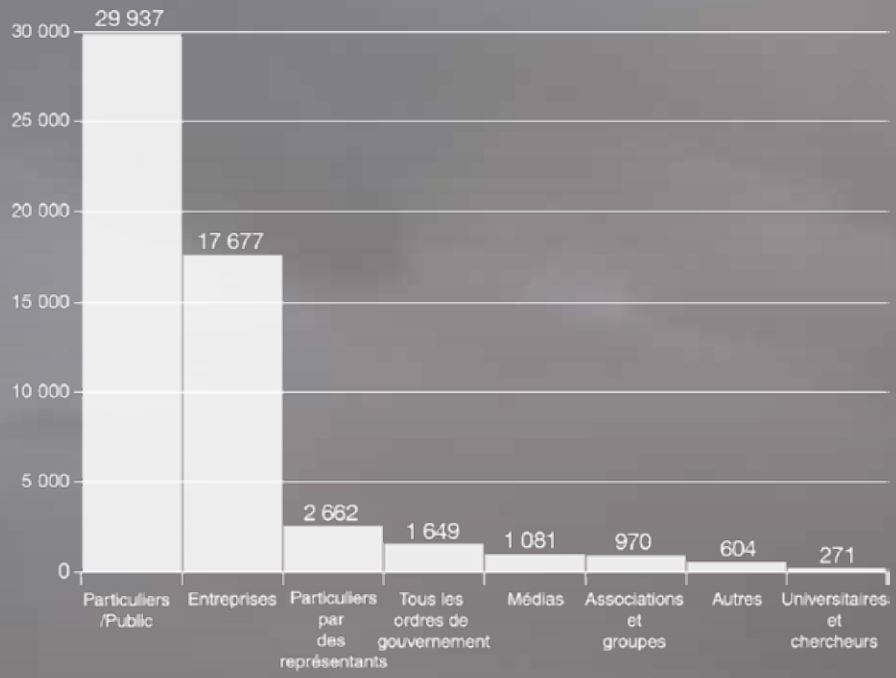
21 431

Demandes d'accès à l'information présentées aux organismes du gouvernement provincial

