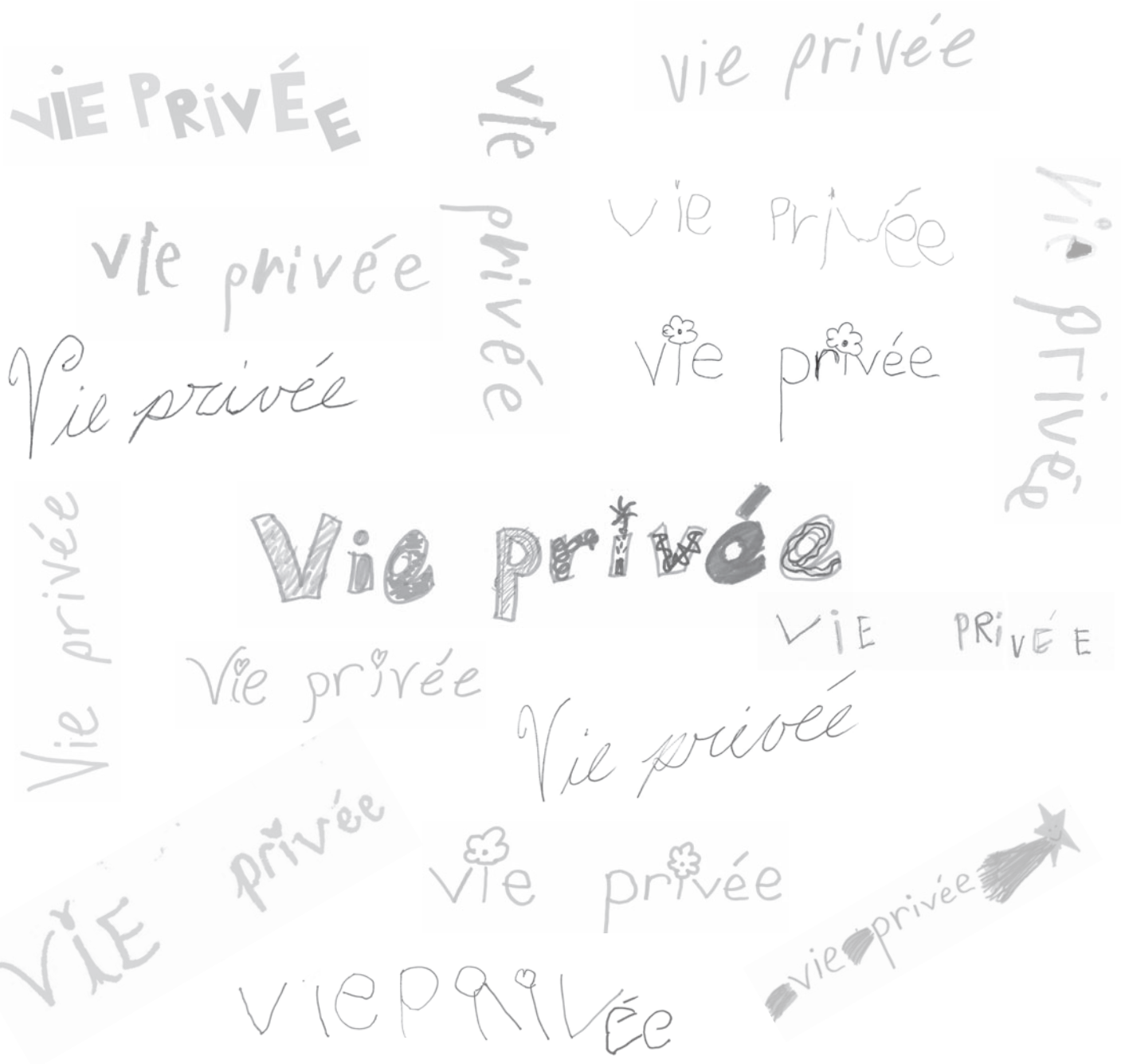
Commissariat
à la protection de
la vie privée du Canada

Rapport annuel au Parlement 2011

Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques*



Les dessins sur cette page ainsi qu'à l'intérieur du présent rapport sont
l'œuvre d'enfants d'employés du Commissariat à la protection de la vie privée du Canada.

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario) K1A 1H3

613-947-1698, 1-800-282-1376
Télécopieur : 613-947-6850
ATS : 613-992-9190

Image de couverture : Alin Popescu / Shutterstock.com

N° de catalogue : IP51-1/2011
1910-0051

Cette publication se trouve également au **www.priv.gc.ca**

Suivez-nous sur Twitter: @privacyprivee

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Juin 2012

L'honorable Noël A. Kinsella, sénateur
Président
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2011.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

original signé par

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Juin 2012

L'honorable Andrew Scheer, député
Président
Chambre des communes
Ottawa (Ontario) K1A 0A6

Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2011.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

original signé par

Jennifer Stoddart

Table des matières

Table des matières

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) établit des règles de base à l'égard de la gestion des renseignements personnels dans le secteur privé.

Elle vise l'atteinte d'un équilibre entre le droit à la protection des renseignements personnels et le besoin qu'ont les organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins commerciales légitimes.

La LPRPDE s'applique aux organisations qui se livrent à des activités commerciales à l'échelle du pays, sauf celles qui sont régies par des provinces disposant de leur propre loi sur la protection des renseignements personnels applicable au secteur privé. Le Québec, l'Alberta et la Colombie-Britannique disposent d'une telle loi. Toutefois, même dans ces provinces, le LPRPDE s'applique au secteur privé assujetti à la réglementation fédérale et aux renseignements personnels dans le cadre de transactions interprovinciales et internationales.

La LPRPDE protège également les renseignements des employés travaillant dans les secteurs sous réglementation fédérale.

Message de la commissaire

Les adolescents d'aujourd'hui vivent dans un monde bien différent de celui dans lequel j'ai grandi.

De nos jours, les jeunes disposent d'une capacité de communication sans précédent. Les membres de la première vague de ce que certains appellent la « génération Facebook » ont adopté le monde en ligne pour rester en contact avec leurs amis — ils y échangent de nouvelles vidéos sur YouTube ou les dernières chansons à succès, y planifient leurs sorties et y parlent de ce qui se passe dans leurs vies.

Je faisais la plupart de ces choses avec mes amis d'école, mais en personne ou au téléphone — que je partageais avec les autres membres de ma famille.

La principale différence entre ce que je faisais alors et ce qui se fait maintenant, c'est qu'il n'existe aucune trace des conversations que j'avais à l'époque. C'est également vrai pour mes propres enfants, qui ne sont encore que dans la vingtaine.

Toutefois, ce n'est manifestement plus le cas pour les adolescents d'aujourd'hui.

Toute cette communication en ligne laisse des traces permanentes qui pourraient comporter des risques pour leur vie privée et leur réputation, pas seulement maintenant, mais peut être même plus à l'avenir.

C'est normal que les adolescents fassent des erreurs en grandissant.

Il est donc très préoccupant de penser que, dans les décennies à venir, il y aura encore des traces électroniques de nombreuses erreurs commises par les jeunes d'aujourd'hui.

En effet, de très nombreux dangers menacent la vie privée et les renseignements personnels des enfants et des jeunes. C'est une des raisons pour lesquelles une bonne part du présent rapport est axée sur eux.

Bien que les jeunes soient souvent les premiers à adopter les nouveaux types de communication numérique, ils ne peuvent généralement pas imaginer les intrusions dans la vie privée qui peuvent découler de ces nouvelles technologies.

Une autre bonne raison justifie le fait de consacrer un chapitre aux efforts que nous déployons pour protéger les renseignements personnels des enfants et des jeunes : ce travail constitue un excellent exemple du leadership dont le Commissariat fait preuve concernant un enjeu prioritaire en matière de protection de la vie privée.

Lorsque j'ai reçu un nouveau mandat de trois ans en tant que commissaire à la protection de la vie privée du Canada, je me suis engagée auprès des députés et des sénateurs à faire preuve de ce leadership. J'ai promis d'en faire l'une de mes trois priorités, les deux autres étant l'appui à la prise de décisions éclairées en matière de protection de la vie privée et l'amélioration des services offerts aux Canadiennes et Canadiens.

Un an après le renouvellement de mon mandat, le moment semble bien choisi pour examiner les progrès relatifs à ces engagements.

ENJEUX IMPORTANTS LIÉS À LA PROTECTION DE LA VIE PRIVÉE

Parlons d'abord du leadership sur les enjeux prioritaires liés à la protection de la vie privée. Comme nous le mentionnons plus loin dans le présent rapport, le Commissariat a été particulièrement actif en 2011 dans le dossier de la protection de la vie privée des enfants et des jeunes. Il a créé une foule de documents de sensibilisation, financé des recherches novatrices et examiné les effets de la surveillance sur les jeunes.

Nous avons aussi terminé une enquête approfondie sur une plainte soulevant des préoccupations quant à la protection de la vie privée sur un site Web de réseautage social conçu particulièrement pour les jeunes. La première enquête du CPVP sur un site de réseautage social destiné aux jeunes était très

« (L)e Commissariat a été particulièrement actif en 2011 dans le dossier de la protection de la vie privée des enfants et des jeunes. Il a créé une foule de documents de sensibilisation, financé des recherches novatrices et examiné les effets de la surveillance sur les jeunes. »

complexe et a entraîné la production d'un rapport de conclusions détaillé de quelque 100 pages comprenant 24 recommandations.

Pourtant, de nombreux problèmes auraient pu être évités si les responsables du site avaient tenu compte de la protection de la vie privée au moment de la conception et du lancement. Le Commissariat considère donc que cette enquête devrait servir de leçon à tous ceux qui traitent les renseignements personnels des jeunes.

Nous avons aussi fait preuve de leadership en ce qui concerne la prolifération des publicités comportementales en ligne. Le terme lui même est peu connu, mais presque tous les internautes canadiens ont vu de telles publicités.

Officiellement, la publicité comportementale consiste à faire le suivi des activités en ligne d'un consommateur dans le but de fournir des publicités adaptées à ses intérêts présumés. En pratique, cela signifie que les réseaux de publicité sur Internet vous suivent à la trace et observent ce que vous faites afin de vous offrir des publicités ciblées.

À la fin de 2011, nous avons publié un document d'orientation sur la façon dont les intervenants qui participent au processus de publicité comportementale en ligne — ou qui en profitent — peuvent s'assurer que leurs pratiques sont justes, transparentes et conformes à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

Nous avons particulièrement mentionné que les organisations faisant de la publicité comportementale en ligne devraient éviter de surveiller les activités des enfants ou les sites qui leur sont destinés, car il serait difficile d'obtenir leur consentement éclairé.

Le projet de loi sur l'accès légal qui avait été annoncé par le gouvernement (et qui a été présenté sous le nom de projet de loi C-30 au début de 2012) est un autre domaine prioritaire pour la protection de la vie privée dans le cadre duquel le Commissariat a exercé son leadership cette année. Ce projet de loi aura des répercussions évidentes sur l'industrie des télécommunications. Après avoir échangé des observations avec les commissaires provinciaux et territoriaux à la protection de la vie privée, j'ai envoyé, en octobre, une lettre ouverte au ministre de la Sécurité publique Vic Toews pour lui faire part de mes préoccupations selon lesquelles le régime de surveillance élargi proposé dans le projet de loi aura de graves conséquences sur le droit à la vie privée.

DÉCISIONS ÉCLAIRÉES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Le deuxième engagement que j'ai pris pour la suite de mon mandat est d'aider les Canadiennes et Canadiens, les organisations et les institutions à prendre des décisions éclairées en matière de protection de la vie privée.

En mai, le Commissariat a jeté des bases solides pour y arriver en publiant un rapport final sur de vastes consultations publiques qui ont eu lieu l'année précédente sur le suivi, le profilage et le ciblage en

ligne et l'infonuagique. Les leçons apprises au cours de ces consultations ont eu plusieurs effets : des fiches conseil sur les fichiers témoins et l'infonuagique; une série de conférences attirant l'attention sur des enjeux inexplorés dans le domaine de la protection de la vie privée; du travail sur la protection de la vie privée des enfants et des jeunes; un document d'orientation sur la publicité comportementale en ligne; la rédaction de certaines questions de notre sondage d'opinion bisannuel, etc.

Ce n'est là qu'un échantillon des efforts déployés par le Commissariat pour faire en sorte que les Canadiennes et Canadiens acquièrent de solides compétences numériques et comprennent mieux leur droit à la vie privée.

Nous avons fourni aux juristes un guide sur les questions de protection de la vie privée qu'ils sont les plus susceptibles d'aborder dans le cadre d'un litige et de la gestion d'un cabinet d'avocats. Pour les petites entreprises, nous avons rédigé une série d'articles pratiques sur la protection des données utiles, y compris les renseignements personnels des clients, contre les menaces en ligne.

En collaboration avec ses homologues de l'Alberta et de la Colombie-Britannique, le CPVP a aussi conçu un outil électronique novateur permettant aux organisations d'évaluer les mesures de protection des renseignements personnels nécessaires dans les domaines de la gestion des documents, de la sécurité des réseaux, de la planification de la continuité des opérations et dans 14 autres secteurs d'activité.

PRESTATION DE SERVICES

Mon troisième engagement consistait à améliorer les services offerts aux Canadiennes et Canadiens. C'est là le cœur des activités du Commissariat, à commencer par le traitement quotidien des demandes d'information et des plaintes.

Des procédures simplifiées et l'expérience acquise nous ont permis de poursuivre l'amélioration du traitement des plaintes en 2011. La durée moyenne du traitement des plaintes reçues a chuté : elle était supérieure à 15 mois en 2010, alors qu'elle dépasse tout juste huit mois aujourd'hui, ce qui est nettement inférieur aux douze mois prévus par la *Loi*.

L'utilisation plus intensive du processus de règlement rapide, qui permet d'éviter une enquête officielle sur certaines plaintes, est un facteur important de cette amélioration du rendement. En collaborant avec le plaignant et avec l'organisation mise en cause, nos agents de règlement rapide ont réussi à traiter plus

de 90 % des plaintes abordées dans le cadre de ce processus sans avoir recours à une enquête complète.

Dans le but de continuer de répondre aux besoins et aux attentes des Canadiennes et Canadiens dans un monde numérique qui évolue rapidement, nous avons renforcé notre laboratoire technologique. Celui-ci soutien nos vérifications et nos enquêtes par l'entremise de ses experts et il appuiera les responsabilités du CPVP sous le régime de la nouvelle loi antipourriel du Canada.

En tant que haute fonctionnaire du Parlement, j'ai une responsabilité particulière envers les parlementaires. La commissaire adjointe et moi-même ainsi que d'autres cadres supérieurs du Commissariat comparaissent devant des comités, examinent les répercussions des textes législatifs sur la protection de la vie privée, formulent des commentaires et interagissent avec des membres du Parlement et leurs employés dans un cadre moins structuré.

Le Rapport annuel 2011 donne de nombreux autres exemples montrant comment nous avons respecté nos engagements dans ces trois secteurs prioritaires.

CHANGER LES CHOSES

Il faut toutefois se poser la grande question suivante : changeons nous vraiment les choses?

Dix ans après l'adoption de la LPRPDE, des signes encourageants montrent que le CPVP a eu une incidence positive sur la protection de la vie privée.

Selon les sondages d'opinion commandés par le CPVP, le pourcentage de Canadiennes et Canadiens considérant que leur vie privée est moins protégée qu'il y a dix ans est passé de 71 % à 61 % entre 2006 et 2011.

Je crois qu'une part du mérite revient au Commissariat à la protection de la vie privée du Canada pour ce changement de perception au sein du public.

Les défis se sont succédé pour le CPVP au cours des dernières années, et notre équipe de professionnels de haut niveau s'améliore constamment. L'année 2011 ne fait pas exception, et je me considère chanceuse de travailler avec des gens aussi déterminés, assidus et ingénieux.

Parmi ces gens, il y a bien sûr mon indispensable commissaire adjointe, Chantal Bernier, dont l'enthousiasme et la curiosité intellectuelle sans faille sont une source constante d'inspiration.

Malgré l'évolution positive des attitudes du public, la proportion de Canadiennes et Canadiens affirmant que la protection de la vie privée sera l'un des plus importants enjeux au pays au cours des dix prochaines années est demeurée stable entre 2006 et 2011; les deux tiers des personnes sondées ont répondu oui à cette question.

Selon moi, l'explication de ce paradoxe apparent est assez simple.

Les Canadiennes et Canadiens se réjouissent du fait que plus d'efforts sont investis pour protéger leur vie privée et leurs renseignements personnels, mais ils sont également conscients qu'il reste beaucoup de travail à faire à cause des nouveaux défis qui se présentent.

Un des plus importants est l'apparition des données massives, c'est-à-dire la possibilité, grâce aux progrès technologiques, de rassembler plus de données que nous aurions pu imaginer il y a quelques années à peine, puis de les passer au crible pour relever des tendances.

AVANTAGES ET DANGERS

On ne peut nier que la société pourrait parfois profiter des données massives. À titre d'exemple quelque peu prosaïque, Google est maintenant en mesure de découvrir les éclosions de grippe en Amérique du Nord plusieurs jours avant les autorités nationales de la santé en repérant les grappes de demandes de renseignements en ligne au sujet des symptômes et des remèdes.

Des intérêts commerciaux ont rapidement profité de cet avantage indéniable du point de vue de la santé. Un article du New York Times a décrit de quelle manière une grande entreprise de marketing a conçu des publicités pour un thermomètre auriculaire qui ont été envoyées sur les téléphones intelligents ayant téléchargé certaines applications qui recueillaient des renseignements de base sur les utilisateurs, comme le sexe et le nombre d'enfants. Ces publicités visaient spécialement les téléphones intelligents utilisés par les mères de jeunes enfants.

En plus, les publicités n'ont été envoyées que dans les régions où Google a détecté de nombreux cas de grippe et aux mères qui se trouvaient dans un rayon de trois kilomètres d'un détaillant vendant ce thermomètre. L'utilisatrice qui appuyait sur la publicité à l'écran du téléphone intelligent était redirigée vers une page comprenant une vidéo d'information sur le produit et une liste des détaillants à proximité.

Certains seront effrayés de voir des annonceurs faire un suivi aussi personnalisé. D'autres trouveront que les publicités ciblées sont pertinentes et utiles.

Peu importe votre point de vue, ce n'est là que le début des possibilités offertes par les données massives.

Les nombreux nouveaux types de communication numérique — les messages texte, les courriels, la messagerie instantanée, etc. — peuvent tous être très facilement lus par des ordinateurs, et donc faire l'objet d'une analyse complexe par ces engins. Des logiciels perfectionnés permettent de suivre une personne à l'aide du numéro d'identification unique de son appareil. Ils révèlent à quel endroit se trouve la personne à quel moment ainsi que la nature de ses activités sur Internet et de ses interactions avec les personnes qui font partie de sa « communauté ».

Comme le prévoyait Leonard Cohen il y a vingt ans, dans sa chanson prophétique intitulée « The Future », tout à l'avenir sera mesurable.

EXPLOSION DE L'INFORMATION

Jusqu'à tout récemment, la définition de renseignements personnels était assez claire pour la majorité des personnes. Elle comprenait l'information qui se trouve sur une pierre tombale et des renseignements plus traditionnels comme l'adresse, le numéro de téléphone, le numéro d'assurance sociale, le permis de conduire, le passeport, etc. De nos jours, les gens éparpillent des fragments numériques comprenant des renseignements personnels chaque fois qu'ils sont en ligne.

Et la quantité de ces fragments augmente à une vitesse vertigineuse.

Le Commissariat a déjà établi des lignes directrices relatives à l'utilisation de renseignements de cette nature dans le cas précis de la publicité comportementale en ligne, mais il y aura sans doute des utilisations impossibles à prévoir en ce moment qui auront des conséquences graves pour la vie privée.

C'est pour cette raison qu'en fin de compte, il est essentiel d'améliorer la compétence numérique de tous les Canadiens et Canadiennes.

La commissaire à la protection de la vie privée du Canada,

Jennifer Stoddart

La protection de la vie privée en chiffres en 2011

Demandes d'information liées à la LPRPDE reçues	5 236
Plaintes officielles liées à la LPRPDE acceptées	281
Plaintes liées à la LPRPDE réglées rapidement	116
Enquêtes liées à la LPRPDE terminées	120
Lois et projets de loi soulevant des questions ayant trait à la LPRPDE examinés sous l'angle de leurs effets sur la protection de la vie privée	11
Documents d'orientation stratégique publiés	5
Comparutions devant un comité parlementaire	5
Autres interactions avec les parlementaires ou leurs employés (par exemple, des rencontres avec des députés ou des sénateurs)	33
Discours et allocutions prononcés	143
Accords de contribution conclus	8
Visites sur le site Web principal du Commissariat	1 843 686
Visite sur les blogues et autres sites Web du Commissariat (y compris le blogue du CPVP, le blogue pour les jeunes, le site Web pour les jeunes, le site Web sur l'inspection approfondie des paquets et le canal YouTube)	871 698
Total	2 715 384
« Gazouillis » envoyés	416
Publications distribuées	11 811
Communiqués diffusés	37

Nota : Sauf mention du contraire, ces statistiques comprennent également les activités menées sous le régime de la *Loi sur la protection des renseignements personnels*, qui font l'objet d'un rapport annuel distinct.