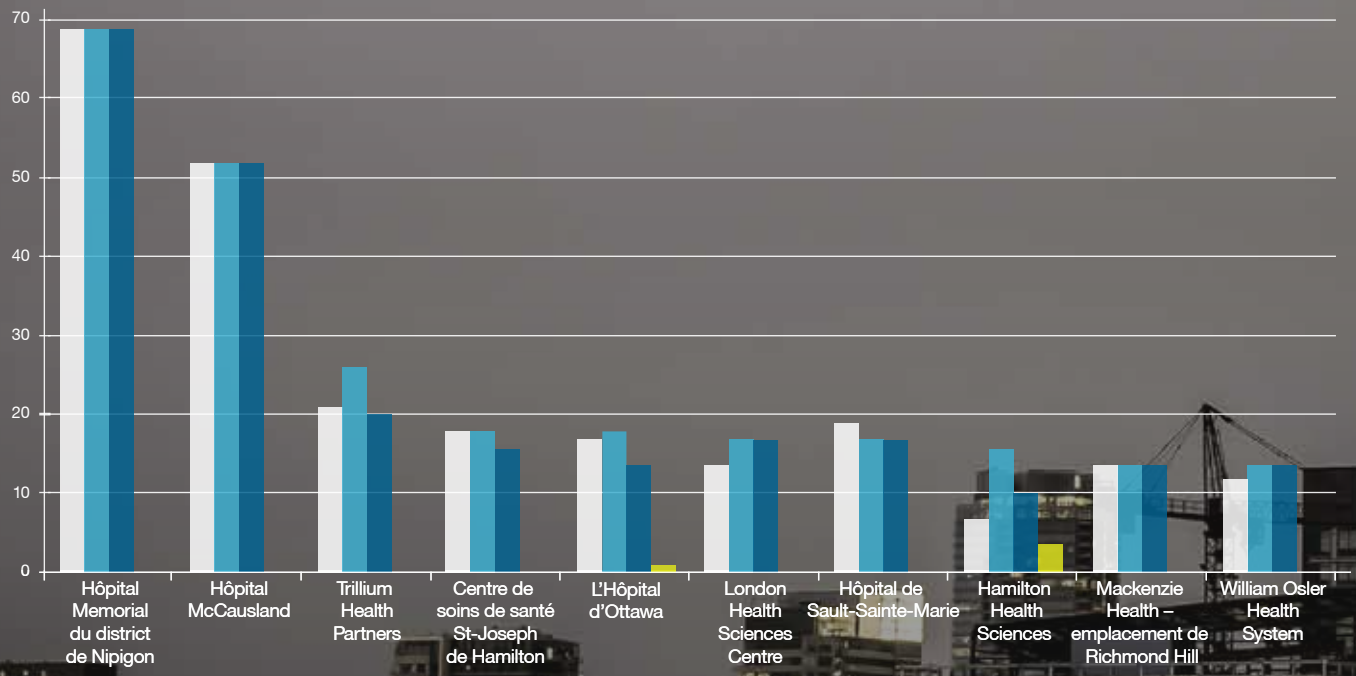
54 851

Demandes d'accès à l'information réglées en Ontario en 2013

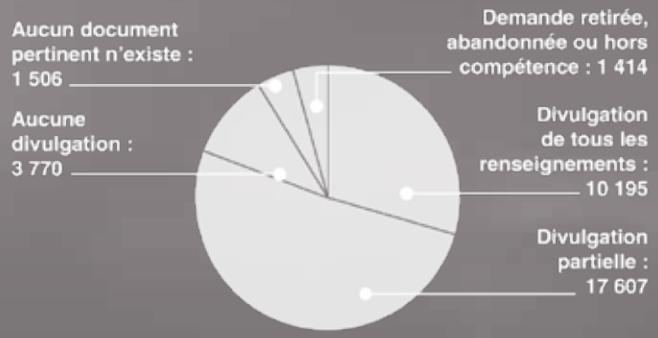
DEMANDES D'ACCÈS À L'INFORMATION RÉGLÉES, SELON LA SOURCE



DIX PREMIERS HÔPITAUX

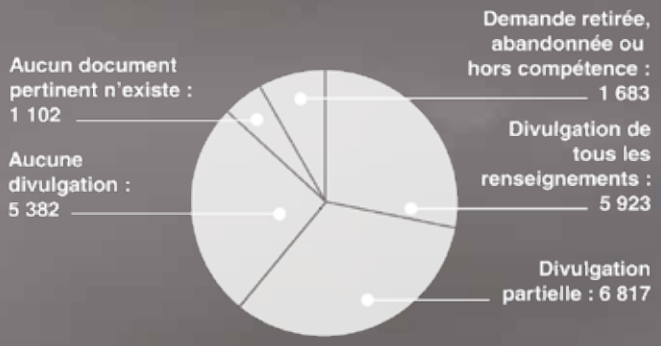


ISSUE DES DEMANDES : PALIER MUNICIPAL



* Les totaux ne concordent pas avec le nombre total de demandes réglées parce que les calculs de ce tableau tiennent également compte des demandes à l'égard desquelles aucune décision n'a été rendue car elles ne relevaient pas de l'institution.

ISSUE DES DEMANDES : PALIER PROVINCIAL



* Les totaux ne concordent pas avec le nombre total de demandes réglées parce que les calculs de ce tableau tiennent également compte des demandes à l'égard desquelles aucune décision n'a été rendue car elles ne relevaient pas de l'institution.

8,24 $ Renseignements personnels

28,09 $ Documents généraux

Coût moyen des demandes au palier municipal

6,04 $ Renseignements personnels

40,57 $ Documents généraux

Coût moyen des demandes au palier provincial

16 118

Demandes où il y a eu divulgation de tous les renseignements

86,5%

Taux de respect du **délai de réponse de 30 jours** des ministères, organismes et autres institutions

77,2%

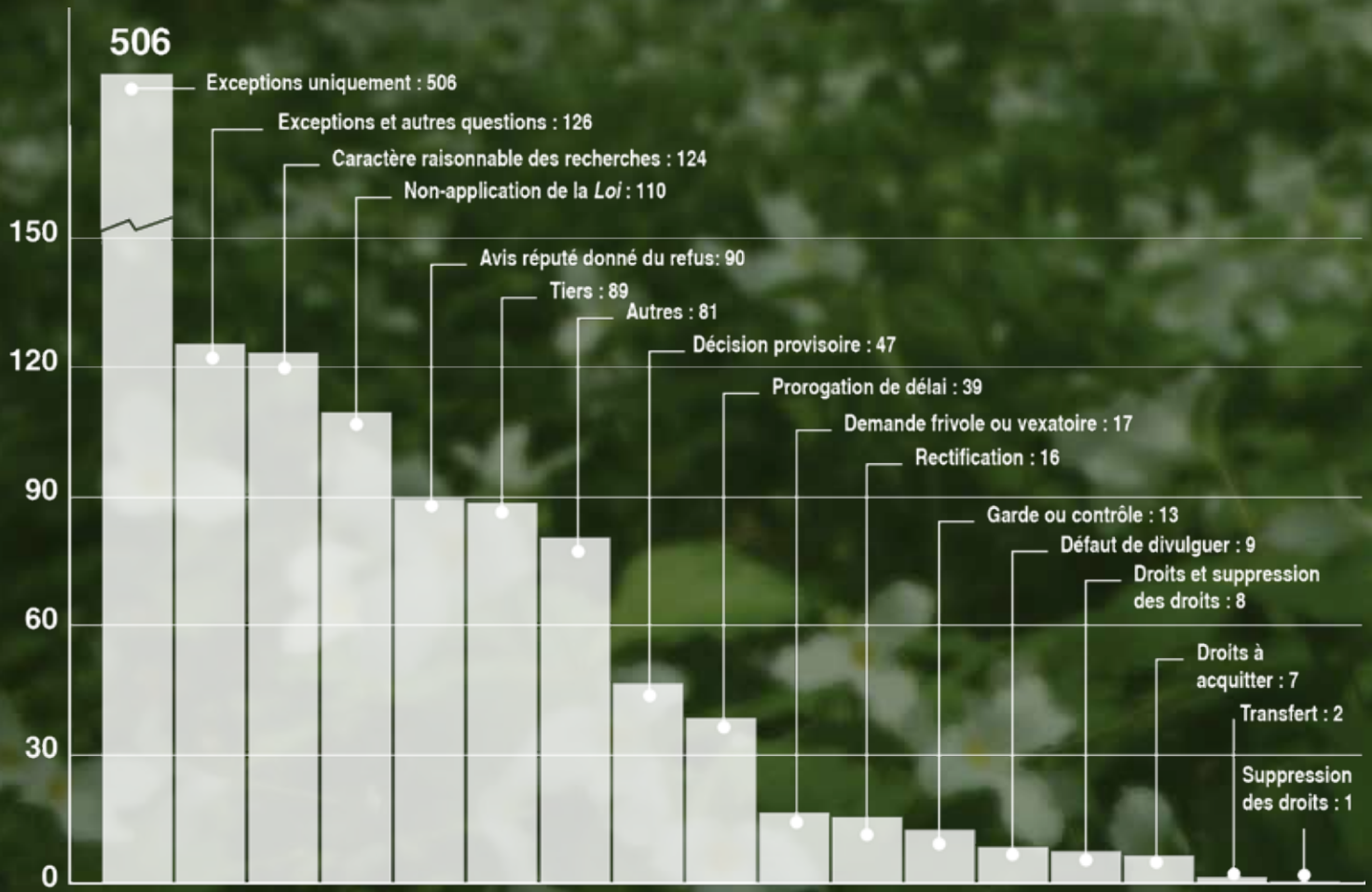
Taux de respect du **délai de réponse de 30 jours** des organismes du gouvernement municipal

1 285
Appels ouverts par le CIPVP en 2013

53,3%
Appels réglées par voie de médiation

11,7%
Appels retirés

QUESTIONS EN LITIGE DANS LES APPELS – DOSSIERS OUVERTS



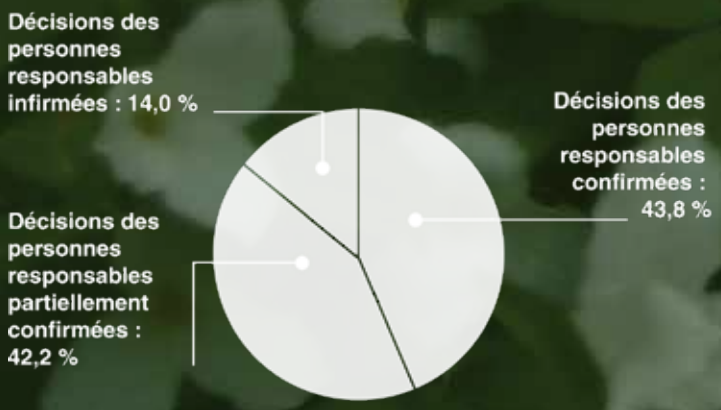
322
Appels réglés par voie d'ordonnance

481
Appels réglés par voie de médiation

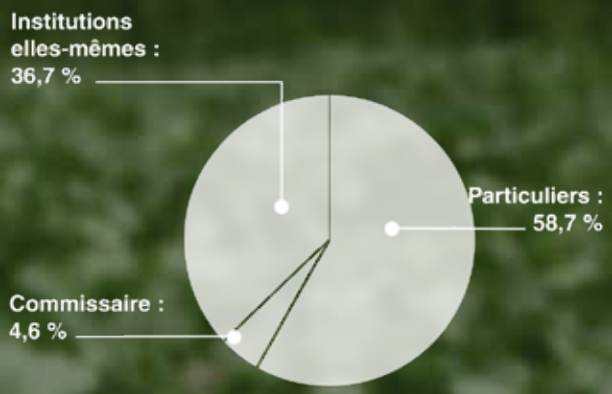
1 002
Appelants étaient des particuliers

173
Appelants étaient des entreprises

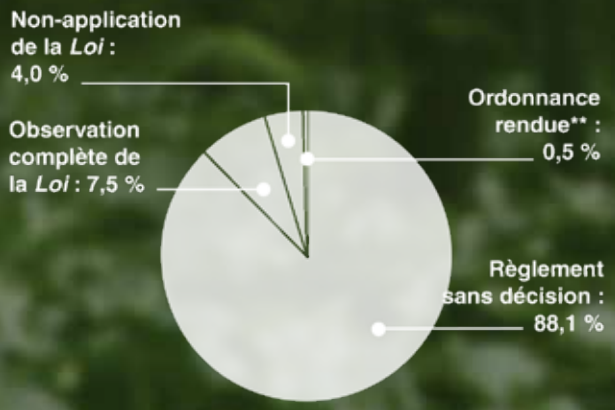
NOMBRE DE DOSSIERS D'APPEL FERMÉS PAR VOIE D'ORDONNANCE



SOURCE DES PLAINTES



ISSUE DES PLAINTES CONCERNANT LA PROTECTION DE LA VIE PRIVÉE



* Le total ne correspond pas au nombre de plaintes, car certaines plaintes portent sur plusieurs enjeux. Les plaintes abandonnées, retirées et exclues ne sont pas incluses.