CHAPITRE 1

Survol de l'année 2011

1.1 PRESTATION DE SERVICES À LA POPULATION CANADIENNE

DEMANDES D'INFORMATION

En 2011, le Commissariat a traité plus de 5 200 appels téléphoniques, courriels et lettres provenant de Canadiennes et Canadiens. Ces communications portaient sur des enjeux de protection des renseignements personnels dans le secteur privé qui sont assujettis à la LPRPDE. Les demandes d'information portent encore souvent sur la question des numéros d'assurance sociale. De plus, nous recevons de plus en plus de demandes liées aux enjeux du cyberespace, surtout en ce qui a trait aux sites de réseautage social. La section 4.1 donne plus de détails à ce sujet.

PLAINTES

Toujours dans l'espoir d'accélérer la prestation des services aux Canadiennes et Canadiens, nous avons créé une unité d'accueil spécialisée qui effectue un examen préliminaire de toutes les plaintes reçues. Au besoin, l'unité assure un suivi auprès du plaignant pour clarifier notre compréhension du dossier et recueillir l'information et les documents nécessaires pour lancer l'enquête le plus tôt possible.

Ce contrôle simplifié a contribué à diminuer la durée moyenne des enquêtes. Cette amélioration et d'autres changements apportés au processus de traitement des plaintes, comme l'utilisation accrue du processus de règlement rapide, ont fait chuter la durée du traitement de toutes les plaintes officielles : la moyenne se situe maintenant à 8,2 mois, bien en deçà du délai maximal de 12 mois imposé par la LPRPDE. (L'annexe 2 donne plus de détails à ce sujet.)

Nous avons reçu 281 plaintes officielles en 2011, comparativement à 207 en 2010. Cette hausse de 35 % s'explique peut être par la complexification des questions traitées, une meilleure connaissance du droit à la vie privée au sein de la population ou des interactions plus intenses avec les entreprises dans le contexte de l'économie numérique.

En 2011, 125 dossiers ont été réglés rapidement, et tous sauf neuf ont été réglés de façon satisfaisante sans qu'une enquête officielle ne soit lancée.

ENQUÊTES SUR LES PLAINTES

Nous avons terminé 120 enquêtes officielles sur des plaintes liées au secteur privé en 2011. Il s'agit d'une forte baisse par rapport à 2010 : cette année là, nous avons parachevé 249 enquêtes pour finir notre opération biennale visant à éliminer un arriéré de plaintes.

Le présent rapport met l'accent sur des enjeux de protection de la vie privée des enfants et des jeunes. Le chapitre 2 comprend des résumés des enquêtes réalisées sur les plaintes déposées à ce sujet.

Les enquêtes portant sur la protection des renseignements personnels d'ordre financier, la vie privée en ligne et la biométrie se trouvent au chapitre 3, qui donne une vue d'ensemble de la protection de la vie privée en 2011. Des renseignements concernant d'autres enquêtes sur des plaintes sont fournis au chapitre 4.

SENSIBILISATION DU PUBLIC

Le Commissariat emploie de nombreux outils pour sensibiliser les Canadiennes et Canadiens à l'importance de la protection de la vie privée : des discours et d'autres allocutions en public; des entrevues dans les médias; des publications sur papier et en ligne; un site Web mis à jour constamment; des médias sociaux comme Twitter et des blogues; des vidéos sur YouTube; des concours pour les jeunes; des trousses pédagogiques pour les enseignants, et même un calendrier sur la protection de la vie privée qui est toujours fort apprécié.

Le chapitre 5 donne plus de détails sur nos activités de sensibilisation du public.

1.2 APPUI AU PARLEMENT

Pour ce qui est des questions législatives, l'élection générale a restreint le calendrier de séances du Parlement et de ses comités en 2011. En outre, les priorités du Parlement étaient surtout axées sur des préoccupations propres au secteur public comme le crime et le budget fédéral. Les comparutions du Commissariat pour des questions liées à la LPRPDE ont donc été moins nombreuses.

Pour la troisième fois depuis 2006, de nouveaux députés ont fait leur entrée à la Chambre des communes à la suite de l'élection fédérale générale du 2 mai 2011. Le Parti conservateur, auparavant minoritaire, a conservé le pouvoir et a obtenu une majorité de sièges pour la 41e législature.

Bien que le gouvernement se soit surtout concentré sur des projets de loi concernant le secteur public, il a aussi redéposé le projet de loi C-12, la *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*. À la fin de l'année, le processus législatif relatif à ce texte venait d'être enclenché et celui-ci n'avait pas encore été présenté à un comité permanent aux fins d'examen.

Le gouvernement a aussi mentionné qu'il présenterait un texte législatif sur la surveillance d'Internet qui n'avait pas été adopté lors de la législature précédente. À cet égard, nous avons continué de faire part de nos préoccupations relatives aux dispositions législatives sur l'accès légal.

COMPARUTIONS DEVANT DES DÉPUTÉS ET DES SÉNATEURS

En 2011, la commissaire et la commissaire adjointe ont comparu devant des comités parlementaires à cinq reprises.

Le CPVP a aussi examiné les éventuelles répercussions sur la protection de la vie privée de onze projets de loi et de deux nouvelles études effectuées par des comités qui ont été présentés au cours de la 41e législature. L'une de ces études portait sur le marché du cybercommerce au Canada et a été réalisée par le Comité permanent de l'industrie, des sciences et de la technologie.

Durant l'année, nous avons également eu des échanges informels avec des parlementaires, comme le suivi de nos comparutions devant les comités, des demandes de renseignements sur des sujets précis formulées par des parlementaires, des rencontres en personne et des séances d'information.

TRAVAUX PARLEMENTAIRES LIÉS À LA LPRPDE

Le calendrier de séances restreint de 2011 a incité le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique à remettre à plus tard l'examen de notre rapport annuel au Parlement de 2010 sur la LPRPDE.

1.3 APPUI AUX ORGANISATIONS

Au cours de la dernière année, nous avons publié le rapport final sur nos consultations de 2010 sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique. Les contributions et les analyses liées aux consultations sont à l'origine de plusieurs activités en 2011, y compris :

- l'élaboration de lignes directrices pour aider les organisations faisant de la publicité comportementale en ligne à s'assurer que leurs pratiques sont équitables, transparentes et conformes à la LPRPDE;
- un travail continu destiné à donner des conseils sur l'infonuagique portant particulièrement sur les enjeux de protection de la vie privée pertinents pour les petites et moyennes entreprises (PME). Ces conseils seront offerts au début de 2012.

Nous avons aussi offert des conseils aux juristes du secteur privé. Le document intitulé *La LPRPDE et votre pratique — Guide sur la protection de la vie privée à l'intention des avocats* a été publié en août. Il

explique comment la LPRPDE s'applique au travail quotidien des avocats canadiens.

Le Commissariat et les Commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique ont conjointement lancé un nouvel outil en ligne destiné à aider les entreprises à mieux protéger les renseignements personnels de leurs clients et de leurs employés. *Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations* est à la fois un questionnaire en ligne détaillé et un outil d'analyse qui aide les organisations à évaluer la qualité de leurs mesures de protection des renseignements personnels, en conformité avec la loi sur la protection des renseignements personnels dans le secteur privé qui s'applique.

Le Bureau de Toronto du CPVP, qui a été créé en 2010, a mené près de 50 activités de sensibilisation en 2011 à l'intention des organisations et des associations industrielles. Ces activités faisaient partie de nos efforts visant à améliorer la compréhension de la LPRPDE et des exigences relatives à la conformité au sein des entreprises.

Le chapitre 5 fournit plus de détails sur ces diverses initiatives.

1.4 DÉVELOPPEMENT DU SAVOIR

DISCUSSIONS INFORMELLES

Une des priorités du Commissariat est d'aider les Canadiennes et Canadiens à mieux comprendre les divers enjeux relatifs à la protection de la vie privée qui les touchent et à connaître les moyens de protéger leur vie privée.

En 2011, nous avons organisé quelques discussions informelles dans le but de présenter des conférenciers qui interpellent les gens et qui présentent de nouveaux points de vue sur la recherche concernant la protection de la vie privée. Nous avons également demandé à chaque participant de présenter de courts documents sur des sujets qui les intéressent dans le domaine de la protection de la vie privée.

En février 2011, nous avons invité l'économiste comportemental Alessandro Acquisti, professeur agrégé en technologie de l'information et en politique publique au Heinz College de l'Université Carnegie Mellon, ainsi que la sociologue Christena Nippert-Eng, professeure agrégée en sociologie au Collège des sciences et des lettres de l'Institut de technologie de l'Illinois, pour discuter de ce qui nous motive à révéler ou à dissimuler les détails de notre vie privée et de la façon dont nous protégeons la vie privée des personnes qui nous entourent.

En avril, nous avons invité des innovateurs dans le domaine de la technologie, Adam Greenfield et Aza Raskin, qui se sont penchés notamment sur les façons dont la protection de la vie privée pourrait être imbriquée dans la conception des appareils

personnels, tels que les téléphones intelligents, qui font littéralement partie de notre quotidien, et dans un environnement où les capteurs se multiplient. Ils ont discuté des occasions que les entreprises doivent saisir pour fournir davantage de choix et de contrôle aux personnes relativement à l'utilisation de leurs données personnelles, et de la possibilité d'établir une meilleure collaboration au sein de leur secteur d'activités et entre les différents secteurs de l'industrie.

En juin, David Murakami-Wood, titulaire d'une chaire de recherche du Canada et professeur agrégé au Département de sociologie de l'Université Queen's, et Craig Forcese, professeur agrégé à la Faculté de droit de l'Université d'Ottawa, ont tous deux examiné les risques pour la protection de la vie privée dans une société qui surveille de plus en plus ses citoyens.

En septembre, nous avons invité deux spécialistes de l'utilisation des médias sociaux chez les jeunes, Kate Raynes-Goldie, étudiante au doctorat au Département des études d'Internet de l'Université de technologie Curtin, et Matthew Johnson, directeur de l'éducation au Réseau Éducation-Médias, pour parler de ce que signifie la protection de la vie privée pour les jeunes et de la manière d'aider ces derniers à préserver leur vie privée en faisant la promotion des compétences numériques.

1.5 INITIATIVES MONDIALES

COOPÉRATION CONCERNANT L'APPLICATION DE LA LOI

En 1973, la Suède a promulgué la première loi nationale sur la protection des renseignements personnels au monde. Quatre décennies plus tard, environ 80 lois nationales sur la protection des renseignements personnels, ou sur la protection des données, comme on les appelle souvent, sont en vigueur dans le monde. Bon nombre d'entre elles ont été adoptées depuis la promulgation de la LPRPDE, le 1er janvier 2001.

Bien que la portée et l'application de ces lois divergent grandement, ces dernières sont généralement fondées sur les « principes relatifs à l'équité dans le traitement de l'information », qui forment l'annexe 1 de la LPRPDE.

Puisqu'ils s'appuient sur les mêmes principes, les commissaires à la protection de la vie privée et les autorités responsables de la protection des données peuvent poursuivre des objectifs communs, même si les lois sont formulées différemment. Par exemple, la « limitation de la collecte » de la LPRPDE correspond au concept de « minimisation des données » dans le droit européen.

En plus d'avoir des objectifs semblables, c'est-à-dire la promotion de la protection des renseignements personnels et des droits de chacun, les autorités

chargées de l'application des lois protégeant la vie privée doivent relever sensiblement les mêmes défis.

Les questions de protection de la vie privée prennent une envergure mondiale. Partout dans le monde, de plus en plus de personnes utilisent les mêmes technologies de l'information et des communications; elles échangent de l'information, des vidéos et des photos à l'aide d'une poignée de sites de réseautage social très populaires; elles jouent à des jeux en ligne sur les mêmes plateformes; elles effectuent des recherches sur les mêmes moteurs de recherche. Par conséquent, quand une de ces multinationales modifie ses pratiques de protection de la vie privée, ou pire encore, est victime d'une atteinte à la protection des renseignements personnels (comme nous l'avons vu sur le réseau PlayStation de Sony en 2011), des millions de personnes sont touchées dans le monde entier.

Pour s'attaquer à des problèmes d'envergure mondiale, il faut une réaction mondiale. Grâce aux modifications apportées à la LPRPDE qui sont entrées en vigueur en 2011, le Commissariat est beaucoup mieux placé pour coopérer avec ses homologues étrangers dans le cadre de dossiers qui touchent des personnes vivant sur d'autres territoires.

Nous pouvons maintenant collaborer et échanger des renseignements avec des responsables ou des organismes d'un État étranger qui exercent, en vertu de lois, des fonctions et responsabilités semblables aux nôtres, ou avec des responsables ou des organismes qui exercent des responsabilités en vertu de lois se rapportant à un comportement qui contreviendrait à la LPRPDE. En mettant en commun nos connaissances et l'information que nous obtenons à la faveur de nos enquêtes, nous pouvons utiliser nos ressources plus efficacement et mener des enquêtes plus approfondies et efficientes.

Notre autorisation de communiquer des renseignements est assortie de conditions, notamment la conclusion d'un accord écrit avec l'autre partie qui doit comprendre des clauses de confidentialité limitant l'utilisation des renseignements que nous communiquons ou recevons. Des accords avec les commissaires à la protection des données des Pays-Bas et de l'Irlande étaient en voie d'être parachevés à la fin de 2011.

Le Commissariat a aussi fait preuve de leadership en favorisant la coopération de façon plus générale.

À la 33e Conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu à Mexico en novembre 2011, les commissaires ont adopté une résolution sur l'intensification de la coordination de l'application de la loi à l'échelle internationale. Le Commissariat est l'un des coprésidents d'un groupe de travail qui a été créé dans le but d'élaborer un cadre et des processus relatifs à d'éventuelles mesures de coordination de l'application de la loi.

Le groupe de travail s'appuiera sur le succès du Global Privacy Enforcement Network (GPEN) et de l'Accord de coopération de l'APEC (la Coopération économique Asie-Pacifique) sur la protection

transfrontière des données, dont nous avons parlé dans notre rapport annuel de 2010.

Le Commissariat est l'un des membres fondateurs du GPEN, qui compte maintenant plus de 20 membres.

Nous sommes également partie à l'Accord sur la protection transfrontière des données, qui regroupe seulement les autorités responsables de l'application de la loi de la région de l'Asie-Pacifique et qui compte maintenant des membres de six économies de l'APEC.

Par ailleurs, le Commissariat est membre du forum des autorités à la protection de la vie privée de l'Asie-Pacifique composé de responsables de la protection de la vie privée dans la région Asie-Pacifique. Le forum a lieu deux fois par année et permet d'échanger des idées et des pratiques exemplaires liées à la réglementation de la protection des renseignements personnels, aux nouvelles technologies et à la sensibilisation aux enjeux de protection de la vie privée.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'Organisation de coopération et de développement économiques (OCDE) ont été élaborées il y a plus de 30 ans. Bien que ce document se soit avéré extrêmement solide, le monde a radicalement changé depuis cette époque.

Consciente de cette situation, l'OCDE a amorcé un examen de ces lignes directrices pour vérifier si elles sont toujours pertinentes « compte tenu de l'évolution des technologies, des marchés et du comportement des utilisateurs ainsi que de l'importance croissante des identités numériques ». Le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée (GTSIVP) réalise cet examen. Il est conseillé et appuyé par un groupe de bénévoles multilatéral présidé par la commissaire Stoddart.

Le groupe de bénévoles formulera des recommandations préliminaires au GTSIVP pouvant porter sur une vaste gamme de sujets. Le Groupe de travail déterminera si les lignes directrices technologiquement neutres sont toujours d'actualité ou s'il faut mettre à jour ou réviser certaines d'entre elles.

FRANCOPHONIE

Le Commissariat a joué un rôle essentiel dans la création, en 2007, d'une organisation représentant les autorités francophones responsables de la protection des données du monde entier : l'Association francophone des autorités de protection des données personnelles (AFAPDP). Nous sommes déterminés à aider l'AFAPDP à accroître son appui aux pays de la Francophonie en voie de développement dans le cadre de leurs efforts destinés à établir un nouveau cadre législatif protégeant le droit à la vie privée de leurs citoyens.

En 2011, la commissaire adjointe Chantal Bernier a assisté, à Dakar (Sénégal), au premier séminaire

de formation de l'Association à avoir lieu sur le continent africain. Au cours de ses allocutions, elle a discuté de l'application des principes de protection des renseignements personnels sous divers régimes juridiques et elle a donné un aperçu de l'importance des lignes directrices de l'OCDE depuis leur création.

Lors d'un deuxième séminaire de l'AFAPDP, qui s'est tenu en parallèle avec la Conférence internationale des commissaires à la protection des données et de la vie privée à Mexico, elle a élaboré sur le principe de responsabilité et sa mise en pratique.

1.6 LABORATOIRE TECHNOLOGIQUE

Notre laboratoire technologique et sa petite équipe permettent au CPVP de rester à jour dans le domaine des nouvelles technologies. Ils fournissent une expertise et soutiennent les vérifications et les enquêtes dans les cas où la technologie joue un grand rôle. Ces technologies varient énormément et vont des applications aux téléphones intelligents en passant par les consoles de jeux. Les technologues du laboratoire peuvent examiner de tels appareils ou applications pour savoir quels renseignements personnels sont stockés, quelles données sont échangées sur le Web et comment ces données sont protégées.

À titre d'exemple de préoccupation actuelle relative à la protection des renseignements personnels, le laboratoire est en mesure d'analyser les techniques de suivi utilisées par ceux qui font de la publicité comportementale en ligne et l'efficacité des contrôles de confidentialité sur les sites de réseautage social.

CHAPITRE 2

Principal enjeu : La protection de la vie privée des enfants et des jeunes

INTRODUCTION

Dans le combat visant à préserver la vie privée dans un monde en ligne, les enfants et les jeunes sont de plus en plus sur les lignes de front.

Les jeunes Canadiennes et Canadiens sont les plus enclins à adopter les nouvelles technologies de communication qui peuvent, dans certains cas, porter atteinte à leur vie privée. Il n'y a rien d'étonnant à ce que cela s'applique aux jeunes de 18 à 34 ans, comme l'a confirmé un sondage d'opinion national mené cette année pour le compte du Commissariat (voir la section 3.3).

Cependant, la jeune génération adopte sans hésitation les médias numériques bien avant cet âge.

Nous savons, par exemple, que des milliers d'applications s'adressant aux bébés et aux jeunes enfants sont désormais disponibles pour montrer aux tout-petits l'alphabet et les amuser avec des comptines.

Même si les éléments de preuve à cet égard relèvent encore majoritairement de l'anecdote, une étude récente n'en conclut pas moins que le tiers des mères de la génération Y de l'Amérique du Nord (celles qui ont de 18 à 27 ans) ont laissé leur enfant utiliser un ordinateur portable avant l'âge de deux ans.

Pour le quart des enfants américains de trois ans, ces ordinateurs portables et tablettes sont connectés à Internet tous les jours, selon le Joan Ganz Center de New York. Pour les enfants de cinq ans, c'est la moitié qui ont accès à Internet.

Nous donnons à nos enfants un accès sans précédent à Internet, mais que faisons nous pour leur apprendre à protéger leur vie privée dans un environnement numérique?

On dit souvent que les jeunes de l'ère numérique ne se soucient guère de protéger leur vie privée. C'est faux.

Bien que les notions relatives à la protection de la vie privée évoluent, et que les jeunes aient tendance à avoir de la vie privée une conception différente de celle de leurs parents, des études successives montrent que les jeunes ont à cœur la protection de leur vie privée.

Quand nous donnons des conférences dans les écoles, les jeunes nous disent qu'ils veulent protéger leur réputation sur le Web, mais nombre d'entre eux ne savent pas comment faire. Ils nous demandent des conseils sur la façon d'exercer un contrôle sur l'accès à leur profil en ligne. Ils veulent savoir comment bloquer les contacts inopportuns sur les sites de réseautage social et comment voir ce que d'autres personnes affichent à leur sujet.

Un certain nombre de raisons expliquent pourquoi de nombreux jeunes Canadiens et Canadiennes se heurtent aux failles de la protection de la vie privée sur le Web.

Une des raisons tient au fait qu'ils sont tellement entichés des technologies en ligne qu'ils essaient parfois les nouvelles applications avant que toutes les lacunes en matière de protection de la vie privée aient été relevées et comblées.