** Dossier de plainte PC12-47 fermé par l'ordonnance PO-3171

256
Plaintes concernant la protection de la vie privée ouvertes en 2013

259
Plaintes concernant la protection de la vie privée fermées en 2013

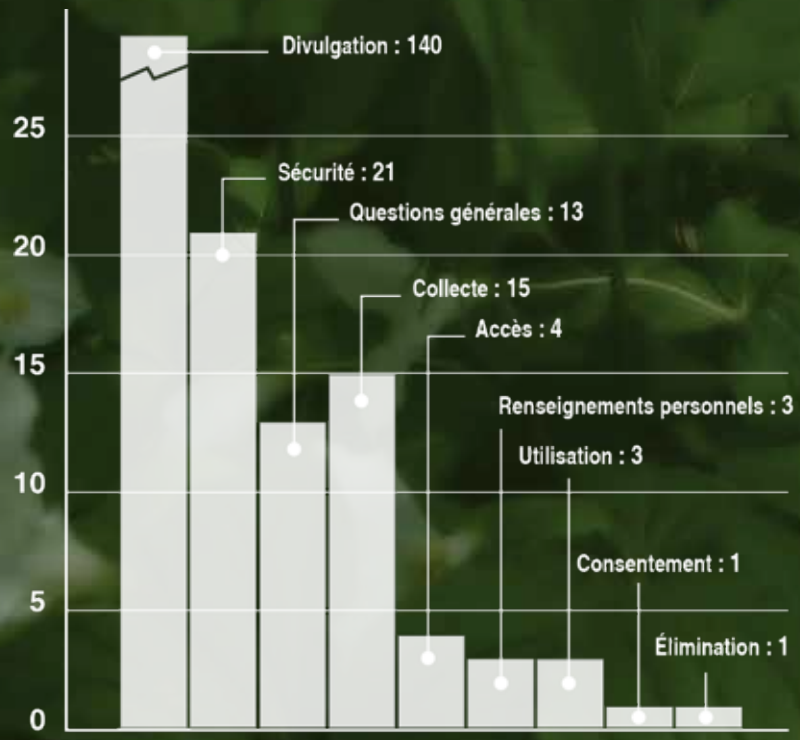
66%
Plaintes réglées

14,3%
Plaintes retirées

152
Plaintes déposées par des particuliers

95
Plaintes déposées par les institutions elles-mêmes

ENJEUX* DES PLAINTES CONCERNANT LA PROTECTION DE LA VIE PRIVÉE



* Le total ne correspond pas au nombre de plaintes, car certaines plaintes portent sur plusieurs enjeux. Les plaintes abandonnées, retirées et exclues ne sont pas incluses.

Révisions judiciaires

***Ministry of Community and Social Services v. Information and Privacy Commissioner et al.*, 2014 ONSC 239 – Révision judiciaire de l'ordonnance PO-2917**

Dans une importante décision rendue au début de l'année, la Cour divisionnaire de l'Ontario a rejeté une demande de révision judiciaire de la part du ministère des Services sociaux et communautaires contestant l'ordonnance du CIPVP l'enjoignant de divulguer des renseignements personnels concernant l'auteur d'une demande, y compris le nom complet des employés du Bureau des obligations familiales (BOF) qui étaient assignés à son dossier.

Lors de l'enquête du CIPVP, le ministère et le Syndicat des employées et employés de la fonction publique de l'Ontario (SEFPO) ont affirmé que les noms complets des employés du BOF figurant dans les documents contenus dans le dossier de l'auteur de la demande étaient visés par l'exception fondée sur les relations de travail de la disposition 3 du paragraphe 65 (6) de la *Loi sur l'accès à l'information et la protection de la vie privée*. Ces noms étaient aussi visés par les exceptions de l'alinéa 14 (1) e) et de l'article 20 concernant les menaces à la santé et à la sécurité. Comme des employés du BOF avaient fait l'objet de menaces de la part de débiteurs alimentaires au fil des ans, le SEFPO avait déposé un grief soutenant que la divulgation des noms au complet menacerait la santé et la sécurité des employés et de leur famille en révélant leur identité à des débiteurs mécontents du BOF qui risqueraient de mettre leurs menaces à exécution. Ce grief a fait l'objet d'un règlement autorisant les membres du personnel du BOF (sans les y obliger) à ne pas divulguer leur nom complet au public dans leurs communications écrites et téléphoniques et à utiliser plutôt leur prénom et un numéro d'identification. Ce règlement a été intégré par la suite dans une « ordonnance de consentement » rendue par la Commission de règlement des griefs (CRG).

Le ministère et le SEFPO ont soutenu que l'exception s'appliquait car en raison de l'ordonnance de consentement de la CRG, les noms complets concernent des communications « en ce qui a trait aux relations de travail ou à des questions en matière d'emploi » au sens de la disposition 3 du paragraphe 65 (6). Même si cette exception ne s'appliquait pas, la divulgation des noms menacerait la santé et la sécurité des employés au sens de l'alinéa 14 (1) e) et de l'article 20. En outre, la divulgation en vertu de la *LAIPVP* irait à l'encontre de l'ordonnance de consentement.

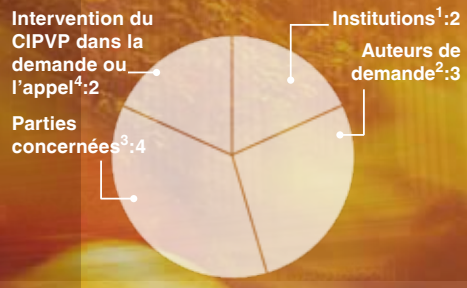
Le CIPVP a rejeté tous ces arguments. L'arbitre a établi que les documents contenant les noms des employés n'avaient pas trait aux relations de travail, mais qu'ils étaient des documents opérationnels courants sur les activités de base du BOF. Le CIPVP a aussi rejeté l'application de l'alinéa 14 (1) e) et de l'article 20 car (1) rien ne prouvait que l'auteur de la demande représentait une menace pour les employés du BOF; (2) rien ne prouvait que les employés en question avaient déjà fait l'objet de menaces; (3) les renseignements contenus dans les documents n'avaient rien d'incendiaire.

Dans son rejet de la demande de révision judiciaire du ministère, la Cour divisionnaire a pris plusieurs décisions importantes qui auront de vastes répercussions sur l'application future de la *LAIPVP*.

Premièrement, la cour, appliquant ainsi des arrêts récents de la Cour suprême du Canada, a refusé d'aller dans

STATISTIQUES SUR LES RÉVISIONS JUDICIAIRES 2013

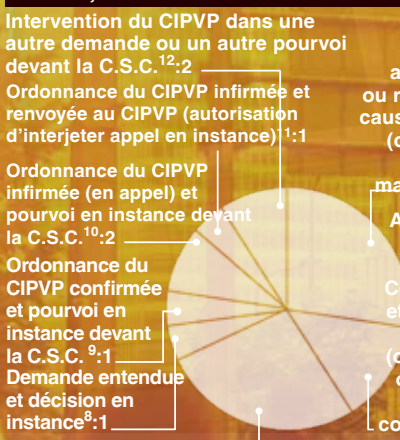
Nouvelles demandes de révision judiciaire déposées



1. Ordonnance PO-3164, ordonnance PO-3171
2. Ordonnance PO-3131, ordonnance PO-3172, ordonnance PO-3222
3. Ordonnance PO-3142, ordonnance PO-3174, ordonnance PO-3176, ordonnance MO-2895
4. *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 R.C.S. 62; *Dr. Rudinskas v. CPSO* (CV-12-466078)

Révisions judiciaires en instance en date du 31 décembre 2013

Révisions judiciaires closes ou entendues



5. Ordonnances PO-3005, ordonnance PO-3034, ordonnance PO-2491 (3 révisions judiciaires), ordonnance MO-2566
6. Ordonnance MO-2370, appels MA09-391-1 et MA09-391-2
7. Ordonnance MO-2659, ordonnance MO-2738, ordonnances PO-3011 et PO-3072-R, ordonnance PO 3131, ordonnance MO-2688
8. Ordonnance PO-2917
9. Ordonnance PO-2811
10. Ordonnances PO-2872 et PO-2899-R
11. Ordonnance PO-3171
12. *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 R.C.S. 62, *Dr. Rudinskas v. CPSO* (CV-12-466078)

le sens de jugements antérieurs et a estimé que la révision des décisions du CIPVP pour ce qui est de l'application de l'exception énoncée au paragraphe 65 (6) doit être fondée sur la norme de la décision raisonnable et non sur la norme du bien-fondé.

Deuxièmement, la cour a rejeté l'interprétation libérale que le ministère a faite du paragraphe 65 (6), qui pourrait exclure des documents opérationnels courants de la *LAIPVP* et « porter atteinte au principe d'ouverture et de responsabilité à l'égard du public que la *Loi* est censée favoriser ».

Troisièmement, en rejetant les arguments du ministère relatifs à la menace à la sécurité, la cour a fait plusieurs observations sur l'application de la *Loi* que le CIPVP préconisait depuis longtemps :

1. Il n'est pas pertinent de tenir compte de la motivation de l'auteur de la demande ou du fait qu'il ait démontré ou non qu'il a « besoin » des renseignements.
2. Le droit d'un particulier d'accéder aux renseignements personnels qui le concernent en vertu de la partie III de la *LAIPVP* doit être évalué différemment du droit d'accès général de la partie II : « En vertu de l'alinéa 47 (1) b), il y a présomption que l'auteur de la demande a le droit d'accéder aux renseignements en question ».
3. La divulgation de documents en vertu de la partie II de la *Loi* représente une « divulgation publique »; la divulgation de renseignements personnels en vertu de la partie III se fait uniquement à l'auteur de la demande.
4. La preuve d'un risque de préjudice général découlant de la divulgation au public ne suffit pas nécessairement pour prouver que la divulgation des renseignements personnels concernant un auteur de demande causerait un préjudice.
5. L'exercice du pouvoir discrétionnaire dont jouit le ministre de divulguer ou non un document assujetti à une exception discrétionnaire [en l'occurrence, celles de l'alinéa 14 (1) e) et de l'article 20] ne peut être entravé par une entente telle que l'ordonnance de consentement de la CRG : « Le ministre ne peut consentir à un arrangement qui aurait pour effet de le soustraire à ses obligations en vertu de la *Loi* ».