De plus, les jeunes ont tendance à croire que leur espace en ligne est privé et que seuls leurs amis en verront le contenu. Ils vivent au présent et oublient souvent que les messages qu'ils envoient ou qu'ils publient aujourd'hui pourraient leur causer du tort dans l'avenir.

Les adolescents qui grandissent dans un monde en ligne font l'objet d'une surveillance et d'une analyse sans précédent.

Un grand nombre des intervenants en ligne se disputent l'attention et la faveur des jeunes dans le but de commercialiser leurs renseignements personnels. Un peu plus loin, nous racontons l'histoire d'un site Web qui tire des revenus de messages publicitaires ciblant les jeunes de 13 à 18 ans, qui représentent le tiers de ses utilisateurs.

Pourtant, même si de nombreux efforts sont consacrés à l'exploitation des renseignements personnels des jeunes et des enfants à des fins lucratives, beaucoup moins de ressources visent à aider les enfants et les jeunes à reconnaître l'importance de la protection de la vie privée et à acquérir les compétences voulues pour protéger leurs renseignements personnels.

Les enfants et les jeunes font face à des dangers particuliers en matière de protection de la vie privée parce qu'ils n'ont pas les connaissances ni l'expérience voulues pour bien évaluer les risques et prendre les mesures qui s'imposent pour y faire échec.

Pour ces raisons, le Commissariat a intensifié ses efforts auprès de ce segment vulnérable de la société canadienne.

Au cours de la dernière année, nous avons élaboré deux trousses abondamment illustrées sur la protection de la vie privée destinées aux milieux scolaire et communautaire, une vidéo s'adressant aux adolescents et des conseils pour les parents. Nous avons maintenu un concours populaire invitant les adolescents à produire de courtes vidéos sur des questions relatives à la protection de la vie privée. Nous avons également continué d'ajouter des ressources documentaires sur notre site Web et notre blogue destinés aux jeunes.

De plus, le Programme des contributions du Commissariat a récemment financé trois initiatives novatrices de recherche et d'éducation du public explorant la relation entre les jeunes et la protection de la vie privée et favorisant la protection des renseignements personnels chez les jeunes.

Cependant, nous ne devons surtout pas en rester là.

Une étude sur les compétences numériques menée dans cinq pays par le Réseau Éducation-Médias pour le Commissariat a conclu que, au Canada, la protection de la vie privée sur le Web ne reçoit pas toute l'attention voulue dans l'enseignement des aptitudes technologiques. De plus, il n'existe pas de stratégie visant la coordination des efforts de sensibilisation à cet égard.

Parmi les neuf recommandations découlant de l'étude du Réseau Éducation-Médias, qui sont énoncées au chapitre 2, mentionnons l'acquisition de compétences numériques par l'ensemble des Canadiennes et Canadiens, telles que la connaissance du droit à la vie privée et des recours en la matière.

Une idée, parmi d'autres : Pourquoi ne pas décerner des insignes aux jeunes qui maîtrisent les compétences numériques, comme ceux remis par les guides et les scouts?

Les idées novatrices comme celle-ci aideraient également les parents qui cherchent à améliorer leurs propres compétences numériques tout en essayant de transmettre à leurs enfants un nouvel ensemble d'aptitudes au quotidien.

On peut comprendre que des parents souhaitent utiliser les nouvelles technologies pour assurer la sécurité de leurs enfants. Cependant, cette volonté peut entraîner le recours à la surveillance vidéo et par GPS, qui ne tient guère compte du droit à la vie privée des enfants et des jeunes.

Il s'agit d'éléments importants parce que, d'abord et avant tout, les enfants retiennent du concept de la protection de la vie privée ce qu'ils voient à la maison.

Notre examen d'études menées dans ce domaine montre que si les enfants sont élevés dans un contexte de surveillance qui fait fi de la vie privée, ils risquent de n'accorder à celle-ci aucune importance. Ces enfants pourraient également ne pas apprendre comment établir leurs propres limites en matière de

protection de la vie privée et être moins disposés à respecter les limites d'autrui.

Peut-être pire encore, la surveillance constante peut susciter la méfiance et la dissimulation dans la vie familiale, en encourageant les enfants à cultiver le secret. Par exemple, si maman surveille la porte d'entrée principale au moyen d'une caméra de surveillance en ligne connectée au système de sécurité de la maison, sa fille pourrait être tentée de faire entrer son petit ami par la porte arrière.

À première vue, de telles spéculations peuvent sembler exagérées, voire alarmistes.

Cependant, danah boyd, spécialiste de la protection de la vie privée de l'Université de New York et de Microsoft, a signalé que les adolescents ont déjà concocté des moyens pour contrer la surveillance parentale dans les forums semi-publics comme Facebook.

Les adolescents maquillent les messages sur leur état d'esprit visibles par tous, a expliqué danah boyd, en utilisant des expressions et références culturelles ayant une connotation spéciale pour leurs amis, mais ne disant rien de particulier aux adultes.

Danah boyd donne l'exemple d'une adolescente malheureuse à la suite d'une rupture amoureuse. Pour cacher son état d'esprit à sa mère, la jeune fille avait affiché sur Facebook les paroles de la chanson de Monty Python's intitulée « Always Look on the Bright Side of Life » (Regarde toujours le bon côté de la vie). Sa mère avait alors répondu par quelques mots indiquant que sa fille semblait heureuse.

Cependant, ses amis avaient compris le contraire étant donné que la chanson est extraite d'un film montrant des personnages sur le point de mourir. Ils ont immédiatement contacté la jeune fille pour lui demander si elle allait bien.

2.1 ENQUÊTES CONCERNANT LES ENFANTS ET LES JEUNES

Enquête sur Nexopia : Un site Web ciblant les jeunes règle certains problèmes liés à la protection de la vie privée mais pas tous

La première enquête menée par le Commissariat à l'égard d'un site de réseautage social ciblant les jeunes a mis au jour d'importantes lacunes en matière de protection de la vie privée. Le cas peut faire école en ce qui concerne les éléments à éviter pour les sites Web qui encouragent la collecte et la publication de renseignements personnels des jeunes.

L'enquête approfondie menée sur Nexopia a fait ressortir plusieurs domaines dans lesquels l'organisation

contrevenait à la LPRPDE et donné lieu à 24 recommandations. Un grand nombre des préoccupations auraient pu être évitées s'il avait été davantage tenu compte de la protection de la vie privée au moment de la création du site Web.

Nexopia a fait montre d'ouverture d'esprit et d'une volonté de coopérer pendant l'enquête, et la commissaire s'est dite satisfaite de la réponse de l'organisation à 20 recommandations. Cependant, quatre recommandations se rapportant à la conservation indéfinie des renseignements personnels n'avaient pas été réglées à la fin de 2011.

CONTEXTE

Créée en 2003, Nexopia, qui a son siège à Edmonton, précède un grand nombre d'autres médias sociaux populaires sur le Web. L'organisation se targue de compter plus de 1,6 million d'utilisateurs inscrits, dont plus du tiers ont de 13 à 18 ans. Environ la moitié des utilisateurs sont de l'Alberta et de la Colombie-Britannique.

Nexopia se considère comme une « communauté ouverte », au contraire des sites comme Facebook. Même si 90 % de ses utilisateurs sont également inscrits sur Facebook, Nexopia soutient que sur Facebook ils communiquent avec leurs vrais amis, tandis que sur Nexopia ils communiquent avec leurs amis virtuels et se mettent en valeur aux yeux du monde.

Comme l'a indiqué la commissaire Stoddart : « Le fait que le site soit destiné aux jeunes a grandement influencé notre démarche au cours de cette enquête. Puisqu'il y a tant de jeunes utilisateurs de Nexopia, il faut redoubler d'efforts pour s'assurer qu'ils connaissent bien les pratiques du site en matière de protection des renseignements personnels. »

« Les autres sites Web destinés aux jeunes doivent prendre note de cette enquête et s'assurer qu'ils ont bien étudié les facteurs relatifs à la protection des renseignements personnels propres à un contexte où les jeunes sont concernés. »

NOS CONSTATATIONS

Notre enquête part d'une plainte du Centre pour la défense de l'intérêt public (CDIP), établi à Ottawa. Les principaux domaines dans lesquels Nexopia contrevient à la LPRPDE sont les suivants :

- paramètres par défaut qui ne conviennent pas à un jeune public et manque d'information précise quant aux paramètres de confidentialité disponibles;
- absence d'un consentement éclairé des utilisateurs pour la collecte, l'utilisation et la communication des renseignements personnels demandés à l'inscription;
- communication de renseignements personnels à des annonceurs et d'autres tierces parties sans un consentement adéquat;
- conservation pour une période indéfinie des renseignements personnels.

ENJEUX

1. Communication des profils d'utilisateur au public et paramètres de confidentialité par défaut

Au début de notre enquête, les paramètres de confidentialité par défaut de Nexopia étaient fixés à « visible to all » (accessible à tous) — c'est-à-dire que les renseignements pouvaient être consultés par tous les internautes.

Compte tenu des circonstances spéciales associées à la protection des renseignements personnels des jeunes utilisateurs, le CPVP a conclu qu'une personne raisonnable trouverait inapproprié que Nexopia choisisse préalablement des paramètres qui incitent les utilisateurs à dévoiler leurs renseignements personnels, qui sont parfois très délicats, à n'importe qui sur Internet.

L'enquête a aussi révélé que Nexopia n'informe pas suffisamment ses utilisateurs au sujet des paramètres de confidentialité par défaut et n'explique pas adéquatement les différences entre les divers paramètres.

Le Commissariat a conclu qu'il serait possible de donner plus d'information sur les paramètres de confidentialité qui sont en place afin que les utilisateurs puissent prendre des décisions éclairées concernant le contrôle de l'accès à leurs renseignements personnels.

On devrait s'attendre à ce que les utilisateurs de Nexopia choisissent activement le paramètre « accessible à tous » — en sachant parfaitement ce que cela implique.

Selon le Commissariat, des paramètres par défaut plus restrictifs, jumelés à une plus grande quantité d'information offerte aux utilisateurs et transmise d'une manière adaptée aux jeunes, permettraient d'atteindre un juste équilibre entre les avantages du réseautage social et la protection de la vie privée.

Le CPVP est convaincu que nos recommandations seront appliquées grâce aux mesures correctrices proposées par Nexopia, qui comprennent la modification des paramètres par défaut et de meilleurs renseignements fournis aux utilisateurs.

2. Absence d'un consentement valable à la collecte, à l'utilisation et à la communication des renseignements personnels recueillis au moment de l'inscription

Notre enquête a révélé que Nexopia ne fournit pas assez d'information sur les objectifs de la collecte, de l'utilisation et de la communication des renseignements personnels que les utilisateurs doivent fournir au moment de s'inscrire.

Par exemple, il est difficile de savoir quels renseignements « de base » et photos figurant dans le profil seraient accessibles par défaut aux utilisateurs de la communauté Nexopia et à tous les internautes.

Nexopia a reconnu que la version actuelle de sa politique de confidentialité n'a pas nécessairement été rédigée en fonction des besoins des jeunes.

Nexopia se fiait passivement aux utilisateurs pour qu'ils lisent et acceptent les modalités de sa longue politique de confidentialité officielle afin d'obtenir leur consentement. Le Commissariat considère qu'un simple lien au bas de la page d'inscription menant à la politique est insuffisant pour obtenir un consentement approprié de la part des jeunes ciblés par l'entreprise.

Le CPVP se réjouit du fait que Nexopia a accepté de mettre à jour sa politique de confidentialité, d'ajouter de l'information et d'utiliser un langage adapté à ses principaux utilisateurs. L'entreprise exigera aussi des utilisateurs qu'ils révisent sa politique de confidentialité dans le cadre du processus d'inscription. Toutefois, le Commissariat a invité Nexopia à examiner des méthodes plus novatrices pour présenter sa politique de confidentialité.

3. Échange de renseignements personnels avec d'autres tierces parties sans consentement valable

Les renseignements que Nexopia fournit aux utilisateurs concernant ses pratiques publicitaires, surtout en ce qui concerne l'échange de renseignements personnels avec des annonceurs, sont incomplets. Des renseignements personnels sont parfois échangés sans que les utilisateurs soient avisés clairement.

Par exemple, Nexopia n'explique pas de façon détaillée en quoi consiste la publicité ciblée et comment fonctionne ce type de publicité. De plus, la politique de confidentialité ne précise pas que l'entreprise permet à de tierces parties, comme des réseaux publicitaires, d'installer des témoins dans les navigateurs des utilisateurs et des visiteurs afin de recueillir des renseignements sur l'utilisation du Web.

Le CPVP estime que l'utilisation de renseignements personnels par Nexopia à des fins publicitaires et la diffusion de publicités comportementales ciblées visant les utilisateurs est une condition de service acceptable, pourvu que les personnes concernées soient pleinement conscientes de la façon dont ces pratiques s'appliquent.

Le Commissariat est cependant d'avis que les personnes devraient pouvoir refuser le suivi de leurs activités par des tiers — dont l'identité leur est habituellement inconnue.

Nexopia a accepté de fournir plus de renseignements dans sa politique de confidentialité et sur son site Web au sujet de la publicité ciblée et de la présence de témoins de suivi et de publicités ciblées affichées par des tiers. Ces changements comprendront des liens vers des pages présentant de l'information sur les publicités et les témoins qui se trouvent sur le site — ainsi que sur la façon dont les témoins fonctionnent et peuvent être supprimés.

Le CPVP est satisfait de la réponse de Nexopia à nos préoccupations.

4. Échange de renseignements personnels avec de tierces parties sans consentement valable

Nexopia communique régulièrement les codes d'utilisateur uniques à l'entreprise responsable du traitement des paiements lorsque des utilisateurs effectuent des achats sur le site. Le site Web communique également l'âge, le sexe et le code d'utilisateur unique à l'entreprise offrant des récompenses chaque fois qu'un utilisateur participe aux offres « Earn Plus » (Obtenez Plus).

Le site n'expliquait pas aux utilisateurs que leurs renseignements personnels pouvaient être communiqués à l'entreprise offrant des récompenses ou que cette communication pouvait s'ajouter aux renseignements que l'utilisateur fournit déjà directement à cette entreprise à titre de condition à une offre particulière « Obtenez Plus ». Nexopia a admis que les énoncés en ligne et les pratiques de communication réelles étaient devenus trompeurs.

Nexopia affirme que l'information fournie à l'entreprise responsable du traitement des paiements et à l'entreprise offrant des récompenses ne pouvait être utilisée pour identifier des utilisateurs ou pour obtenir d'autres renseignements à leur sujet. Cependant, nos tests ont démontré que le code d'utilisateur unique peut être lié au profil de l'utilisateur et possiblement donner accès à tous les renseignements personnels qui s'y trouvent.

À notre avis, Nexopia pourrait utiliser un autre code unique ou numéro d'identification qui limiterait la quantité de renseignements personnels échangés entre les parties, et qui permettrait tout de même de traiter efficacement la facturation et les paiements.

Nexopia a accepté d'arrêter de fournir les codes d'utilisateur uniques à l'entreprise responsable du traitement des paiements et de retirer entièrement le service « Obtenez Plus » du site. Par conséquent, le site ne communiquera plus les renseignements personnels des utilisateurs à l'entreprise offrant des récompenses.

Le CPVP est satisfait de la réponse de Nexopia.

5. Conservation des renseignements personnels

Nexopia recueille les adresses électroniques des non-utilisateurs à partir d'invitations à joindre le site envoyées par les utilisateurs. Avant de fournir au site l'adresse électronique de l'ami, les utilisateurs n'ont pas besoin de confirmer à Nexopia qu'ils ont le consentement de leur ami pour ce qui est de l'envoi de l'invitation à se joindre au site Web.

Un non-utilisateur qui ne veut plus recevoir d'invitations peut cliquer sur un lien qui le transfère à une page intitulée « Opt out of Nexopia.com invites » (ne plus recevoir d'invitations de Nexopia.com).

Toutefois, le non-utilisateur n'est pas informé que Nexopia conservera son adresse électronique. Pour que cette fonction soit efficace, le site explique qu'il doit conserver, pour une durée indéterminée, une liste des adresses auxquelles plus aucun message ne sera envoyé à l'avenir.

Selon nous, il est important que l'utilisateur fournissant l'adresse électronique s'assure d'avoir obtenu le consentement préalable du propriétaire de cette adresse, c'est-à-dire de son ami, pour que Nexopia envoie le courriel d'invitation.

Le Commissariat a aussi recommandé à Nexopia d'offrir aux non-utilisateurs un choix clair entre a) ne plus recevoir les courriels d'invitation à se joindre au site et b) la suppression permanente de leur adresse électronique.

Le CPVP est satisfait de la réponse de Nexopia à nos préoccupations relatives à ce sujet.

Nexopia a convenu d'ajouter un avis à sa fonction « Find and Add Friends » (rechercher et ajouter des amis) pour informer les utilisateurs qu'ils doivent obtenir le consentement préalable des non-utilisateurs avant de fournir leurs adresses électroniques au site Web.

L'entreprise a également accepté de faire en sorte qu'à l'avenir, les non-utilisateurs qui reçoivent des courriels d'invitation seront en mesure de demander la suppression permanente de leur adresse électronique dans les bases de données de Nexopia.

Le Commissariat s'est aussi penché sur la question de la suppression des comptes.

Lorsque les utilisateurs cliquent sur l'option « Delete Account » (supprimer un compte), ils apprennent que : *Cette action supprimera votre compte, y compris votre profil, vos photos, votre liste d'amis, vos messages, etc. Vos articles de forum, vos commentaires et vos messages contenus dans la boîte de réception d'autres utilisateurs ne seront pas supprimés* [traduction].

En fait, Nexopia nous a informés que seuls les « cris » de l'utilisateur sont supprimés. Les autres renseignements sont stockés indéfiniment (par exemple le nom d'utilisateur; le code d'utilisateur; l'adresse électronique; l'adresse IP et les renseignements de connexion; la liste d'amis; les galeries de photos; le contenu du profil; les messages et les commentaires; les photos du profil).

Une autre préoccupation est liée à la désactivation des comptes, que la décision provienne de Nexopia ou de l'utilisateur. Les renseignements personnels qui se trouvent dans les comptes désactivés demeurent inactifs sur les serveurs de Nexopia pour une durée indéterminée et ne font pas l'objet d'examens périodiques.

Nexopia a admis qu'elle n'a pas supprimé l'information contenue dans les comptes depuis 2004, que ce soit dans les comptes « supprimés » ou désactivés.

Il est manifestement trompeur de fournir une option « supprimer un compte ». Le CPVP a recommandé que Nexopia fournisse une véritable option de suppression des comptes et des renseignements personnels des utilisateurs.

Malheureusement, Nexopia a affirmé qu'elle n'appliquera pas cette recommandation, car le coût de cette opération serait prohibitif. Elle a également soutenu que les renseignements enregistrés dans les

archives ne sont accessibles qu'aux administrateurs du système et sont seulement récupérés si le site reçoit un mandat de la part d'un organisme d'application de la loi.

Le CPVP ne sous-estime pas les défis techniques associés à l'élimination permanente des renseignements personnels des utilisateurs, mais la pratique d'archiver indéfiniment tous les renseignements personnels d'une personne va à l'encontre de la LPRPDE.

Il est clair que les organismes d'application de la loi ont parfois besoin d'accéder à l'information. De tels demandes ou mandats peuvent justifier une période de conservation plus longue dans certains cas particuliers, mais ils ne justifient pas la conservation entière et indéfinie de tous les dossiers sous prétexte qu'une demande pourrait être faite un jour.

La pratique de Nexopia qui consiste à conserver indéfiniment des renseignements personnels dans ses archives, au cas peu probable où ces renseignements feraient l'objet d'un mandat, n'est donc pas acceptable.

De plus, la conservation d'une grande quantité de renseignements personnels concernant les anciens utilisateurs, bien après que le but d'origine a été atteint, comporte des risques de sécurité. En outre, le Commissariat craint que les utilisateurs de Nexopia aient l'impression qu'ils pourront supprimer leurs renseignements personnels s'ils le désirent, ce qui est trompeur.

À la fin de notre enquête, cette question n'était toujours pas résolue. Le CPVP s'attaque aux questions non résolues à l'aide des pouvoirs qui nous sont conférés par la LPRPDE, ce qui comprend la possibilité de demander à la Cour fédérale que les recommandations soient appliquées.

Le rapport d'enquête intégral figure sur notre site Web.

Une garderie a modifié son système de surveillance par caméra Web afin d'accroître la protection de la vie privée

CONTEXTE

Le plaignant avait inscrit son fils dans une garderie privée et appris que les parents pouvaient profiter de services de surveillance par caméra Web, moyennant des frais, pour pouvoir observer le local de leur enfant en temps réel. Les parents regarderaient les images transférées par la caméra Web sur Internet après avoir inscrit un mot de passe qui leur est propre.