Enfin, la cour a confirmé le principe selon lequel elle ne cherchera pas activement à relever les incompatibilités d'application des décisions de deux tribunaux administratifs. Elle a observé que l'ordonnance prévoyant la divulgation ne portait pas atteinte à la capacité des employés du BOF de ne pas se servir de leur nom au complet dans leurs communications avec le public. L'ordonnance de la CRG n'allait donc pas à l'encontre de la décision du CIPVP ni le l'emportait sur elle.

La *Loi sur la protection des renseignements personnels sur la santé* en 2013

Comme toujours, cette année a été riche en défis et en progrès relativement à la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*). Le gouvernement a déposé le projet de loi 78, *Loi de 2013 sur la protection des renseignements personnels sur la santé figurant dans un dossier de santé électronique*, mais il s'est produit d'autres infractions relatives aux renseignements personnels sur la santé, ce qui témoigne de la pertinence de notre travail relativement à la pratique « prenez vos appareils personnels » (PAP), qui gagne en popularité.

Projet de loi 78, Loi de 2013 sur la protection des renseignements personnels sur la santé figurant dans un dossier de santé électronique

En mai, le gouvernement de l'Ontario a déposé, comme je le proposais depuis un certain temps, des modifications à la *LPRPS* portant sur les aspects des dossiers de santé électroniques touchant la protection de la vie privée et la sécurité. La *LPRPS* est un texte de loi modèle en matière de protection des renseignements personnels sur la santé dans l'ensemble du pays depuis son entrée en vigueur en 2004, mais elle ne régit pas adéquatement les droits des particuliers et les obligations des fournisseurs de soins de santé en ce qui a trait aux dossiers de santé électronique. Les modifications proposées à la *LPRPS* préciseront le droit des patients de limiter la collecte, l'utilisation et la divulgation des renseignements personnels sur la santé les concernant dans leur dossier de santé électronique par l'application

Ces modifications proposées à la *LPRPS* faciliteront l'implantation des dossiers de santé électroniques, ce qui permettra de **moderniser la prestation des soins de santé** dans toute la province.

de directives en matière de consentement. Les modifications proposées préciseront aussi le droit des patients d'accéder à leur dossier de santé électronique, d'en demander la rectification et de savoir qui y a eu accès. Elles prévoient aussi que seuls les fournisseurs de soins de santé autorisés et leurs représentants peuvent accéder aux renseignements personnels sur la santé figurant dans le dossier de santé électronique du patient, et elles limitent les fins auxquelles il sera possible d'accéder à ces renseignements. Il faudra également consigner et surveiller l'accès aux dossiers de santé électronique afin d'éviter la collecte, l'utilisation et la divulgation non autorisées de renseignements personnels sur la santé.

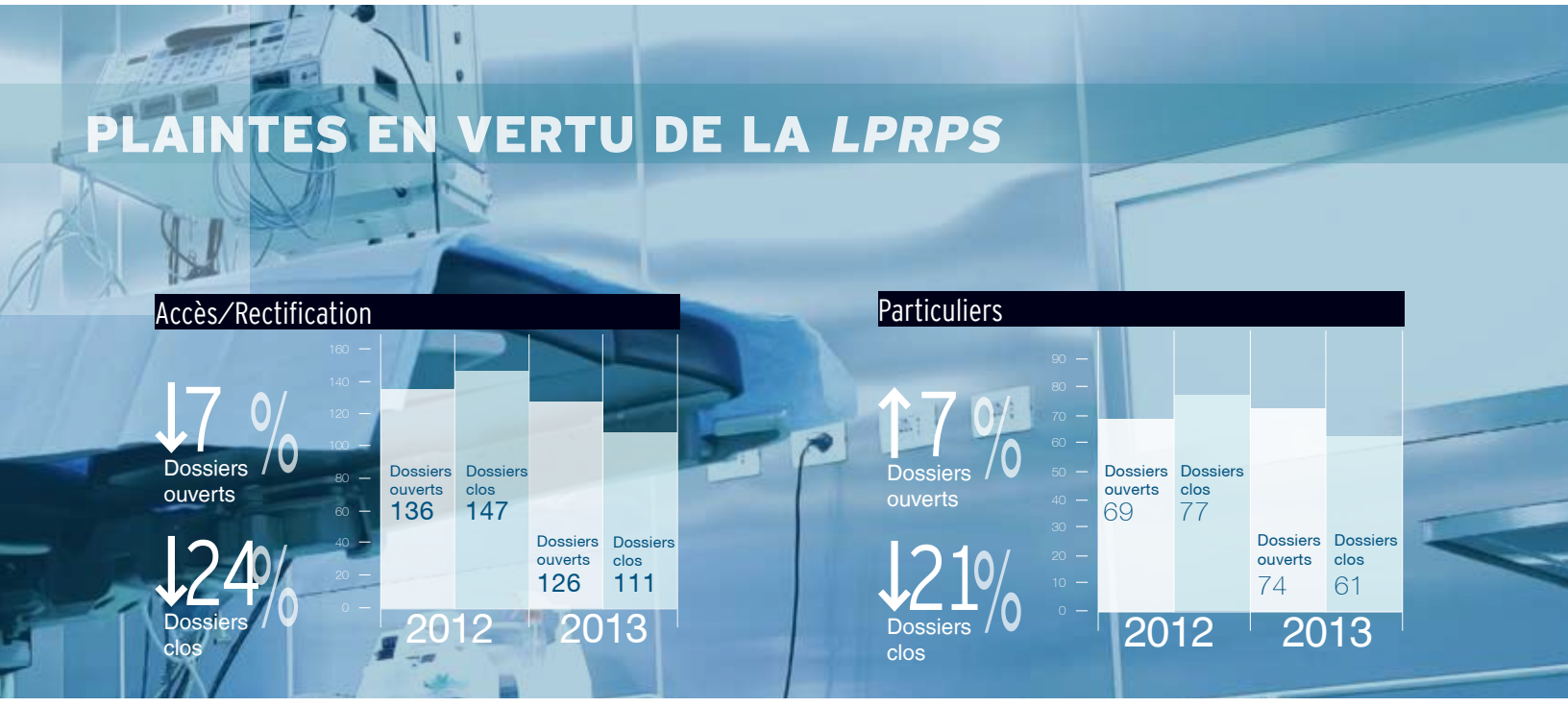
Ces modifications proposées à la *LPRPS* faciliteront l'implantation des dossiers de santé électroniques, ce qui permettra de moderniser la prestation des soins de santé dans toute la province. Ces dossiers pourraient améliorer considérablement le diagnostic et le traitement, rehausser la sécurité des patients et faciliter la coordination et l'intégration des services, de sorte que le système de santé sera plus efficient et efficace.

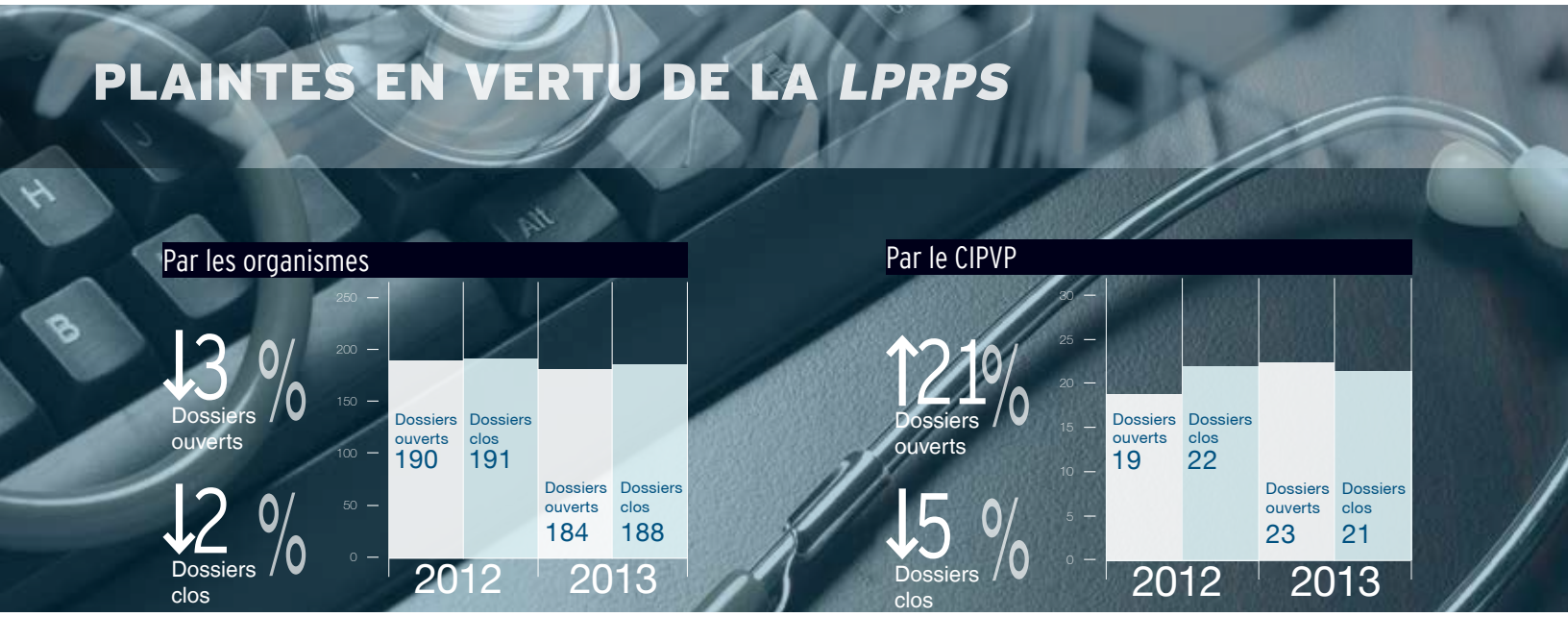
Prenez vos appareils personnels

La perte et le vol d'appareils informatiques mobiles et de dispositifs de stockage (ordinateurs portables, tablettes, téléphones intelligents, clés USB et cartes mémoire) constituent les principales causes d'atteinte à la sécurité et à la confidentialité. Ils comptent aussi parmi les plus prévisibles et les plus faciles à prévenir.