La garderie a indiqué qu'elle avait instauré le service de caméra Web pour deux raisons : la première, pour pouvoir surveiller les locaux pour des raisons de sécurité et, la seconde, pour montrer aux parents le déroulement des activités.

La garderie a indiqué au Commissariat qu'environ 60 % des parents des enfants inscrits s'étaient abonnés au service de surveillance.

Le plaignant a par la suite appris que les images captées par la caméra Web étaient enregistrées. Il a fait

savoir à la garderie qu'il s'opposait à l'enregistrement et que celle-ci n'avait pas instauré des mesures adéquates de protection de la vie privée.

La garderie, après avoir appris qu'une enquête était en cours, a supprimé les fichiers de surveillance vidéo et modifié ses systèmes de manière à ce que ceux-ci n'enregistrent plus les images captées par la caméra Web. Elle a également instauré une politique de confidentialité exigeant que tous les parents signent un formulaire de consentement à la surveillance par caméra Web, et ce, qu'ils s'inscrivent ou non au service.

La garderie a reconnu qu'un parent pourrait enregistrer et diffuser les images captées par la caméra Web et visionnées sur son ordinateur personnel. Conformément à la suggestion du Commissariat, la garderie a demandé aux parents qui utilisent le service de caméra Web de signer un contrat en vertu duquel ils s'engagent à ne pas enregistrer les images captées par la caméra Web et à garder leur mot de passe secret.

NOS CONSTATATIONS

Il s'agissait de déterminer si la garderie recueillait les renseignements personnels du fils du plaignant sans le consentement de ce dernier et avait négligé de protéger comme il se doit les renseignements personnels du fils.

Au départ, le Commissariat estimait que la garderie ne respectait pas les principes 4.7 (mesures de sécurité) et 4.3 (consentement) ainsi que le paragraphe 5(3) (fins acceptables) de la LPRPDE et avait recommandé que la garderie abandonne son système de surveillance par caméra Web.

Pendant l'enquête, toutefois, la garderie a amélioré ses mesures de sécurité organisationnelles et technologiques en cessant d'enregistrer les images captées par vidéo, en mettant en œuvre une politique de confidentialité et en améliorant les caractéristiques de protection par mots de passe. Quoi qu'il en soit, le Commissariat a recommandé que la garderie perfectionne ses mesures de sécurité technologiques et mette en œuvre d'autres dispositions contractuelles afin de prévenir une utilisation à mauvais escient des renseignements recueillis par caméra Web.

Pendant l'enquête, le Commissariat a consulté le ministère des Services à l'enfance et à la jeunesse de l'Ontario, qui a indiqué que, sur les 4 784 programmes de garde d'enfants autorisés en Ontario, seulement 61 offraient la transmission d'images vidéo en direct et que plusieurs garderies sans services de surveillance par caméra Web existaient près du domicile du plaignant. Comme il semble que plusieurs options s'offrent aux parents en matière de garderies, rien ne prouve que le consentement n'était pas volontaire.

CONCLUSION

La garderie a fait savoir qu'elle avait mis en œuvre toutes les recommandations du Commissariat, et nous avons conclu que la plainte avait été résolue.

2.2 SURVEILLANCE DES ENFANTS

Après avoir traité la plainte susmentionnée, le Commissariat a décidé qu'il serait utile d'approfondir des questions connexes et a mené une recherche au sujet des effets de la surveillance sur les enfants.

Nous avons procédé à une revue documentaire visant le recensement et l'analyse des travaux de recherche portant sur l'incidence des pratiques en vigueur en matière de surveillance sur les enfants, y compris la surveillance vidéo et en ligne et l'utilisation de la biométrie.

Nous avons examiné la surveillance au Canada et dans les sociétés semblables à la nôtre en étudiant les travaux qui ont déjà été effectués. Malgré le nombre limité d'études dans le domaine, la conclusion générale veut qu'une surveillance constante change à long terme la façon dont les enfants voient le monde et interagissent avec les autres.

Tous les travaux de recherche ont souligné la présence envahissante de la surveillance dans la vie des enfants d'aujourd'hui. En effet, les parents utilisent des appareils de surveillance des bébés et des gardiennes et, plus tard, Internet, des logiciels de surveillance des téléphones cellulaires et les systèmes GPS. Les écoles ont des caméras de sécurité, des appareils d'identification par radiofréquence (IRF) et des lecteurs de géométrie palmaire. Les entreprises surveillent l'activité des enfants en ligne à des fins de marketing.

La surveillance est maintenant la norme, et ce, pour plusieurs raisons. Les parents sont très inquiets en raison des reportages faisant état avec moult détails des risques posés par les « inconnus » (démentis par les statistiques), et la surveillance est abordable, accessible et facile à utiliser.

De plus, ils voient l'État faire appel à la surveillance pour détecter et prévenir les comportements asociaux, tandis que les entreprises font appel à la surveillance en ligne dans un but lucratif.

Selon les études publiées, la surveillance excessive des enfants que l'on réalise sans fixer des limites appropriées ou fournir des explications adéquates peut avoir un effet sur :

- **L'autonomie et le développement social**
  Privés de la liberté de faire des choix et de poser des jugements critiques et éthiques à partir de leur expérience, les enfants risquent de prendre des décisions fondées sur la peur et le risque d'encourir une punition. Ils pourraient devenir moins susceptibles d'apprendre à régir et à guider leurs propres comportements.

- **La confiance, la peur et la capacité d'évaluer les risques**
  La surveillance peut créer un cadre artificiel, dénué de risque, dans lequel les enfants n'auront peut-être pas la possibilité d'acquérir la confiance en eux et en leurs capacités de gérer le risque.

- **Les capacités numériques**
  Les logiciels de surveillance risquent d'empêcher le développement chez les enfants des compétences numériques nécessaires pour naviguer sur Internet de manière efficace.

- **La compréhension de la notion de vie privée**
  Si les enfants sont élevés dans un cadre de surveillance, dans lequel la vie privée n'est pas valorisée, il est possible qu'ils ne la valorisen pas à leur tour. En outre, ces enfants pourraient ne pas apprendre comment établir leurs propres limites en matière de respect de la vie privée et être moins susceptibles de respecter les limites d'autrui.

2.3 INITIATIVES DE SENSIBILISATION DES JEUNES

Nous avons lancé avec succès deux trousses de présentation pour les jeunes destinés à une utilisation auprès des élèves de la 7e et 8e année et de la 9e à la 12e année[1].

Notre objectif consiste à montrer aux jeunes les effets de la technologie sur leur vie privée et la façon dont ils peuvent établir en ligne des identités sûres tout en protégeant leurs renseignements personnels.

Ressources pour parents et enseignants

Chaque trousse contient un ensemble de diapositives dynamiques en PowerPoint accompagnées de notes pour l'animateur afin d'aider les enseignants ou d'autres adultes à donner des exposés efficaces et intéressants dans les écoles ou la communauté. Les exposés durent environ 30 minutes, mais il est recommandé de prévoir du temps supplémentaire pour une discussion en groupe.

Les présentateurs sont invités à faire des commentaires au Commissariat de sorte que nous puissions améliorer constamment les trousses.

Nous avons également mis au point une vidéo de quatre minutes et demie intitulée *Que pouvez-VOUS faire pour protéger votre réputation en ligne?*, qui s'adresse directement aux adolescents et

Que pouvez-VOUS faire pour protéger votre réputation en ligne? - vidéo

1 Secondaire I et II et secondaire III à V au Québec.

aborde les grands principes relatifs à la protection de la vie privée que les jeunes doivent prendre en considération lorsqu'ils communiquent des renseignements en ligne. La vidéo — lancée en janvier 2012 — peut être regardée en ligne ou téléchargée pour alimenter une discussion sur des questions relatives à la protection de la vie privée avec des adolescents.

Le Commissariat a aussi élaboré des conseils destinés aux parents qui veulent parler à leurs enfants de protection de la vie privée dans le monde en ligne. Les conseils exhortent les parents à « tester » l'espace en ligne que leurs enfants utilisent, à suivre l'évolution de la technologie, à souligner l'importance d'utiliser des mots de passe et à dire à leurs enfants de « penser avant de cliquer »

12 conseils pratiques en matière de protection de la vie privée à l'usage des parents

Notre troisième concours annuel national de vidéo Ma vie privée et moi a encore remporté un vif succès, avec plus de 100 vidéos reçues. Les gagnants provenaient de toutes les régions du Canada.

Les élèves de 12 à 18 ans peuvent participer au concours en produisant des messages d'intérêt public sur format vidéo de une à deux minutes portant sur des questions concernant la protection de la vie privée.

Renseignements sur le concours de vidéo

Un quatrième concours a été lancé en septembre, et les gagnants devraient être annoncés en mars 2012.

On peut trouver des précisions sur toutes ces initiatives sur notre site Web spécial destiné aux jeunes, www.viepriveedesjeunes.ca.

2.4 COMPÉTENCES NUMÉRIQUES

Les compétences numériques comprennent les capacités d'utiliser des ordinateurs et Internet, d'en comprendre le fonctionnement et de créer avec ces outils. Au contraire de l'Australie et du Royaume-Uni, le Canada n'a pas de stratégie nationale relative aux compétences numériques.

L'acquisition de compétences numériques faisait partie du processus de consultation du gouvernement fédéral en vue de l'élaboration d'une stratégie nationale sur l'économie numérique, en mai 2010, mais la question est restée sans suite.

Pour mieux comprendre la situation, le Commissariat a octroyé un contrat à l'organisme Réseau Éducation-Médias pour qu'il recense les principales initiatives menées dans le domaine des compétences numériques au Canada et à l'étranger évalue leurs volets se

rapportant à la protection de la vie privée, et relève les possibilités s'offrant au Commissariat de contribuer à sensibiliser davantage les Canadiennes et les Canadiens à la protection de la vie privée en ligne et de renforcer leurs compétences à cet égard dans le cadre des initiatives en cours.

Le Réseau a conclu que même si l'importance des compétences numériques est reconnue au Canada, la protection de la vie privée en ligne, en tant qu'aspect particulier de ces compétences, ne reçoit pas l'attention voulue, et que les efforts déployés à cet égard sont ralentis par l'absence de stratégie coordonnée.

Dans son rapport, le Réseau a comparé les programmes de compétences numériques canadiens à ceux qui sont offerts au Royaume-Uni, aux États-Unis, en Australie et au Brésil. L'organisme a relevé les tendances suivantes :

- Les jeunes représentent le principal groupe ciblé par les interventions d'acquisition de compétences numériques, y compris celles relatives à la protection de la vie privée. Même si les adultes sont aussi exposés aux risques d'atteintes à la vie privée, ils sont jugés comme étant moins prioritaires à cet égard.

- Les interventions en cours dans le domaine n'essaient pas d'anticiper les risques, mais tentent plutôt tant bien que mal de suivre les progrès technologiques.

- Hormis les groupes largement définis, comme les jeunes, les adultes et les personnes âgées, les programmes en vigueur ne s'attardent guère aux autres facteurs susceptibles d'avoir une incidence sur les capacités numériques, comme le statut d'immigrant ou le sexe.

- Malgré la possibilité d'offrir des programmes d'acquisition de compétences numériques en ligne, tous les pays étudiés préfèrent les cours en personne, particulièrement pour les personnes âgées.

Sur la foi de ses constatations, le Réseau a fait les recommandations suivantes :

- Définir les compétences en matière de protection de la vie privée que les Canadiennes et Canadiens doivent posséder afin de gérer leurs renseignements personnels en ligne. Les compétences en question vont de la sensibilisation au fait que les renseignements personnels sont de plus en plus traités comme un produit jusqu'à la connaissance du droit à la vie privée et des mécanismes de recours à cet égard.

- Promouvoir auprès des Canadiennes et Canadiens les compétences en matière de protection de la vie privée comme un droit.

- Intégrer les notions de protection des données et de démocratie dans les modules didactiques.

- Cibler davantage les adultes.

- Appuyer les programmes d'éducation permanente dans le domaine des compétences numériques pour tous les élèves des niveaux primaire et secondaire.
- Élaborer des ressources pédagogiques sur la protection de la vie privée pouvant être adaptées à de nombreux publics.
- Appuyer les sites du Programme d'accès communautaire à titre de véhicules de sensibilisation à la protection de la vie privée.
- Promouvoir et appuyer les ressources existantes de grande qualité.
- Favoriser des efforts nationaux axés sur la culture numérique.

2.5 PROJETS DU PROGRAMME DES CONTRIBUTIONS AYANT TRAIT AUX JEUNES CANADIENS

Au cours des dernières années, le Programme des contributions du Commissariat a financé des initiatives novatrices de recherche et de sensibilisation du public qui examinaient la relation entre les jeunes et la protection de la vie privée et moussaient la protection des renseignements personnels auprès des jeunes. Par exemple :

Le Réseau Éducation–Médias a reçu une aide financière en 2011-2012 pour son projet intitulé *Jeunes Canadiens dans un monde branché — phase III*. Il s'agit de l'étude la plus complète et la plus vaste sur l'utilisation d'Internet par les enfants et les jeunes au Canada. La phase III complète la phase de recherche qualitative déjà menée par le Réseau au moyen de groupes de discussion composés de parents et de jeunes à Calgary, à Toronto et à Montréal, et comprend la rédaction du rapport final de recherche qualitative ainsi que l'élaboration et la mise en œuvre d'une stratégie de communications.

Également en 2011-2012, Atmosphere Industries a reçu des fonds pour son projet intitulé *La protection de la vie privée et les jeux : Créer un jeu sur la protection de la vie privée avec des enfants Canadiens*. Dans le cadre du projet, des enfants seront mis à contribution pour la création, le déploiement et la recherche de jeux multimédias destinés aux enfants âgés de huit ans et plus en vue de l'acquisition de compétences en matière de protection de la vie privée. Les jeux multimédias mettent à profit les espaces physiques et numériques et les technologies pour créer des expériences uniques où les gens se retrouvent dans des espaces publics et collaborent pour résoudre des problèmes et atteindre des objectifs.

En 2009-2010, le Commissariat a financé un projet réalisé par l'Université de Guelph, intitulé *La protection de la vie privée sur Facebook : La communication des renseignements des jeunes et des adultes et la perception des risques d'atteinte à la vie privée*. L'initiative visait à faire avancer la compréhension de la communication de renseignements sur Facebook par les élèves du niveau secondaire et des adultes sur le marché du travail au moyen d'un examen de la documentation et d'un sondage réalisé auprès de 600 Canadiennes et Canadiens. La recherche portait sur les facteurs qui motivaient la communication de renseignements et l'utilisation des paramètres de confidentialité tout en examinant les impressions des utilisateurs de Facebook à l'égard des risques d'atteinte à la vie privée et la connaissance qu'ils ont des paramètres de confidentialité. Le rapport final comporte des recommandations visant à aider le Commissariat à élaborer des stratégies afin de sensibiliser le public aux risques pour la vie privée des sites de réseautage social et à la nécessité de prendre des décisions plus éclairées au sujet de l'échange d'information.

Le Commissariat espère que les résultats de ces études seront mis en œuvre et utilisés à bon escient par les utilisateurs finaux en vue du recensement des besoins en matière de protection de la vie privée des jeunes quand ceux-ci affrontent les défis modernes du monde numérique.

CHAPITRE 3

La protection de la vie privée

APERÇU DES AUTRES GRANDS ENJEUX ABORDÉS PAR LE COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA AU COURS DE L'ANNÉE

Au chapitre de la protection de la vie privée en 2011, nous avons vu des évolutions graduelles et des changements abrupts pareils au lent mouvement de la croûte terrestre ponctué de rares événements tectoniques.

Comme toujours, la structure fondée sur des principes de la LPRPDE s'est avérée suffisamment souple et solide pour aborder la grande majorité des défis en matière de protection de la vie privée. Pourtant, la *Loi* elle-même évolue, et d'autres changements à celle-ci pourraient s'avérer nécessaires afin d'englober les nouveaux défis en matière de protection de la vie privée qui, de par leur portée et leur nature, ne ressemblent en rien aux enjeux abordés au cours des dix années d'existence de la *Loi*.

Pendant l'année, la commissaire a indiqué que la perspective d'amendes considérables semblait nécessaire pour convaincre les entreprises de prendre au sérieux la prévention des atteintes à la sécurité des données. Elle a également diffusé une lettre ouverte dans laquelle elle demandait au gouvernement fédéral de justifier son texte de loi proposé sur « l'accès légal », qui aurait « de graves conséquences sur le droit à la vie privée ».

Les Canadiennes et Canadiens semblent reconnaître les défis qui pointent à l'horizon. Un sondage de l'opinion publique, commandé par le Commissariat, a révélé un nombre considérable de préoccupations nouvelles en matière de protection de la vie privée découlant des avancées technologiques en communication par rapport au sondage mené il y a seulement deux ans.

Sur les quelque 2 000 Canadiennes et Canadiens choisis au hasard pour répondre au sondage, quatre sur dix ont indiqué que les ordinateurs et Internet représentent des dangers pour leur vie privée, soit une augmentation de 25 % par rapport au sondage mené en 2009. Les craintes en matière de protection de la vie privée sont également en hausse en ce qui concerne les sites de réseautage social en ligne, les téléphones cellulaires et les services financiers en ligne.

Comme le montrent les résumés de certaines enquêtes présentées dans ce chapitre, les craintes en question sont souvent fondées.

Dans le domaine de la protection des renseignements financiers, par exemple, nous avons constaté qu'une compagnie d'assurance, une agence d'évaluation du crédit, un fabricant de voitures et une coopérative de crédit avaient contrevenu à la LPRPDE.

Nous avons également relevé de nouvelles préoccupations au sujet de Facebook, un géant du réseautage social dont nous avons déjà parlé dans des rapports précédents. De plus, nous continuons de surveiller la mise en œuvre par Google d'améliorations à la protection de la vie privée que nous avons recommandées lorsqu'il a été trouvé que l'entreprise avait recueilli des renseignements personnels de manière inappropriée.

Afin de suivre l'évolution rapide du domaine de la protection de la vie privée, le Commissariat a diffusé des documents d'orientation sur la biométrie et la publicité comportementale en ligne — deux sous-produits de la nouvelle technologie. Nous avons également renforcé notre expertise en matière de technologie, en partie pour appuyer le rôle que doit jouer le Commissariat dans la nouvelle loi canadienne antipourriel, qui doit entrer en vigueur cette année.

Il sera question de tous ces faits nouveaux dans les pages qui suivent, qui portent sur certains des grands enjeux que nous avons examinés en 2011.

3.1 PROTECTION DES RENSEIGNEMENTS FINANCIERS

La plupart des gens protègent leurs données financières aussi jalousement que leur NIP au moment de passer à la caisse ou au guichet automatique. Leur pire cauchemar serait d'apprendre qu'un escroc se balade avec leur carte de crédit.

À cause de cette sensibilité et de la quantité énorme de transactions réalisées avec des Canadiennes et Canadiens, le secteur financier est visé régulièrement par la proportion la plus élevée de plaintes officielles acceptées par le Commissariat. En 2012, il a également été l'objet de plusieurs enquêtes dignes de mention, qui sont résumées ci-après.

ENQUÊTES

UNE AGENCE D'ÉVALUATION DU CRÉDIT SUPPRIME DES ANTÉCÉDENTS EN MATIÈRE D'EMPRUNT DU RAPPORT DE SOLVABILITÉ D'UNE PERSONNE À SON INSU

CONTEXTE

Un particulier a financé l'achat d'un véhicule automobile usagé en faisant appel à une entreprise de financement tierce. Pour payer son véhicule, le

plaignant voulait traiter avec un prêteur relevant d'une agence nationale d'évaluation du crédit. Il y tenait parce qu'il était convaincu que des antécédents favorables de remboursement pourraient contribuer à améliorer sa cote de crédit générale.

Le plaignant a commencé à rembourser son prêt automobile en juillet 2004. Dès juin 2008, il avait remboursé la somme intégralement.

En 2008, à la suite du remboursement de son prêt automobile, le plaignant a voulu se prévaloir d'un programme provincial offrant des subventions aux demandeurs admissibles en vue de l'achat d'une propriété. Le plaignant semblait avoir obtenu une préapprobation auprès d'un courtier en hypothèques, sous réserve de son admissibilité à la subvention.

Selon le plaignant, après avoir reçu un avis confirmant qu'il était admissible à la subvention, il a communiqué avec le courtier en hypothèques ayant émis la préapprobation conditionnelle, qui lui a dit qu'il n'aurait plus droit au prêt.

Bien qu'il soit difficile d'établir avec certitude les raisons sous tendant le refus du prêt au plaignant — les prêteurs et institutions financières ont le droit d'appliquer leurs propres critères pour l'approbation de crédit —, le courtier en hypothèques a fait savoir au Commissariat que les données relatives au prêt automobile remboursé par le plaignant ne figuraient pas dans le dossier de crédit de celui-ci.