Comme toujours, j'espérais qu'il ne se produise aucune atteinte à la vie privée en 2013, mais mon vœu n'a pas été exaucé. Il y a eu plusieurs incidents faisant intervenir des renseignements personnels sur la santé, presque tous touchant des appareils mobiles. Par exemple, le vol d'une carte mémoire contenant des renseignements personnels sur la santé non chiffrés concernant 18 000 patients du service de santé publique de la région de Peel illustre à quel point les renseignements personnels sont vulnérables dans un environnement où l'on utilise de plus en plus des appareils informatiques mobiles.

Il ressort des enquêtes de mon bureau sur ces incidents que les dépositaires de renseignements sur la santé se doivent de protéger tous leurs appareils mobiles par le chiffrement et des mots de passe, mais dans la réalité, des moyens techniques simples permettent rarement de prévenir les fuites de données dans un environnement complexe où un grand nombre de personnes ont accès aux données. La gestion efficace des données tout au long de leur cycle de vie requiert des pratiques d'atténuation des risques fondées sur une démarche structurée s'appuyant sur des normes, et notamment sur un ensemble d'objectifs de gouvernance de base en matière de technologie de l'information axé sur la prévention de la perte de données,





comme nous le préconisons dans le document que nous avons publié en décembre 2012 en collaboration avec le Centre des sciences de la santé Sunnybrook et CryptoMill Technologies intitulé *Encryption by Default and Circles of Trust.*

La nécessité d'adopter une démarche globale et systématique pour assurer la sécurité des appareils mobiles est l'une des conclusions majeures du document que j'ai publié conjointement avec Telus concernant la pratique de plus en plus populaire appelée *prenez vos appareils personnels* (PAP), ou parfois *apportez votre équipement personnel de communication* (AVEC). Cette pratique consiste pour les organisations à autoriser leurs employés à se servir de leurs appareils personnels à des fins professionnelles. Les entreprises canadiennes sont les chefs de file mondiaux de cette pratique et de l'implantation d'applications de type grand public en milieu de travail. Cependant, plus de la moitié des organisations canadiennes perdent chaque année des données délicates contenues dans les appareils dont leurs employés se servent.

Ce document conjoint intitulé *BYOD: (Bring Your Own Device) Is Your Organization Ready?* vise à fournir des conseils pratiques sur la façon de déterminer et d'atténuer les différents risques pour la vie privée que comporte un programme PAP, selon une démarche à cinq étapes, allant de la définition des exigences jusqu'au soutien apporté aux utilisateurs, comme le précise le document. Ces étapes s'appuient sur les principes fondamentaux de la *PIVP* : proactivité, méthodes intégrées, résultats à somme positive et précautions efficaces de bout en bout sans perte de fonctionnalité.

Ces conseils tombent à point nommé, car de nos jours, de plus en plus d'organismes de santé cherchent à permettre à leurs employés, et aux médecins qui ne font pas partie de leur personnel, de relier leurs appareils personnels à leurs réseaux internes. Cependant, l'utilisation d'appareils mobiles personnels dans un contexte professionnel soulève de nombreuses questions en matière de protection de la vie privée et de sécurité; il faut y répondre pour éviter les atteintes à la vie privée et que l'approche PAP, au lieu de constituer un avantage, ne représente une perte pour les organisations.

L'approche PAP est devenue une tendance inexorable qui propose de nouveaux avantages assortis de risques, notamment en matière de sécurité des données, aux organisations de toutes tailles. Heureusement, je crois qu'il est désormais possible de gérer ces avantages et ces risques de façon optimale en adoptant une démarche globale fondée sur la *protection intégrée de la vie privée.*

Afin de mieux orienter les organisations de soins de santé et d'autres institutions concernant l'identification et l'atténuation des risques généraux pour la vie privée que présente l'utilisation d'appareils mobiles à des fins professionnelles, j'ai publié une brochure intitulée *La protection de la vie privée et les appareils mobiles*. Elle propose des conseils pratiques pour assurer la protection des renseignements personnels sur la santé et les renseignements identificatoires lors de l'utilisation de tels appareils.

État financier

	Prévisions 2013-2014 $	Prévisions 2013-2013 $	Chiffres réels 2012-2013 $
TRAITEMENTS ET SALAIRES	10 211 500	10 132 000	9 663 655
AVANTAGES SOCIAUX	2 348 900	2 330 900	1 847 769
TRANSPORTS ET COMMUNICATIONS	337 500	337 500	231 119
SERVICES	1 960 300	1 960 300	1 785 107
FOURNITURES ET MATÉRIEL	336 000	336 000	319 067
TOTAL	15 194 200	15 096 700	13 846 717

Remarque : L'exercice financier du CIPVP s'échelonne du 1er avril au 31 mars.
L'état financier du CIPVP est vérifié chaque année par le Bureau du vérificateur général de l'Ontario.

DROITS D'APPEL PERÇUS EN 2013

(année civile)

DOCUMENTS GÉNÉRAUX	RENSEIGNEMENTS PERSONNELS	TOTAL
15 039 $	2 940 $	17 979 $

Voir autres renseignements financiers, y compris les traitements du CIPVP divulgués en vertu de la Loi de 1996 sur la divulgation des traitements dans le secteur public à www.ipc.on.ca.

2013

ACCÈS À L'INFORMATION ET VIE PRIVÉE

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

2, rue Bloor Est, Bureau 1400
Toronto (Ontario) M4W 1A8
Canada

www.ipc.on.ca