Le courtier en hypothèques a dit estimer que l'absence des données relatives au prêt automobile pourrait avoir nui à la cote de crédit du plaignant. Il estimait aussi que l'emprunt contracté par le plaignant auprès de la société de financement, avec son historique de remboursement positif, pourrait avoir contribué en partie à rétablir la cote de crédit du plaignant. Il croyait comprendre que la cote de crédit du plaignant avait diminué considérablement entre le moment où celui-ci avait obtenu la préapprobation hypothécaire jusqu'à celui où le plaignant a été jugé admissible à la subvention.

NOS CONSTATATIONS

Même si nous n'avons pas pu établir la mesure dans laquelle la cote de crédit du plaignant a pu souffrir de l'absence d'information sur le prêt automobile, notre enquête a corroboré le fait que les données relatives au prêt automobile contracté auprès de la société de financement, qui ont déjà figuré dans le rapport de solvabilité du plaignant, ont par la suite disparu.

L'enquête a révélé que la société de financement transmettait tous les mois des données sur le remboursement de l'emprunt du plaignant à une agence d'évaluation du crédit. Cependant, quelque temps avant que le plaignant acquitte intégralement son emprunt, la compagnie de finance a cessé de transmettre les données à l'agence.

L'agence d'évaluation du crédit a indiqué qu'elle avait pour politique de cesser de déclarer toute information d'une source de données avec laquelle elle n'a pas de lien permanent (c.-à-d., « une source de données aseptisée ») quelque 60 jours après la rupture du lien avec la source des données. Cette politique a pour effet de supprimer tous les renseignements associés

à une source de données aseptisée — positifs comme négatifs —, effaçant toute trace des antécédents de crédit dans le dossier du particulier. L'agence d'évaluation du crédit soutient que cette façon de faire est nécessaire pour que l'information contenue dans les rapports de solvabilité soit exacte, complète et à jour.

Notre enquête a porté essentiellement sur les obligations de l'agence d'évaluation du crédit quant à l'exactitude et à l'exhaustivité du dossier de crédit du plaignant. Nous avons examiné aussi des préoccupations se rapportant à la transparence. À cette fin, nous avons regardé attentivement les politiques et pratiques de l'agence d'évaluation du crédit concernant les sources de données aseptisées, à la lumière des obligations de l'entreprise en vertu des dispositions provinciales sur les renseignements relatifs au crédit et la protection du consommateur.

Malgré nos réticences initiales à l'égard de la suppression des antécédents de crédit du plaignant, pendant notre enquête, l'agence d'évaluation du crédit a fourni suffisamment d'éléments de preuve montrant la façon dont les renseignements obtenus d'une source de données aseptisée pourraient compromettre l'intégrité des rapports de solvabilité. Même si, dans le cas qui nous occupe, la suppression des renseignements relatifs à un emprunt du rapport de solvabilité du plaignant a fait en sorte que le dossier de crédit de celui-ci est devenu incomplet, nous pouvons imaginer autant d'autres cas dans lesquels le fait de ne pas supprimer l'information obtenue d'une source de données aseptisée aurait pu donner un rapport de solvabilité tout aussi inexact ou incomplet. À cause de la rupture du lien avec la source de données, l'agence d'évaluation du crédit ne pouvait pas garantir que l'information figurant dans les rapports de solvabilité était récente, fiable et à jour. L'agence d'évaluation du crédit n'aurait pas été en mesure de déclarer les modifications apportées au rapport de solvabilité d'un particulier ni même de vérifier les inexactitudes dans les données et mener enquête à ce sujet.

En dépit de tout ce qui précède, nous continuons de déplorer que les renseignements relatifs au crédit aient été entièrement supprimés du dossier de crédit du plaignant, à son insu. Dans le cas en l'espèce, le plaignant ignorait totalement que ses renseignements personnels seraient supprimés, et les tiers susceptibles de se fier aux rapports de l'entreprise pour accorder des prêts semblaient n'avoir aucune idée de ses politiques et pratiques.

Au moment de notre enquête, l'agence d'évaluation du crédit ne publiait pas sa politique consistant à conserver pendant 60 jours les renseignements obtenus de sources de données aseptisées. La politique de conservation des données était ainsi libellée : « Une opération de crédit sera automatiquement supprimée du système six (6) ans à compter de la date de la dernière activité. »

Si le plaignant avait été au courant de la politique de l'agence d'évaluation du crédit, il aurait été mieux à même de surveiller son dossier et d'envisager de faire ajouter un commentaire à son rapport de solvabilité. Il aurait également pu envisager de prendre des dispositions afin d'obtenir l'information directement

de la source de données aseptisée de manière à compléter son dossier de crédit.

CONCLUSION
Étant donné que la LPRPDE prévoit qu'une organisation doit faire connaître ses politiques et pratiques concernant la gestion des renseignements personnels, et dans la mesure où l'agence d'évaluation du crédit n'a pas fait montre de transparence auprès du plaignant au sujet de sa politique sur les sources de données aseptisées, nous avons jugé que la plainte était fondée. L'agence d'évaluation du crédit a accepté de mettre en œuvre les recommandations du Commissariat pour régler le problème.

La banque a eu raison de raturer l'information relative à l'enquête sur une fraude par carte de crédit

La plaignante alléguait qu'une banque lui aurait refusé l'accès à ses renseignements personnels dans le cadre d'une enquête relative à des allégations d'utilisation frauduleuse de sa carte de crédit.

La banque mise en cause avait fait savoir à la plaignante que sa carte de crédit serait annulée à cause d'une utilisation potentiellement frauduleuse de sa carte. Après plus de six mois d'échanges avec les services à la clientèle et le bureau de l'ombudsman de la banque, la plaignante a présenté une demande d'accès à l'information au responsable de la protection de la vie privée de la banque, dans laquelle elle demandait tous les documents se rapportant à l'utilisation frauduleuse de sa carte de crédit et à son annulation subséquente. Elle avait expressément demandé le nom du commerçant où aurait eu lieu la fraude alléguée.

La banque a fourni cinq pages de documents relatifs au compte de carte de crédit, mais avait raturé les noms de personnes et de certaines des commandes informatiques utilisées par la banque. Estimant qu'il manquait de l'information, la plaignante a déposé une plainte d'accès à l'information en vertu de la LPRPDE contre la banque.

Le Commissariat a jugé que la banque avait à bon escient raturé les renseignements personnels d'autres personnes, les commandes du système informatique utilisées pendant l'enquête et les renseignements produits par l'enquête à l'égard de la fraude alléguée.

Nous avons également conclu que l'information raturée pouvait être décrite comme des renseignements commerciaux confidentiels. Nous convenons que, si les renseignements raturés étaient communiqués, les intérêts commerciaux de la mise en cause seraient irrémédiablement compromis. La communication constituerait une contravention aux obligations contractuelles de la mise en cause en matière de confidentialité et, de plus, pourrait faire courir des risques aux commerçants avec lesquels la banque a des obligations contractuelles en matière de confidentialité.

Le Commissariat a conclu que la plainte n'était pas fondée.

Une coopérative d'épargne et de crédit aurait dû obtenir le consentement avant de mener une vérification de la solvabilité de la conjointe

Un homme s'est plaint qu'une coopérative d'épargne et de crédit aurait recueilli ses renseignements personnels dans le cadre de ce qu'il considère comme un processus de demande de crédit trompeur. Il a également allégué que ses renseignements personnels auraient été conservés sans son consentement et que la coopérative aurait refusé de détruire l'information. Enfin, il a déploré que l'organisation avait mené une vérification de la solvabilité de sa conjointe sans son consentement et avait utilisé et communiqué les renseignements ainsi obtenus de manière inadéquate.

Le Commissariat a conclu que la mise en cause avait expliqué clairement au plaignant le type de renseignements personnels nécessaires dans le cadre du processus de demande. Nous avons également pris en considération l'obligation juridique mentionnée par la coopérative concernant la conservation des renseignements personnels du plaignant.

Cependant, l'enquête a soulevé des préoccupations concernant la collecte de renseignements sur la conjointe du plaignant. Même si le nom de la conjointe figurait sur le formulaire de demande, celle-ci n'avait pas consenti à la vérification de la solvabilité.

Le Commissariat a recommandé que la coopérative revoie ses procédures de manière à obtenir le consentement de chaque client qui demande un prêt avant d'obtenir un rapport conjoint auprès de l'agence d'évaluation du crédit. La coopérative a confirmé qu'elle avait renforcé son manuel de procédures de manière à ce que l'obtention du consentement des deux consommateurs devienne une condition obligatoire avant l'obtention d'un rapport conjoint auprès de l'agence d'évaluation du crédit.

Le Commissariat a conclu que les plaintes se rapportant à la collecte et au consentement en ce qui concerne les renseignements personnels du plaignant n'étaient pas fondées.

Au sujet de la question de la conservation des renseignements, nous sommes convaincus que l'obligation juridique invoquée par la coopérative pour la conservation des renseignements personnels du plaignant pendant une période de sept ans était raisonnable. Pour cette raison, nous avons conclu que la plainte n'était pas fondée.

Les plaintes se rapportant au consentement à la collecte des renseignements personnels de la conjointe et à l'utilisation et à la communication de ces renseignements étaient fondées et ont été résolues.

GROUPE DE TRAVAIL SUR L'EXAMEN DU SYSTÈME DE PAIEMENT

Le système moderne de paiement va des achats en espèces au dépanneur jusqu'aux virements de millions de dollars entre entreprises. Il englobe la totalité des institutions, des instruments et des services qui appuient le transfert des fonds entre les parties à une

transaction, ce qui comprend l'argent, les instruments financiers, voire l'échange de renseignements.

Ce secteur connaît des changements importants en raison des avancées technologiques de l'économie numérique qui ont facilité l'émergence d'un marché en ligne dans lequel les paiements revêtent des formes nouvelles et novatrices.

En juin 2010, le ministre des Finances a annoncé la création du Groupe de travail sur l'examen du système de paiement. À l'été 2011, le Groupe de travail a sollicité des mémoires se rapportant à la transformation du système canadien de paiement. Le Commissariat a présenté un mémoire sur les préoccupations relatives à la protection de la vie privée et à la sécurité que nous estimions importantes pour le Groupe de travail, les acteurs du système de paiement et les particuliers.

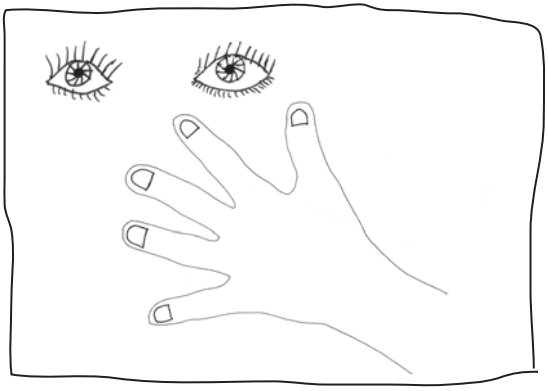
Étant donné que les paiements concernent souvent des renseignements très délicats comme les données sur les finances personnelles, le mémoire du Commissariat faisait ressortir l'importance pour l'industrie des paiements d'être consciente des difficultés associées à la définition des renseignements personnels à l'ère numérique, des défis associés aux nouvelles technologies ainsi que du risque de repersonnalisation des données. Nous avons lancé un appel en faveur du déploiement d'efforts proactifs pour la mise en œuvre des mesures les plus solides de protection de la vie privée à toutes les étapes du processus du système de paiement.

Nous sommes heureux que le Groupe de travail a reconnu la protection de la vie privée en tant que principe directeur associé à la transformation du système de paiement et a inclus la protection de la vie privée dans son cadre de gouvernance. Pour cette raison, nous avons recommandé que toutes les mentions relatives à la protection de la vie privée dans le système de paiement reconnaissent ce principe, et que le système soit conçu de manière à respecter les obligations relatives à la protection de la vie privée prévues dans les dispositions législatives.

Le Commissariat est conscient que les innovations qui marquent le système de paiement contribuent à favoriser la croissance économique. De nouvelles pratiques et technologies commerciales dynamiques sont instaurées afin de rendre plus conviviales les transactions commerciales et financières. Pourtant, ces innovations permettent la collecte, l'utilisation et la communication de plus en plus fréquentes d'énormes quantités de renseignements personnels sur les consommateurs au point de paiement, d'où la nécessité d'aborder en profondeur les préoccupations relatives à la protection de la vie privée et à la sécurité.

Pour appuyer l'innovation et construire une économie numérique solide, les consommateurs doivent adopter les nouvelles pratiques et technologies. Pour cela, les consommateurs doivent faire confiance au système. Le respect des obligations relatives aux droits à l'information et à la vie privée contribue à édifier la confiance nécessaire et, de ce fait, encourage la participation à la vie économique.

3.2 BIOMÉTRIE



Une nouvelle préoccupation se pointe dans le domaine de la protection de la vie privée — la biométrie. Un mot que bien des gens n'avaient jamais entendu il y a cinq ans fait de plus en plus partie de notre quotidien, à mesure que les appareils balaient l'iris des yeux, les visages, le bout des doigts, la paume des mains et même la démarche pour confirmer ou authentifier l'identité d'une personne.

Cette nouvelle technologie apporte de nouvelles préoccupations en matière de protection de la vie privée, préoccupations qui ont incité le Commissariat à produire cette année un document d'orientation à ce sujet. De plus, l'enquête dont il est question ci-après montre la façon dont la biométrie et la protection de la vie privée peuvent s'affronter dans la réalité.

ENQUÊTE

Une candidate à un examen s'oppose au balayage de la paume de la main

CONTEXTE

Une femme s'est opposée à ce qu'un appareil balaie la paume de sa main avant un examen en 2009 et à ce que l'information soit communiquée à une organisation américaine.

L'examen appartient à une organisation américaine, qui en assure l'administration. Les renseignements personnels sont recueillis et utilisés au Canada aux fins de l'examen par les employés canadiens d'un centre d'examen canadien, où plus de 8 000 examens ont été donnés en 2008.

L'administrateur de l'examen authentifie les candidats au moyen du balayage de la paume de la main, technologie qui trace le réseau veineux sous la peau de la main d'une personne et le conserve sous forme de gabarit crypté numérique (binaire) (une « clé numérique »). L'administrateur utilise cette technologie pour détecter la fraude et l'usurpation d'identité pendant les examens.

Le processus n'est pas réversible. Aucune donnée biométrique n'est conservée dans un fichier déchiffrable. Il est extrêmement difficile de forger une identité fondée sur le réseau veineux parce que les veines sont à l'intérieur du corps et comportent de

nombreuses caractéristiques détectables et différentes. L'administrateur de l'examen a soutenu qu'une simple identification visuelle et vérification par document d'identité n'est pas entièrement fiable étant donné que les fraudeurs prendront tous les moyens pour ressembler physiquement à une personne et usurper son identité.

Chaque fois que les candidats à l'examen sortent de la salle d'examen ou y reviennent, le gabarit du réseau veineux sert à vérifier leur identité. De plus, ce gabarit est comparé à tous les autres recueillis par l'administrateur de l'examen en d'autres lieux ou lors d'examens antérieurs même si c'était sous un nom différent.

NOS CONSTATATIONS

Le Commissariat a déterminé qu'une personne raisonnable trouverait justifié que l'administrateur de l'examen utilise le balayage du réseau veineux pour identifier les candidats et assurer l'intégrité de l'examen. Nous avons également jugé acceptable que l'administrateur de l'examen recueille et utilise des photos numériques avec le gabarit du réseau veineux étant donné que, dans quelques cas relevés par le passé, la photo avait protégé des candidats des répercussions d'une correspondance erronée du balayage de leur réseau veineux.

L'administrateur de l'examen a donné deux grandes raisons pour la collecte des renseignements personnels des candidats, y compris les données biométriques : 1) pour vérifier l'identité des candidats à l'examen; 2) pour faire en sorte que les résultats envoyés aux écoles reflètent exactement les capacités des étudiants.

Nous avons tiré nos conclusions après avoir examiné trois facteurs : le risque de fraude, la mesure dans laquelle la technologie utilisée par l'administrateur de l'examen pour le balayage du réseau veineux respecte la vie privée, et les normes de sécurité applicables à la conservation et à l'utilisation des gabarits.

FRAUDE

L'administrateur de l'examen a fourni des preuves de tentatives de fraude et d'activités illégales lors de séances d'examen.

Il a fait état de spécialistes rémunérés pour passer l'examen pour quelqu'un d'autre et signalé que, en 2003-2004, cinq individus de Montréal et de New York avaient fait l'examen pour 185 personnes aux États-Unis. Les fraudeurs ont été traduits en justice et condamnés et ont purgé une peine de prison dans un établissement pénitentiaire fédéral aux États-Unis. L'une des personnes condamnées a déclaré avoir fait l'examen plus de 300 fois. Pour cette raison, un grand nombre des écoles qui utilisaient l'examen dans le cadre de leur processus d'admission (c'est le cas de 57 écoles au Canada) ont demandé à l'administrateur d'adopter une approche beaucoup plus rigoureuse à l'égard de la sécurité de l'examen.

L'administrateur de l'examen a affirmé que la technologie biométrique est efficace en tant que moyen de dissuasion. Par exemple, après l'instauration du programme de biométrie, l'entreprise a constaté une diminution considérable des tentatives

de fraude. Et dans deux cas, deux personnes ont quitté précipitamment le centre d'examen — avant le balayage du réseau veineux de la paume de leur main — quand on leur a demandé d'expliquer le manque de concordance des photos et des signatures recueillies pour le même nom lors d'une séance d'examen précédente.

Pour ce qui est de la prévention de l'usurpation d'identité, l'administrateur de l'examen a indiqué que les premières expériences de l'entreprise avec la technologie de balayage de la paume de la main ont permis de dépister un individu qui avait fait l'examen cinq fois sous cinq identités différentes. La technologie a également permis de repérer 23 personnes qui avaient recruté le même imposteur pour qu'il fasse l'examen pour elles. Dans les deux cas, les imposteurs avaient utilisé de fausses pièces d'identité gouvernementales.

Un professionnel de l'examen du Canada a essayé de s'inscrire au centre d'examen en 2009 pour faire l'examen pour une quatrième fois, mais a été pris sur le fait parce que l'empreinte de la paume de sa main ne correspondait pas à celle enregistrée lors de la séance précédente. Cette personne n'a jamais plus contacté l'administrateur de l'examen.

PROTECTION DE LA VIE PRIVÉE

À la lumière des expériences récentes de l'administrateur de l'examen avec les méthodes de vérification de l'identité et des diverses solutions de rechange adoptées au fil des ans, le balayage du réseau veineux de la paume de la main ne semble pas trop porter atteinte à la vie privée. L'administrateur de l'examen a commencé à chercher une solution de rechange à la dactyloscopie (empreintes digitales numérisées) en 2006, après que les étudiants, les organisations de protection des données et des employés des centres d'examen ont exprimé des réserves à l'égard de la prise des empreintes digitales.

Le Commissariat estime que toutes les mesures biométriques portent plus ou moins atteinte à la vie privée étant donné qu'elles supposent la collecte des caractéristiques physiques d'une personne. Cependant, ce ne sont pas tous les usages de la biométrie qui portent gravement atteinte à la vie privée. Nous estimons que la représentation binaire du balayage du réseau veineux de la paume de la main d'un candidat, à la lumière de l'utilisation que fait de la technologie l'administrateur de l'examen, n'est pas un renseignement personnel très sensible.

Par exemple, nous constatons que les balayages de la paume de la main sont immédiatement transformés en un gabarit binaire chiffré, que le code binaire est irréversible et qu'aucune image biométrique brute n'est conservée. De plus, l'information relative au code binaire conservée à partir du balayage ne peut pas être interprétée facilement par d'autres parties ni utilisée à d'autres fins, et le gabarit est conservé séparément de tous les autres renseignements personnels relatifs au candidat. Le balayage de la paume est également considéré comme une méthode biométrique qui ne laisse pas de trace, étant donné qu'il est impossible de laisser des images latentes sur des objets, y compris le système servant au balayage.

NORMES DE SÉCURITÉ APPLICABLES AU STOCKAGE DES DONNÉES ET CONSERVATION

En ce qui concerne la communication, la conservation et le stockage des renseignements personnels, nous n'avons pas conclu que l'administrateur de l'examen contrevenait à ses obligations en vertu de la *Loi*.

Après avoir visité un centre d'examen, nous avons conclu que les données relatives à la biométrie, à l'identité et aux examens sont chiffrées en vue de la communication et du stockage et que l'accès aux données est limité. L'algorithme de chiffrement qu'utilise le sous-traitant de l'administrateur de l'examen correspond à une norme reconnue en matière de chiffrement assortie de bons niveaux de sécurité pour les données sensibles. De plus, les données sont protégées par de nombreuses mesures de protection de haut niveau au centre d'entreposage des données. Les politiques relatives à la sécurité sont documentées, et des accords écrits, entre l'administrateur de l'examen et son sous-traitant, régissent les procédures de protection des données. Par conséquent, l'obligation de responsabilité prévue au principe 4.1.3 de la LPRPDE est respectée.

La plaignante s'est aussi inquiétée que ses renseignements personnels soient transmis, conservés et entreposés aux États-Unis. À cet égard, nous avons constaté que dans son bulletin d'information, l'administrateur de l'examen indique clairement que les renseignements personnels seront transmis aux États-Unis. Nous concluons donc que les mesures prises par l'administrateur de l'examen répondent au principe 4.8 (« transparence ») de la LPRPDE.

En 2009, le Commissariat a diffusé ses *Lignes directrices sur le traitement transfrontalier des données personnelles*, lesquelles énonçaient des conclusions clés découlant d'enquêtes menées au fil des ans. Par exemple : « La LPRPDE n'interdit pas aux organisations du Canada de transférer des renseignements personnels à une organisation dans un pays étranger aux fins de traitement. »

Nous avons également estimé raisonnable la période de cinq ans établie par l'administrateur de l'examen pour la conservation des données biométriques et les résultats d'examen et constaté l'existence d'un processus automatisé et ponctuel de nettoyage des données à l'issue de la période de cinq ans. Par conséquent, la nécessité de limiter l'utilisation, la communication et la conservation décrite au principe 4.5 de la LPRPDE est respectée.

CONSENTEMENT

Lorsque nous avons retracé les étapes nécessaires à l'inscription à l'examen, nous avons constaté que les candidats étaient suffisamment informés en ce qui concerne la collecte de leurs renseignements personnels et les fins de la collecte.

Quatre vingt quinze pour cent des inscriptions à l'examen sont faites en ligne, ce qui suppose que les candidats cochent une case indiquant qu'ils acceptent les conditions énoncées et la politique de confidentialité (des liens à celles-ci sont bien fournis). Sur le site, les candidats sont invités à lire le bulletin d'information de l'administrateur de l'examen, document essentiel en ligne (que l'on peut aussi obtenir par la poste) qui expose les conditions en

matière d'identification que le candidat doit remplir le jour de l'examen et leurs raisons d'être.

Le bulletin fait état des politiques et méthodes applicables à l'examen et de la politique de confidentialité, qui contient des précisions. Il renseigne les candidats sur les types de renseignements personnels qui seront réunis, conservés et transmis aux États-Unis, sur le chiffrement des données et sur les utilisations prévues des renseignements par l'administrateur de l'examen. Il prévient également les candidats que, le jour de l'examen et au moment de la signature du document sur les règles et du contrat, ils consentiront à ce que le réseau veineux de la paume de leur main soit balayé afin de prévenir la fraude. De plus, sur son site Web, l'administrateur de l'examen affiche d'autres renseignements détaillés au sujet de l'utilisation de méthodes biométriques le jour de l'examen et fournit un lien vers une foire aux questions portant expressément sur la façon dont il utilisera la technique de reconnaissance du réseau veineux. Le site Web souligne clairement que le balayage de la paume de la main par l'administrateur de l'examen est une condition essentielle pour tous les candidats.

CONCLUSION

Le Commissariat a conclu que la plainte n'était pas fondée.

Remarque : On peut lire au chapitre 6 (Devant les tribunaux) le compte rendu d'une autre affaire concernant l'utilisation de la biométrie.

DOCUMENT D'ORIENTATION SUR LA BIOMÉTRIE

Votre visage, le bout de vos doigts, l'iris de vos yeux, votre démarche : toutes ces « caractéristiques biométriques » peuvent être utilisées par des machines de différentes façons pour reconnaître automatiquement les personnes et confirmer ou vérifier leur identité.

Comme les organisations et entreprises s'intéressent de plus en plus aux systèmes biométriques, le Commissariat a établi des orientations détaillées qui expliquent le fonctionnement des technologies et leurs répercussions sur la protection de la vie privée.

Le document d'orientation, intitulé *Des données au bout des doigts — La biométrie et les défis qu'elle pose à la protection de la vie privée*, explore les avantages et les inconvénients de la biométrie. D'une part, la technologie peut contribuer à l'édification de systèmes d'identification très fiables et solides — plus fiables, par exemple, que les systèmes fondés sur le papier. D'autre part, elle peut également poser des défis considérables en matière de protection de la vie privée, comme :

- la collecte et l'utilisation secrètes de données biométriques, notamment avec les nouveaux systèmes de balayage de l'iris qui peuvent saisir subrepticement des images des yeux jusqu'à deux

mètres de distance et des empreintes digitales à l'aide des empreintes laissées lorsqu'on touche des surfaces dures;

- les comparaisons, lorsqu'un trait biométrique recueilli à une fin donnée est utilisé à une autre fin à l'insu d'une personne et sans son consentement;

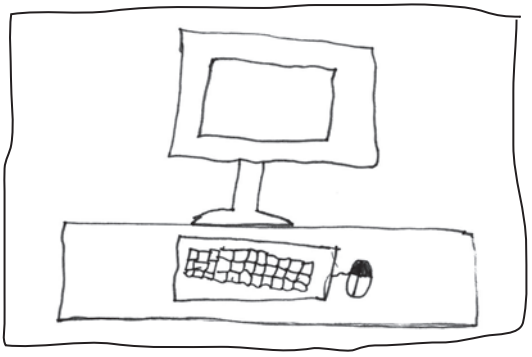
- la communication inopportune de renseignements secondaires compris dans l'ADN ou d'autres caractéristiques biométriques au sujet d'une personne.

À l'heure actuelle, le Canada n'a pas de politique régissant l'utilisation de la biométrie dans le secteur public ou privé. Cependant, le document du Commissariat souligne qu'un bon nombre des méthodes déjà en vigueur pour renforcer les mesures de protection de la vie privée dans d'autres domaines devraient aussi s'appliquer aux initiatives dans le domaine de la biométrie.

Cela comprend la prise en compte de la protection de la vie privée d'entrée de jeu et la conduite d'une évaluation des facteurs relatifs à la vie privée. De plus, le Commissariat encourage les organisations à appliquer un critère en quatre parties bien établi qui est énoncé en détail dans le document d'orientation.

Ces considérations sont désormais prises en compte dans l'évaluation de cas particuliers concernant l'utilisation de systèmes biométriques dans le secteur privé.

3.3 PROTECTION DE LA VIE PRIVÉE EN LIGNE



Les Canadiennes et Canadiens sont les plus grands utilisateurs d'Internet sur la planète puisqu'ils passent en moyenne quelque 45 heures en ligne par mois.

Nous sommes également parmi les plus grands amateurs de réseautage en ligne au monde. Environ un Canadien sur deux est sur Facebook.

Il n'est donc pas étonnant, à la lumière de ces statistiques, que la protection de la vie privée représente une préoccupation permanente pour le grand public canadien et le Commissariat. Cette année, nous avons publié des fiches d'information portant sur les conséquences, pour la protection de la vie privée, de l'infonuagique, des témoins et de la publicité comportementale en ligne. Nous avons également fait enquête à l'égard de plaintes relatives

aux nouvelles fonctions lancées par Facebook, dont il est question plus en détail ci-après.

ENQUÊTES

Facebook applique des pratiques en matière de protection de la vie privée améliorées, mais pas encore idéales

En 2011, nous avons mené enquête à l'égard d'un certain nombre de plaintes relatives à la protection de la vie privée déposées contre Facebook. Même si les plaintes variaient aux plans de la gravité et de la portée, la plupart découlaient du lancement de nouvelles fonctions liées à sa plateforme de réseautage social. Deux de nos enquêtes les plus récentes à l'égard de l'entreprise portaient sur des plaintes concernant :

- une fonction de « suggestion d'amis », qui vise à encourager les non-utilisateurs à s'inscrire au site de réseautage social en leur envoyant une liste « d'amis » et des photos d'utilisateurs actuels;

- des extensions sociales, qui permettent aux utilisateurs d'obtenir un contenu personnalisé sur les sites de tiers.

Le Commissariat était satisfait des résultats obtenus à la suite des enquêtes à cet égard.

En général, Facebook semble accorder davantage d'attention à la protection de la vie privée que lorsque nous avons commencé à faire enquête à son sujet. Pourtant, l'entreprise pourrait mieux prévoir les répercussions sur la vie privée des nouvelles applications avant de les lancer.

Nonobstant les améliorations générales apportées aux pratiques de Facebook en matière de protection de la vie privée (et aux paramètres de confidentialité détaillés de sa plateforme), nous déplorons que l'entreprise n'a pas prévu les importantes préoccupations relatives à la protection de la vie privée qui ont fait suite au lancement de l'application de suggestion d'amis. À notre avis, les considérations relatives à la protection de la vie privée auraient dû être prises en compte à l'étape de la conception de l'application — et non pas ajoutées après coup, en réponse aux réactions négatives d'utilisateurs et d'autorités de protection des données.

SUGGESTION D'AMIS

Trois personnes ont porté plainte auprès du Commissariat après avoir reçu des courriels les invitant à s'inscrire au site de réseautage social. Les invitations comprenaient des « suggestions d'amis » — une liste d'utilisateurs qui, dans la majorité des cas, étaient des personnes que les plaignants connaissaient. Comme ils ignoraient comment l'entreprise avait pu produire les suggestions en question, les plaignants craignaient que Facebook ait, en contravention de la *Loi*, eu accès à leurs carnets d'adresses électroniques.

L'enquête n'a pas établi que l'entreprise avait accédé aux carnets d'adresses personnels des plaignants ni à ceux de leurs amis suggérés. Les « suggestions d'amis » ont plutôt été produites par un algorithme

complexe comparant des ensembles communs de données téléchargées par les utilisateurs.

Au moment où les plaintes ont été déposées, les invitations émanant du site de réseautage social ne comportaient guère d'information sur le fonctionnement de l'application de suggestion d'amis. Pendant notre enquête, cependant, l'entreprise a accepté d'apporter des changements. Particulièrement, elle a supprimé toutes les suggestions d'amis figurant dans les invitations initiales et n'a fourni de suggestions que dans les rappels subséquents, ce qui permettait aux non-utilisateurs d'en apprendre davantage sur le service ou de se désabonner des suggestions d'amis et de tout autre message émanant de l'entreprise.

EXTENSIONS SOCIALES

En ce qui concerne les extensions sociales, l'entreprise a lancé une application permettant à ses utilisateurs de voir le contenu extrait de leur profil d'utilisateur sur les sites Internet de tiers. Les boutons comme « J'aime » et « Recommandé » apparaissaient sur les sites Internet de tiers et permettaient aux utilisateurs des sites de suggérer et recommander du contenu à d'autres amis. Par exemple, un membre connecté qui visite un site Internet de nouvelles au moyen des extensions sociales de l'entreprise pourrait voir une liste des articles recommandés par ses amis.

Le plaignant, dans cette affaire, craignait l'échange d'information entre l'entreprise et les plus de deux millions de sites Web qui hébergent les extensions sociales de l'entreprise.

Même si l'enquête a permis de confirmer que l'entreprise ne communiquait pas de renseignements personnels aux sites Internet de tiers au moyen des extensions sociales, le fonctionnement de cette application représentait un mystère pour bien des Canadiennes et Canadiens. Nous avons eu encore l'impression que l'entreprise aurait pu mieux renseigner le public et ses utilisateurs sur le fonctionnement de cette nouvelle application et veiller à intégrer des mesures de protection de la vie privée suffisantes au moment de la conception des nouveaux produits.

VÉRIFICATION DE L'IDENTITÉ

Il s'agissait de déterminer si Facebook a recueilli plus de renseignements personnels auprès de la plaignante que cela n'était nécessaire à titre de condition de service. Il fallait aussi déterminer si l'entreprise avait fourni à la plaignante la possibilité de contester le respect de la LPRPDE auprès des responsables compétents.

La plaignante a créé un compte personnel sur le site de réseautage social en septembre 2010. Elle a allégué qu'elle a pu utiliser son compte pendant quelques jours, mais qu'elle a dû par la suite fournir un numéro de téléphone cellulaire pour confirmer son identité et pouvoir accéder à nouveau à son compte.

Étant donné qu'elle n'a pas de numéro de téléphone cellulaire, la plaignante a indiqué qu'elle a été incapable de confirmer son identité.

La plaignante a également allégué que Facebook ne lui aurait pas permis de faire valoir une contestation

au sujet du respect des principes de la LPRPDE auprès des responsables du respect des politiques de l'entreprise. La plaignante a indiqué qu'elle a envoyé plusieurs courriels aux services à la clientèle et à d'autres services de l'entreprise concernant la vérification de son identité, mais qu'elle n'avait reçu que des messages automatiques de l'entreprise la dirigeant vers le bouton Aide.

Facebook a fait savoir au Commissariat qu'elle utilisait les numéros de téléphone cellulaire dans le cadre du processus de vérification des comptes lorsqu'un compte était considéré comme à risque à cause d'activités douteuses émanant d'un réseau de zombies ou d'envoi de pourriels. L'entreprise a indiqué que le compte de la plaignante avait été désigné comme étant à risque.

L'entreprise a indiqué que la vérification de l'identité au moyen du numéro de téléphone cellulaire représentait l'un des nombreux moyens disponibles pour la vérification d'un compte. L'utilisateur peut aussi confirmer le nom de ses amis sur le site en identifiant ceux et celles figurant sur les photos publiées sur Facebook. Il peut également vérifier son compte en fournissant son nom au complet, sa date de naissance et son adresse électronique de connexion et en téléchargeant une carte d'identité gouvernementale en veillant à ce que son nom, sa date de naissance et la photographie soient clairement visibles. Facebook a signalé qu'elle encourage les utilisateurs à masquer les renseignements personnels superflus figurant sur la pièce d'identité gouvernementale. L'entreprise a déclaré qu'elle avait offert à la plaignante la possibilité d'utiliser une autre façon de vérifier son compte, sans toutefois préciser laquelle.

En ce qui concerne la plainte relative à la possibilité de porter plainte à l'égard du non respect des principes, Facebook a indiqué qu'elle offre divers formulaires de contact pour les questions et les commentaires relatifs à la protection de la vie privée. Par exemple, la politique de confidentialité de l'entreprise indique que les personnes peuvent présenter une plainte relative à la protection de la vie privée contre Facebook par l'intermédiaire du Programme de surveillance de TRUSTe pour la résolution des litiges.

Le Commissariat a conclu que Facebook avait clairement informé ses utilisateurs des fins de la collecte, c'est-à-dire que la collecte de renseignements personnels constitue une mesure de sécurité servant à faire en sorte que l'utilisateur est bien une personne réelle qui possède un compte. De plus, le Commissariat a conclu que l'entreprise offrait à ses utilisateurs des choix pour l'authentification, chaque option correspondant à un niveau différent d'atteinte à la vie privée. Dans ce contexte, le Commissariat n'a pas jugé que le fait de demander aux utilisateurs de télécharger des pièces d'identité gouvernementales à des fins d'authentification (en masquant les renseignements personnels autres que le nom, la date de naissance et la photographie) contrevenait à la LPRPDE.

En ce qui concerne la possibilité de porter plainte à l'égard du non respect des principes, le Commissariat a jugé que Facebook fournissait au début de sa politique de confidentialité un formulaire Web

permettant aux utilisateurs de porter plainte auprès de l'entreprise au sujet de la protection de la vie privée. Pour cette raison, le Commissariat a estimé que l'entreprise avait adopté des procédures de traitement des plaintes relatives à la protection de la vie privée accessibles et conviviales.

Le Commissariat a conclu que les allégations n'étaient pas fondées.

GOOGLE TENUE DE CORRIGER DES LACUNES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

En juin 2011, le Commissariat a annoncé les résultats du suivi réalisé à la suite d'une enquête menée à l'égard de la collecte, par Google Inc., de données très sensibles à partir de réseaux sans fil non protégés.

Nous avions indiqué que Google s'était engagée à mettre en œuvre des mesures correctives ayant pour effet de réduire le risque d'atteintes futures à la vie privée, mais que la commissaire Stoddart avait également pris la mesure sans précédent de demander que l'entreprise fasse l'objet d'une vérification indépendante de ses programmes de protection de la vie privée pendant l'année et en communique les résultats au Commissariat.

L'incident concernait la collecte inappropriée, par les voitures de Google Street View, de renseignements personnels comme les courriels, les noms d'utilisateur, les mots de passe, les numéros de téléphone et les adresses au cours des 13 mois consacrés à l'arpentage des rues dans tout le pays. Des milliers de Canadiennes et Canadiens ont pu être touchés par la pratique.

Dans un rapport préliminaire publié en octobre 2010, nous avions indiqué que Google avait informé le Commissariat que l'incident découlait d'une initiative prise par un ingénieur et de l'absence de mesures de contrôle à l'égard des processus pour assurer le respect de la vie privée.

Nous avons conclu que la collecte représentait une grave atteinte au droit à la vie privée des Canadiennes et Canadiens ainsi qu'une mesure illégale parce qu'elle contrevient aux principes fondamentaux de la LPRPDE qui prévoient que la collecte de renseignements personnels doit se faire avec le consentement et au su des personnes. Le détail de notre enquête a été publié dans notre rapport annuel de 2010 et est affiché sur le site Internet du Commissariat.

Google s'était notamment engagée à prendre les mesures correctives suivantes :

- augmenter substantiellement la formation sur la protection de la vie privée et la sécurité offerte à tous les employés;
- mettre en place un système permettant d'exercer un suivi sur tous les projets nécessitant la collecte, l'utilisation ou la mise en mémoire de renseignements personnels, et exiger des ingénieurs et des gestionnaires responsables de ces projets qu'ils rendent des comptes au sujet de la confidentialité;
- obliger tous les chefs de projets d'ingénierie à rédiger, à conserver, à présenter et à tenir à jour

pour chaque projet un document de définition de la confidentialité afin de s'assurer que les équipes techniques et les équipes de conseillers en produits évaluent les répercussions de leurs produits et services sur la vie privée, depuis leur conception jusqu'à leur lancement;

- créer une équipe de vérification interne qui procèdera à des contrôles périodiques pour s'assurer que les documents de définition de la confidentialité sélectionnés ont bien été préparés et qu'ils ont été révisés par les gestionnaires compétents;

- lancer un projet pilote d'examen dans le cadre duquel les membres de l'équipe technique en matière de confidentialité, de l'équipe de conseillers en produits et de l'équipe de conseillers en matière de confidentialité étudient les propositions associées à des données géodépendantes, ainsi que les programmes logiciels servant à la collecte des données.

Google a également commencé à supprimer les données qu'elle avait recueillies au Canada. Le processus s'est toutefois complexifié à cause des divers règlements et règles que l'entreprise doit respecter en vertu des lois canadiennes et américaines. L'entreprise a indiqué que, jusqu'au moment où les données pourront être supprimées, celles-ci seront en sécurité et ne seront pas utilisées.

Le Commissariat assurera le suivi auprès de Google en 2012 pour voir si nos recommandations ont été pleinement mises en œuvre.

Le Commissariat figurait parmi plusieurs autorités internationales de protection des données qui ont fait enquête au sujet du fiasco de la collecte de données au sujet de réseaux sans fil de Google. Ainsi, l'autorité de protection des données de la France a imposé une amende de 100 000 euros (plus de 140 000 $ CAN à l'époque) à Google.

LOI CANADIENNE ANTIPOURRIEL

Le Canada a désormais sa loi antipourriel, même si elle n'est pas encore en vigueur.

La loi antipourriel vise à empêcher les communications électroniques non désirées en régissant l'envoi de messages électroniques commerciaux, y compris les courriels et les messages textes. Sauf exceptions limitées, les expéditeurs de messages électroniques commerciaux devront obtenir le consentement du destinataire avant d'envoyer le message, inclure des renseignements permettant d'identifier l'expéditeur et fournir au destinataire un moyen de retirer son consentement.

La loi vise également à faire échec à d'autres pratiques nuisibles comme la collecte d'adresses électroniques et l'installation de logiciels malveillants sur les ordinateurs.

Lorsque la loi entrera en vigueur, le Commissariat assumera la responsabilité d'appliquer celle-ci, avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence.

Il incombera au CRTC de faire enquête au sujet de l'envoi de messages électroniques commerciaux non

désirés, de la modification non autorisée de données de transmission et de l'installation de logiciels sans le consentement de l'intéressé.

Le Bureau de la concurrence se penchera sur les fausses représentations et les pratiques de commercialisation trompeuses sur le marché électronique.

Nous concentrerons nos efforts sur la collecte non autorisée de renseignements personnels, notamment :

- la collecte d'adresses électroniques, y compris l'établissement de listes de courriels au moyen de programmes informatiques qui explorent Internet à la recherche d'adresses;

- la collecte de renseignements personnels par l'accès aux systèmes informatiques en contravention d'une loi du Parlement.

La nouvelle loi permet au Commissariat d'échanger de l'information et de collaborer avec le CRTC et le Bureau de la concurrence pour assurer l'application efficace des dispositions législatives. En 2011, nous avons travaillé étroitement avec ces deux organisations et avec Industrie Canada à préparer la mise en œuvre de la loi en produisant notamment des outils de communication destinés à sensibiliser le public et en élaborant des procédures de coopération.

La nouvelle loi devrait entrer en vigueur en 2012.

Rapport sur les consultations de 2010 sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique

CONSULTATIONS SUR LA PROTECTION DE LA VIE PRIVÉE DES CONSOMMATEURS

En mai 2011, le Commissariat a rendu public son *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*. Ces consultations visaient à orienter et à encadrer nos activités en matière d'établissement de politiques et de recherche sur les nouveaux enjeux. Dans la foulée de l'engagement à intervenir énoncé dans le Rapport, nous avons lancé de nouvelles initiatives en 2011 visant la promotion de l'acquisition de capacités en matière de protection de la vie privée pour l'ensemble des Canadiennes et Canadiens, les entreprises canadiennes et les responsables de l'élaboration de technologie au Canada.

Nous avons produit des fiches d'information sur les témoins, l'infonuagique et la publicité

Les témoins sous la loupe

Introduction à l'infonuagique

Lorsque le moindre de vos gestes est surveillé... Les annonceurs font un suivi de vos comportements en ligne

comportementale en ligne. Destinées essentiellement au grand public, ces fiches fournissent des renseignements d'ordre général. Nous avons aussi actualisé notre bulletin d'interprétation sur la définition des renseignements personnels.

En décembre 2011, nous avons publié un document d'orientation sur la publicité comportementale en ligne, technique qui consiste dans le suivi, par des tiers, des habitudes de navigation d'utilisateurs d'Internet afin d'axer la publicité sur les intérêts perçus de ceux-ci. Le document énonce la façon dont les entreprises qui relèvent les habitudes de navigation et celles qui tirent parti des résultats peuvent s'assurer que leurs pratiques sont justes, transparentes et conformes à la LPRPDE.

Les organisations de protection des données aux États-Unis et en Europe, les annonceurs et les milieux technologiques (créateurs de navigateurs) mènent un grand nombre d'activités et tiennent de nombreuses discussions sur les questions du consentement et de la transparence. Nous avons jugé opportun de faire connaître notre point de vue et d'offrir un cadre, reposant sur la LPRPDE, pour les pratiques en cause.

ORIENTATIONS SUR LA PUBLICITÉ COMPORTEMENTALE EN LIGNE

Dans nos *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, nous soutenons que les données associées à la publicité comportementale en ligne seront généralement considérées comme des renseignements personnels.

Nous estimons que les fins de la publicité comportementale en ligne sont raisonnables dans les circonstances, mais que celle-ci ne devrait pas être considérée comme une condition de service pour naviguer sur Internet. Nous soulignons que les internautes doivent avoir l'information voulue sur la pratique et fournir leur consentement. Le consentement peut être implicite si :

- les personnes sont avisées des objectifs de la pratique de façon claire et compréhensible — ces objectifs doivent être manifestes et ne peuvent être enfouis dans une politique de protection de la vie privée. Les organisations devraient être transparentes quant à leurs pratiques et se demander comment elles peuvent informer efficacement les utilisateurs de leurs pratiques en matière de publicité comportementale en ligne à l'aide d'une variété de solutions de communication, comme l'utilisation de bannières en ligne, de technologies multicouches et d'outils interactifs;

- les personnes sont informées de ces objectifs au plus tard au moment de la collecte et reçoivent de l'information sur les divers intervenants qui participent au processus de publicité comportementale en ligne;

- les personnes peuvent facilement renoncer à la pratique — idéalement au plus tard au moment où les renseignements sont recueillis;

- la renonciation est immédiate et durable;

- les renseignements recueillis et utilisés sont limités, dans la mesure du possible, aux renseignements non sensibles (éviter les renseignements sensibles comme les renseignements sur la condition médicale ou la santé);

- les renseignements recueillis et utilisés sont détruits dans les plus brefs délais ou anonymisés efficacement.

Nos lignes directrices relèvent aussi des pratiques que nous estimons problématiques.

Certains types de technologie ont récemment été utilisés pour la publicité comportementale en ligne (par exemple, les témoins dits « zombies ») que l'on ne peut pas supprimer ou empêcher de suivre la navigation sur Internet. Selon nos lignes directrices, si une personne ne peut refuser le suivi et le ciblage parce qu'il n'existe aucun moyen viable de contrôler la technologie utilisée, ou parce que le refus rendrait le service inutilisable, les organisations ne devraient alors pas faire appel à ce type de technologie à des fins de publicité comportementale en ligne.

Nos lignes directrices soulignent également que, étant donné la difficulté d'obtenir le consentement éclairé d'un enfant à des fins de pratiques de publicité comportementale en ligne, les organisations devraient éviter de suivre les enfants ou les sites Web destinés aux enfants.

SONDAGE SUR LA PROTECTION DE LA VIE PRIVÉE

Au cours des deux dernières années, les préoccupations des Canadiennes et Canadiens quant aux conséquences pour leur vie privée d'un éventail de technologies de communication ont monté en flèche, selon un sondage de l'opinion publique commandé par le Commissariat.

Pourtant, d'après le même sondage, un grand nombre de gens qui utilisent ces nouvelles technologies ne prennent même pas les mesures les plus rudimentaires pour protéger leur vie privée.

Une enquête téléphonique menée auprès de 2 000 adultes choisis au hasard a révélé que quatre personnes sur dix indiquent que les ordinateurs et Internet posent des risques pour leur vie privée, ce qui représente une augmentation par rapport au quart des répondants (26 %) dans un sondage similaire mené il y a deux ans.

Quinze pour cent des répondants ont expressément mentionné les sites de réseautage social en ligne — élément presque absent du paysage en 2009 (2 %). Les craintes liées aux téléphones cellulaires et aux autres technologies de télécommunication ont presque quadruplé (passant de 3 à 11 %) et les réticences à l'égard des cartes de crédit ou de débit et des services bancaires en ligne ont également augmenté.

À la fin de février et au début de mars, la firme Harris/Decima a constaté que les trois quarts (74 %) des répondants ont indiqué posséder au moins un appareil de communication mobile, comme un téléphone cellulaire, un téléphone intelligent ou une tablette.

Cependant, seulement quatre répondants sur dix utilisaient un mot de passe pour verrouiller leur appareil ou ont ajusté les paramètres de leur appareil afin de limiter la quantité de renseignements personnels pouvant être stockés sur celui-ci.

Le *Sondage sur les Canadiens et la protection de la vie privée, 2011* a également révélé que le tiers des Canadiennes et Canadiens utilisent les réseaux WiFi dans les lieux publics comme les cafés et les aéroports, où les communications en ligne ne sont pas toujours protégées par des méthodes de chiffrement. De ce nombre, un bon 85 % reconnaissent s'inquiéter quelque peu des risques possibles pour la sécurité de leurs renseignements personnels.

Sondage sur les Canadiens et la protection de la vie privée, 2011

Une très grande majorité de répondants favorisent des sanctions sévères contre les organisations qui omettent de protéger la vie privée des personnes. Plus de huit répondants sur dix veulent que soient adoptées des mesures comme divulguer le nom des organisations fautives, imposer des amendes ou intenter des poursuites contre celles-ci.

Si les jeunes Canadiens de 18 à 34 ans sont parmi les utilisateurs les plus enthousiastes des nouvelles technologies, le sondage a révélé qu'ils sont également les plus susceptibles d'utiliser les mécanismes offerts pour protéger leur vie privée, ce qui porte à croire que, même s'ils n'hésitent pas à adopter les nouvelles technologies, ils tiennent aussi à protéger leur vie privée et sont disposés à prendre des mesures pour ce faire.

On peut consulter le sondage en entier sur notre site Web à www.priv.gc.ca.

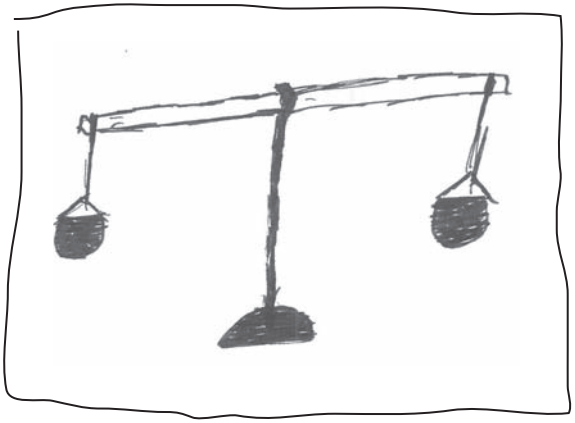
LABORATOIRE TECHNOLOGIQUE

La protection de la vie privée en ligne peut parfois exiger l'utilisation de la plus haute technologie, et c'est ici qu'entre en scène le laboratoire technologique du Commissariat. Le laboratoire permet au Commissariat de rester à l'affût des tendances technologiques et offre un soutien spécialisé dans les vérifications et les enquêtes dans lesquelles la technologie tient une place importante.

L'environnement contrôlé du laboratoire permet aux technologues de vérifier le type de renseignements personnels qui sont stockés sur un large éventail d'appareils ou d'applications et la façon dont ceux-ci sont protégés.

Par exemple, le laboratoire peut analyser les techniques de suivi utilisées en ligne par les annonceurs faisant appel à la publicité comportementale de même que l'efficacité des paramètres de confidentialité offerts sur les sites de réseautage social.

3.4 MODERNISATION DES LOIS SUR LA PROTECTION DE LA VIE PRIVÉE



MISE EN OEUVRE DES MODIFICATIONS À LA LPRPDE

En avril 2011, des modifications à la LPRPDE sont entrées en vigueur et accordaient à la commissaire des pouvoirs discrétionnaires élargis applicables à la conduite d'enquêtes et à l'échange de renseignements avec ses homologues provinciaux et internationaux.

La commissaire peut désormais refuser d'enquêter sur une plainte et abandonner des enquêtes, dans certaines circonstances particulières, comme lorsque la plainte pourrait être réglée de manière plus appropriée par d'autres recours en vertu d'autres lois ou lorsqu'elle n'a pas été déposée dans une période de temps raisonnable. Ces modifications contribueront à maximiser l'utilisation des ressources du Commissariat pour les plaintes qui soulèvent d'importantes préoccupations relatives à la protection de la vie privée ou les problèmes de nature systémique tout en apportant un équilibre entre la prestation de services à l'ensemble des Canadiennes et Canadiens et les préoccupations des plaignants.

En vertu de ces nouveaux pouvoirs discrétionnaires, en 2011, la commissaire a décidé d'abandonner l'instruction de deux plaintes et refusé d'en amorcer une troisième. Dans les trois cas, nous avons décidé que les litiges pouvaient être réglés de manière plus appropriée par d'autres moyens.

En ce qui concerne l'échange de renseignements, les modifications permettent à la commissaire de conclure des ententes avec ses homologues provinciaux et internationaux à cet égard, y compris pour des données jugées confidentielles en vertu de la LPRPDE, sous réserve de l'application de certaines mesures de protection.

À l'échelon provincial, le Commissariat œuvre depuis longtemps avec les commissaires à la protection de la vie privée des provinces afin d'assurer l'adoption d'une méthode harmonisée et concertée à l'égard de l'application des lois régissant la protection des renseignements personnels dans le secteur privé. Les capacités accrues en matière d'échange de renseignements permettront au Commissariat de travailler encore plus étroitement avec les commissaires provinciaux.

À cet égard, en novembre, nous avons conclu un nouveau protocole d'entente de coopération et de collaboration avec les commissaires de la Colombie-Britannique et de l'Alberta en ce qui concerne les

politiques relatives à la protection des renseignements personnels dans le secteur privé, l'application des lois et la sensibilisation du public. Dans le cadre de ces activités, nous examinons les plaintes instruites par nos homologues provinciaux afin de relever, s'il y a lieu, les préoccupations communes.

Sur la scène internationale, la capacité d'œuvrer de concert avec des homologues d'autres pays devient une nécessité étant donné l'augmentation de la circulation transfrontalière des données et des atteintes à la vie privée touchant de multiples administrations. Le Commissariat a amorcé des pourparlers au sujet d'accords d'échange d'information et de coopération avec plusieurs autorités de protection des données étrangères et était sur le point de s'entendre avec les Pays-Bas et l'Irlande à la fin de l'année.

RÉDUCTION DU RISQUE D'ATTEINTES À LA PROTECTION DES DONNÉES

À l'automne 2011, le gouvernement fédéral a déposé à nouveau des modifications à la loi rendant obligatoire la divulgation de certains types d'atteintes au Commissariat et aux personnes touchées.

En vertu du projet de loi C-12, les organisations devraient déclarer toute atteinte importante aux mesures de sécurité au Commissariat. Elles devraient évaluer s'il s'agit d'une atteinte « importante » en prenant en compte des facteurs comme la sensibilité des renseignements en cause, le nombre de personnes touchées et la nature systémique du problème.

Les organisations devraient également informer les personnes « s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à [leur] endroit », selon la sensibilité des renseignements et la probabilité que ceux-ci soient utilisés à mauvais escient.

Bien qu'un système obligatoire de déclaration nous donnerait une meilleure idée du nombre d'atteintes, des raisons pour lesquelles elles se produisent et des mesures à prendre pour réduire le risque d'autres incidents de ce genre, nous sommes d'avis que les dispositions contenues dans le projet de loi C-12 concernant la déclaration d'atteintes à la vie privée sont dépassées et requièrent une importante mise à jour.

Il convient de noter que les changements proposés au Parlement à la fin de 2011 découlent de recommandations datant de 2006 et restées sans suite.

Bien des choses ont changé au fil des ans. Les propositions relatives à la déclaration des atteintes à la protection des données contenues dans le projet de loi constituent un premier pas dans la bonne direction, quand il s'agit de favoriser la responsabilité et la transparence, mais il faudra clairement aller plus loin.

Nous avons été témoins ces dernières années de très graves atteintes à la protection des données d'une ampleur inégalée. Le signalement des atteintes, en soi, pourrait ne pas représenter un incitatif suffisant

pour que les organisations prennent davantage au sérieux les problèmes de sécurité dans le contexte actuel.

De nombreux pays adoptent une approche plus sévère à l'égard des atteintes. Par exemple, les États-Unis sont un chef de file dans le domaine, et pratiquement tous les États ont des dispositions législatives relatives aux atteintes à la protection des données. Entre-temps, un règlement proposé par la Commission européenne au début de 2012 prévoyait des dispositions relatives aux atteintes à la protection des données ainsi que l'octroi de vastes pouvoirs d'imposition d'amendes aux autorités européennes de protection des données.

La commissaire Stoddart encourage le gouvernement fédéral à explorer des mesures d'exécution de la loi plus strictes et davantage propres à encourager les organisations à bien protéger les renseignements personnels.

EXAMEN DE LA LPRPDE

La LPRPDE, qui se voulait axée sur des principes et neutre sur le plan technologique, a été promulguée en 2001 et doit être examinée par le Parlement tous les cinq ans.

Le premier examen a commencé en 2006. Le projet de loi C-12, qui propose des modifications à la LPRPDE découlant du premier examen, a été déposé à la Chambre des communes en septembre 2011. Il a remplacé le projet de loi C-29, qui est mort au Feuilleton à la suite de la dissolution du Parlement, le 26 mars 2011.

Le Parlement n'avait pas émis d'appel officiel pour un deuxième examen à la fin de 2011. Cela ne nous a pas empêchés de commencer à évaluer la façon dont le texte de loi et les pratiques en vigueur devraient évoluer pour mieux servir les Canadiennes et Canadiens face aux défis d'aujourd'hui en matière de protection de la vie privée.

Le prochain examen représentera une occasion d'évaluer si la LPRPDE reste suffisamment souple et efficace pour répondre aux défis relatifs à la protection de la vie privée découlant de l'évolution rapide de la technologie.

Notre position sur la question de savoir si la LPRPDE doit être modifiée et dans l'affirmative, de quelle façon, pour aborder ces nouveaux défis reposera sur notre réflexion à l'égard de trois thèmes clés : 1) des mécanismes d'exécution et des incitatifs suffisants pour assurer le respect de la *Loi*; 2) les notions centrales, comme les « renseignements personnels » et l'« activité commerciale », qui ont une influence directe sur la portée de l'application de la LPRPDE; 3) des approches novatrices pour que les organisations assument leur responsabilité à l'égard des pratiques de gestion des renseignements personnels et rendent des comptes à ce sujet.

CHAPITRE 4

Répondre aux préoccupations des Canadiennes et Canadiens

Répondre aux questions et examiner les plaintes constituent l'essentiel de notre travail au Commissariat. Nous sommes en contact direct avec les Canadiennes et Canadiens — que ce soit en répondant à leurs questions sur la protection de la vie privée ou en nous penchant et en enquêtant sur les plaintes déposées à la suite de problèmes avec lesquels ils ont été aux prises lors de leurs communications avec diverses organisations.

Cette année, le Commissariat a continué d'améliorer ses processus de traitement des questions et des plaintes en vue de mieux servir les Canadiennes et Canadiens.

4.1 DEMANDES D'INFORMATION

Notre centre d'information, qui a été réorganisé, a répondu à 5 236 demandes d'information liées aux questions de protection de la vie privée dans le secteur privé en 2011, ce qui représente une légère augmentation par rapport à 2010. La grande majorité des demandes (4 518) ont été faites par téléphone, comme les années précédentes.

Les sites de réseautage social constituaient la catégorie la plus importante des demandes, et notre système de suivi indique qu'il y avait une forte augmentation lorsque les médias faisaient état de controverses liées à Facebook et à Google. Les personnes qui appelaient étaient notamment préoccupées par la communication éventuelle de renseignements personnels sans leur consentement, l'efficacité des paramètres de confidentialité, la collecte d'identificateurs personnels pour rétablir un compte, et l'utilisation abusive de renseignements personnels déjà affichés en ligne.

Les nouvelles technologies servant à surveiller le lieu de travail étaient aussi un thème récurrent. Les employés se sont dits préoccupés par la collecte de leurs renseignements personnels au travail sans qu'ils puissent s'y soustraire.

Les appels augmentaient aussi lorsque se produisait une atteinte à la sécurité des données très médiatisée, comme celle qui concernait les comptes des utilisateurs du réseau PlayStation de Sony. Les personnes qui appelaient ne se renseignaient pas nécessairement au sujet d'une atteinte précise, mais elles posaient souvent des questions sur la sécurité des renseignements personnels en général.

Le Commissariat a continué de recevoir presque tous les jours des appels concernant des préoccupations relatives à la collecte de renseignements personnels, comme le numéro d'assurance sociale, la date de naissance et des renseignements sur le compte bancaire, pour conclure un contrat de location, obtenir un rapport de solvabilité ou pour retourner un produit à un magasin de détail. La collecte de renseignements personnels suscite des inquiétudes quant aux mesures de protection subséquentes et aux pratiques des différentes organisations en matière de conservation.

Parmi les autres sujets de préoccupation, mentionnons ce que les gens définissaient comme une collecte abusive de renseignements médicaux par les compagnies d'assurances, l'exactitude des renseignements personnels détenus par les banques et les agences d'évaluation du crédit, et la difficulté à avoir accès aux renseignements que possèdent les entreprises de télécommunications pour en vérifier l'exactitude.

4.2 ACCUEIL

En 2011, dans le cadre de nos efforts pour améliorer nos services de première ligne, nous avons créé une unité spéciale pour l'accueil.

Toutes les plaintes écrites portant sur la protection de la vie privée sont transmises à cette unité. L'unité d'accueil examine la plainte et, s'il y a lieu, elle fait rapidement le suivi avec le plaignant pour clarifier notre compréhension du problème et obtenir des renseignements ou des documents supplémentaires pour entreprendre une enquête.

Si le plaignant n'a pas encore fait part de ses préoccupations à la personne responsable de la protection de la vie privée de l'organisation concernée, un agent de l'unité d'accueil demandera au plaignant d'essayer de régler le problème directement avec l'organisation et, s'il n'y parvient pas, de communiquer de nouveau avec nous.

De plus, comme c'est souvent le cas lorsque des gens appellent nos agents d'information, l'équipe de l'unité d'accueil peut parfois régler le problème de façon satisfaisante sur-le-champ, de sorte que le Commissariat n'a pas à s'occuper de la question comme s'il s'agissait d'une plainte officielle.

Par exemple, si une enquête antérieure a démontré que les activités faisant l'objet de la plainte sont conformes à la LPRPDE, un agent d'accueil l'expliquera à la personne concernée.

Ou, si nous avons déterminé précédemment que notre juridiction ne s'étendait pas à l'organisation ou au type d'activité mis en cause, un agent l'expliquera à la personne et tentera de l'orienter vers d'autres ressources ou formes d'aide.

4.3 PLAINTES REÇUES

Globalement, en 2011, le Commissariat a accepté 281 plaintes officielles en vertu de la LPRPDE. Cela représente une augmentation de 35 % par rapport aux 207 plaintes de 2010. Cette augmentation peut être liée à divers facteurs, comme la complexité croissante des questions que les Canadiennes et Canadiens soulèvent (ce qui fait que davantage de plaintes deviennent officielles), la possibilité que la population canadienne soit de plus en plus consciente de son droit à la vie privée, ou des changements dans la façon dont nous interagissons tous avec les entreprises dans une économie de plus en plus numérique.

4.4 PLAINTES PAR SECTEUR D'ACTIVITÉ

Le secteur financier continue d'être à l'origine de la proportion la plus importante des plaintes officielles que nous avons acceptées, soit environ une plainte sur cinq.

Selon notre expérience, les institutions financières sont parmi les organisations dotées des meilleures politiques et pratiques en matière de protection de la vie privée, même si nos enquêtes continuent de mettre en évidence des aspects problématiques. L'explication de ce nombre élevé semble liée à la taille du secteur financier et au nombre gigantesque de transactions effectuées par les Canadiennes et Canadiens.

Le nombre de plaintes liées au secteur du transport a grimpé en flèche cette année, si on compare avec les années précédentes. Il a doublé, de sorte que ce secteur occupe maintenant la deuxième place pour ce qui est du nombre de plaintes. Un peu plus de la moitié des plaintes portaient sur l'accès. On ne sait pas exactement ce qui explique cette augmentation, qui a été constatée dans tous les sous secteurs du transport. Nous avons l'intention d'observer attentivement cette tendance dans l'année qui vient pour en déterminer les implications éventuelles.

Par ailleurs, les plaintes relatives au secteur de l'assurance (auparavant l'un des trois principaux secteurs) ont diminué ces deux dernières années.

Ce pourrait être parce que, au cours des deux dernières années, on a vu que les règles de protection de la vie privée du secteur de l'assurance devenaient plus explicites et qu'elles étaient mieux connues.

Principaux secteurs visés par les plaintes

Secteur	2011	2010	2009
Secteur financier	22 %	22 %	24 %
Transport	12 %	6 %	6 %
Télécommunications	11 %	9 %	18 %*
Services	10 %	17 %	4 %
Assurance	9 %	13 %	18 %

*Avant 2010, les plaintes liées à Internet entraient dans la catégorie des télécommunications, mais elles constituent maintenant une catégorie distincte.

Nota : L'annexe 2 présente des statistiques et des définitions pour tous les secteurs d'activité.

4.5 TYPES DE PLAINTES REÇUES

L'utilisation et la communication de renseignements personnels, l'accès à ceux-ci, de même que la collecte de tels renseignements ont été, une fois de plus, parmi les trois principales questions soulevées dans les plaintes adressées au Commissariat.

De plus, nous avons remarqué que la proportion de plaintes qui portaient sur les corrections ou les annotations liées aux renseignements personnels a augmenté considérablement cette année, passant à 5 % de toutes les plaintes officielles acceptées (comparativement à 1 % ou moins dans les années précédentes). Cela pourrait s'expliquer par une sensibilisation accrue des Canadiennes et Canadiens à la façon dont leurs renseignements personnels sont recueillis et utilisés et au fait qu'ils savent qu'ils ont le droit de voir et de faire corriger les dossiers qui les concernent.

Trois principaux types de plaintes reçues dans les trois dernières années

Type de plainte	2011	2010	2009
Utilisation et communication : Plaintes alléguant l'utilisation ou la communication inopportunes de renseignements personnels, sans consentement de l'intéressé, à des fins autres que celles pour lesquelles ils avaient été recueillis	32 %	27 %	26 %
Accès : Plaintes concernant la difficulté d'accès à ses propres renseignements personnels	26 %	24 %	28 %
Collecte : Plaintes concernant la collecte superflue de renseignements personnels, ou la collecte illégitime ou illégale de renseignements personnels, par exemple sans un consentement approprié	20 %	16 %	14 %

4.6 RÈGLEMENT RAPIDE

Nous avons mis en place un mécanisme de règlement rapide, dont s'occupent certains agents. Cela nous permet d'offrir un meilleur service aux Canadiennes et Canadiens en réglant les plaintes rapidement, grâce à une approche moins structurée que notre processus d'enquête officiel.

Lorsque nous recevons une plainte écrite au sujet d'un problème susceptible d'être réglé rapidement, l'unité d'accueil transmet le cas à un agent de règlement rapide.

Cet agent travaille à la fois avec le plaignant et l'organisation mise en cause pour en arriver à une solution.

Le processus de règlement rapide est très efficace. Dans certains cas, un problème qui n'aurait été réglé qu'après des mois dans le cadre du processus d'enquête officielle l'est maintenant en quelques jours. Nous avons reçu des commentaires très positifs sur le processus, aussi bien de la part des plaignants que des organisations.

PLAINTES POUR RÈGLEMENT RAPIDE

En 2011, nous avons examiné 125 dossiers en vue d'un règlement rapide. Comme le montrent les statistiques détaillées de l'annexe 2, nous avons réussi à trouver une solution appropriée dans 116 de ces dossiers. Les neuf autres cas ont été transférés pour qu'une enquête officielle soit menée.

Pour continuer d'améliorer l'efficacité et la rapidité d'exécution des services que nous offrons à la population canadienne, nous avons augmenté considérablement le nombre de plaintes traitées au moyen de ce processus, soit près de la moitié des plaintes officielles, alors que c'était environ le quart en 2010.

Malgré ce volume accru, nous maintenons l'amélioration apportée l'an dernier dans la rapidité de résolution de ces plaintes. En 2011, les plaintes qui ont fait l'objet d'un règlement rapide ont, en moyenne, été réglées dans un délai de deux mois après l'acceptation de la plainte, comparativement à 14 mois lorsqu'il y avait une enquête complète.

De plus, nous avons maintenu un taux extrêmement élevé de règlement satisfaisant : plus de 90 %.

Le processus de règlement rapide continuera d'être un outil important pour s'occuper rapidement et efficacement des questions que les Canadiennes et Canadiens portent à l'attention du Commissariat.

Nous encourageons également tous les enquêteurs à recourir à des méthodes de règlement rapide lorsqu'ils ont l'occasion de le faire. Par exemple, le premier cas exemplaire présenté dans la section suivante est un cas qui avait été assigné à un enquêteur. Dès les premières étapes de l'enquête, l'enquêteur s'est rendu compte qu'il était possible d'utiliser les méthodes de règlement rapide, et il a réglé la plainte rapidement.

Bien entendu, les plaintes ne peuvent pas toutes être résolues ainsi. Celles qui soulèvent des questions complexes ou systémiques ou qui renvoient à des enjeux nouveaux continueront d'être traitées dans le cadre du processus d'enquête officielle.

PLAINTES POUR RÈGLEMENT RAPIDE LIÉES À LA LPRPDE EN 2011

Nombre total d'interventions de règlement rapide menées à terme	Nombre de dossiers transférés pour une enquête plus approfondie	Nombre de plaintes résolues de manière satisfaisante
125	9	116

Nota : L'annexe 2 contient d'autres statistiques sur les secteurs visés, les types de plaintes et les décisions des interventions de règlement rapide fructueuses.

DES CAS DE RÈGLEMENT RAPIDE EXEMPLAIRES

Inquiétudes concernant les mesures de protection pour les mots de passe des clients

Après s'être inscrit en ligne au programme de fidélisation d'une entreprise, le plaignant a reçu un courriel de confirmation contenant son mot de passe sécurisé. À la demande de l'un de nos enquêteurs, l'entreprise a examiné la pratique consistant à envoyer le mot de passe dans le courriel de confirmation. Elle a conclu que ce n'était pas nécessaire et a mis un terme à cette pratique. Les représentants de l'entreprise ont présenté leurs excuses au plaignant et l'ont remercié d'avoir attiré leur attention sur cette question. La réponse rapide et efficace de l'entreprise a satisfait le Commissariat et le plaignant.

L'ancien ami de cœur d'une plaignante utilise son rapport de solvabilité pour la retrouver

Alors qu'elle vérifiait son rapport de solvabilité, une personne a remarqué qu'elle avait fait l'objet d'une enquête de la part d'un détaillant qui employait son ancien ami de cœur, qu'elle avait quitté. La personne a communiqué avec le Commissariat parce qu'elle craignait que son ancien ami ait utilisé les renseignements de son rapport de solvabilité pour la retracer.

Un agent de règlement rapide a communiqué avec le détaillant, qui a confirmé qu'un employé avait enfreint la politique de l'entreprise. Le détaillant a pris des mesures disciplinaires et il a aussi restreint l'accès au système de vérification de la solvabilité à la haute direction. L'entreprise a présenté ses excuses à la plaignante.

La personne était satisfaite de la réponse du détaillant, mais elle craignait encore que quelqu'un puisse faire une vérification de sa solvabilité pour savoir où elle vivait. Un agent de règlement rapide a communiqué avec le responsable de la protection de la vie privée de l'agence d'évaluation du crédit, qui a accepté de collaborer avec la plaignante pour éviter que cet incident ne se reproduise.

Renseignements sur le permis de conduire recueillis inutilement

Alors qu'il achetait des billets pour la location d'un go-kart, un homme s'est fait demander de fournir son permis de conduire. Interrogé sur la raison de cette demande, le propriétaire lui a répondu que la date de naissance et le numéro du permis de conduire étaient consignés à des fins de marketing et qu'il ne pourrait pas utiliser ses billets s'il ne fournissait pas ces renseignements. Un agent de règlement rapide a communiqué avec le propriétaire de l'entreprise et lui a transmis les publications du Commissariat portant sur l'utilisation des permis de conduire et lui a fait part d'une décision antérieure relativement à cette question.

Le propriétaire et son personnel ont lu les documents et ils ont pris conscience du caractère délicat de l'information qu'ils consignaient. Cette petite entreprise a immédiatement pris des mesures importantes pour s'acquitter de ses obligations en matière de protection de la vie privée : a) modifier le

logiciel de collecte des données; b) mettre au point une formation sur la nouvelle politique en matière de protection de la vie privée et l'offrir au personnel; c) afficher dans un endroit public, à l'intention des consommateurs, sa politique sur la collecte de renseignements. Le propriétaire était reconnaissant pour l'information fournie, et le plaignant était satisfait des mesures prises pour régler sa plainte.

Difficulté à avoir accès à ses propres renseignements personnels

Une personne s'est plainte au Commissariat qu'une entreprise de télécommunications n'avait pas répondu à sa demande d'accès à ses renseignements personnels. L'agent de règlement rapide a communiqué avec l'entreprise afin de savoir pourquoi elle n'avait pas donné suite à la demande. L'entreprise a fait enquête et a découvert que deux services de son organisation étaient au courant de la demande mais qu'aucun d'eux n'avait répondu, car ils avaient pensé que l'autre l'avait déjà fait. Après avoir déterminé ce qui s'était passé, l'entreprise a immédiatement répondu à la demande, et elle a apporté des changements pour s'assurer que ce genre d'incident ne se reproduise pas. Le plaignant a reçu le document qu'il avait demandé et s'est dit satisfait de la réponse de l'entreprise.

Suppression de renseignements personnels sur un site Web hébergé au Royaume-Uni

Une personne a communiqué avec nous pour se plaindre qu'un site Web de réseautage social hébergé au Royaume-Uni avait ignoré ses demandes répétées pour faire supprimer son profil, et qu'il continuait de recevoir des messages de ce site Web.

L'agent de règlement rapide a communiqué avec le siège du site Web au Royaume-Uni. Le responsable de la protection de la vie privée de l'entreprise a passé en revue les politiques et procédures de la compagnie concernant la suppression d'un profil, et il a été incapable d'expliquer pourquoi le profil du plaignant n'avait pas été supprimé. Cependant, l'entreprise a répondu immédiatement à notre demande d'effacer le profil du plaignant, et elle s'est assurée que cette mesure était permanente. Le plaignant était satisfait des mesures prises par l'entreprise.

4.7 ENQUÊTES SUR LES PLAINTES

En 2011, nous avons mené à terme 120 enquêtes sur des plaintes. Ces enquêtes officielles ont été effectuées dans les cas où les plaintes soulevaient des questions complexes ou systémiques ou renvoyaient à des enjeux nouveaux.

Le nombre d'enquêtes conclues est nettement plus faible qu'en 2010, alors que nous avions parachevé 249 enquêtes, dans le cadre d'un effort de deux ans pour éliminer l'arriéré de plaintes.

En 2011, grâce à l'élimination de l'arriéré et à l'utilisation accrue du règlement rapide, nous avons pu revenir aux niveaux de dotation de 2008 tout en améliorant la rapidité d'exécution de nos enquêtes.

Le délai moyen pour les enquêtes sur des plaintes officielles a chuté à 14 mois — une diminution de plusieurs mois par rapport aux années précédentes. Cette amélioration, combinée aux plaintes qui ont mené à un règlement rapide, s'est traduite par une diminution notable du délai de traitement moyen des plaintes acceptées.

La moyenne globale est maintenant d'un peu plus de huit mois.

Nous nous réjouissons également du fait que, dans la majorité des enquêtes, nous avons pu en arriver à une conclusion satisfaisante. Dans seulement 11 % des cas, les plaintes ont été jugées fondées (mais non résolues) à la suite des enquêtes, ce qui veut dire que nous ne sommes pas parvenus à une conclusion que nous jugions acceptable. (Voir plus loin pour plus de détails.)

En 2011, nous avons constaté une augmentation du nombre d'enquêtes pour lesquelles nous avons conclu que la LPRPDE ne s'appliquait pas à l'organisation ou à l'activité faisant l'objet de la plainte. Ce nombre est passé à 15 % des enquêtes, alors qu'il était de 3 % l'année précédente.

Cette augmentation est en partie attribuable à la décision rendue en 2010 par la Cour fédérale sur la portée de l'application de la LPRPDE. Cette décision portait sur la collecte de renseignements personnels en vue de défendre une personne assurée contre une réclamation en responsabilité civile délictuelle découlant d'un accident de la route. Quelques dossiers ont alors été fermés parce que les plaintes avaient été reçues avant cette décision relative au champ de compétence et qu'elles concernaient des activités pour lesquelles la Cour avait jugé que la LPRPDE ne s'appliquait pas.

Nous avons aussi constaté une diminution importante de la proportion de plaintes considérées comme résolues, ou considérées comme fondées et résolues. Cette proportion a diminué des deux tiers, passant de 33 % de tous les cas en 2010 à seulement 11 % en 2011.

Cette diminution a été presque complètement contrebalancée par l'augmentation de la proportion des cas résolus grâce au processus de règlement rapide, qui a pratiquement doublé, passant de 24 % en 2010 à 49 % en 2011.

Ces deux changements démontrent comment les dossiers qui étaient auparavant réglés dans le cadre du processus d'enquête, qui prenait un temps considérable, le sont maintenant plus rapidement dans le cadre du processus de règlement rapide. Les chiffres montrent éloquemment les gains d'efficacité réalisés au profit de la population canadienne grâce au règlement rapide.

4.8 APERÇU DES ENQUÊTES DE 2011

Nombre d'enquêtes menées à terme	Nombre de plaintes jugées fondées (et non résolues)	Nombre de plaintes réglées de manière satisfaisante
120	13	107

Nota : L'annexe 2 contient d'autres statistiques sur les secteurs visés, les types de plaintes et les décisions liées aux enquêtes menées à terme.

RÉSUMÉS DES ENQUÊTES

La section suivante porte sur des enquêtes parachevées en 2011. Des renseignements supplémentaires sur certaines d'entre elles se trouvent sur notre site Web.

La commissaire a rendu public le nom des organisations contre lesquelles des plaintes ont été déposées seulement lorsqu'il était dans l'intérêt public de le faire.

Les enquêtes portant sur des cas liés aux jeunes Canadiennes et Canadiens sont abordées au chapitre 2, la section spéciale sur la protection de la vie privée des enfants et des jeunes. Les cas se rapportant à la protection des renseignements financiers et biométriques et à la protection de la vie privée en ligne sont abordés au chapitre 3, qui présente la protection de la vie privée en 2011.

La présente partie fait ressortir certains risques pour les renseignements personnels que nous avons cernés au cours de nos enquêtes.

RISQUE : NE PAS INDIQUER COMME IL SE DOIT LA RAISON DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS

Un chercheur d'emploi est mal informé des fins pour lesquelles des renseignements personnels étaient recueillis

Le plaignant a été contacté par courriel par une associée de l'industrie d'une compagnie ayant son siège à Toronto et exploitée sous le nom de Job Success. Ayant obtenu une copie du curriculum vitae du plaignant à partir d'un site Web de recherche d'emploi, et dans le but manifeste de lui offrir des services de recherche d'emploi et de gestion de carrière, l'associée a informé le plaignant qu'il pourrait être invité à se présenter à une « entrevue ».

Lorsque l'entreprise a appelé le plaignant pour fixer un rendez-vous, ce dernier a demandé des précisions. Il voulait notamment savoir si l'entrevue concernait un emploi précis. L'employée qui organisait la rencontre a répondu qu'elle ne possédait pas cette information, en ajoutant que des renseignements complémentaires lui seraient fournis en personne.

Après avoir accepté l'invitation à une entrevue, le plaignant s'est rendu au bureau de la mise en cause et a été présenté à un directeur principal. Après les présentations, le directeur principal a demandé au plaignant d'où il était originaire et où il avait fait ses études. Il lui a aussi demandé de donner des précisions sur les expériences professionnelles mentionnées dans son curriculum vitae et de parler de ses aspirations professionnelles.

Vers la fin de la rencontre, qui a duré environ 45 minutes, le directeur principal a abordé la question du « processus de sélection » de l'entreprise et des prétendus avantages qu'il y avait à faire affaire avec Job Success (c'est-à-dire, aide pour faire son autopromotion auprès d'employeurs éventuels, obtenir des entrevues intéressantes et apprendre comment se comporter lors des entrevues).

Jusque-là, le plaignant avait l'impression que l'entreprise menait une entrevue d'emploi. C'est pourquoi le plaignant maintenait qu'il avait été induit en erreur quant aux raisons pour lesquelles ses renseignements personnels avaient été recueillis.

Notre enquête a porté sur l'obligation qu'a Job Success d'indiquer, au moment de la collecte ou avant celle-ci, les fins pour lesquelles des renseignements personnels sont recueillis. Aux termes de la LPRPDE, une organisation doit documenter les fins pour lesquelles les renseignements personnels sont recueillis et indiquer ces fins aux personnes auxquelles les renseignements appartiennent.

Au moment où nous avons amorcé notre enquête, il était difficile de trouver des renseignements sur les pratiques de gestion de l'information de l'entreprise. Initialement, la politique sur la protection de la vie privée ne se trouvait pas sur le site Web de l'entreprise et on ne pouvait trouver nulle part d'information sur les raisons pour lesquelles elle recueillait des renseignements personnels.

Non seulement le site Web de l'entreprise manquait d'information, mais Job Success a en outre omis de préciser les fins pour lesquelles elle recueillait des renseignements personnels avant de rencontrer le plaignant.

Au cours de l'enquête, nous avons posé des questions à la mise en cause sur le peu d'information qu'elle donne sur ses services. L'entreprise a répondu que son site Web ne visait pas à fournir de l'information, mais à susciter de la curiosité à son sujet et donc à inciter les gens à venir sur place.

À notre avis, Job Success a négligé d'indiquer clairement aux personnes concernées, au moment de la collecte ou avant celle-ci, les fins pour lesquelles les renseignements personnels sont recueillis.

De plus, étant donné que l'entreprise n'a pas fait suffisamment d'efforts pour s'assurer que le plaignant était informé des fins auxquelles serviraient ses renseignements personnels, d'une manière qu'il pourrait raisonnablement comprendre, elle a négligé d'obtenir le consentement valable du plaignant pour la collecte et l'utilisation de ses renseignements personnels.

Au cours de l'enquête, Job Success a accepté de prendre des mesures correctives dans un délai de 90 jours après la présentation de notre rapport final. Nous avons jugé que la plainte était fondée et conditionnellement résolue.

RISQUE : UTILISATION DE RENSEIGNEMENTS PERSONNELS SENSIBLES AUX FINS D'IDENTIFICATION

Les entreprises de câblodistribution et de communications utilisent des renseignements personnels sensibles aux fins d'identification

Au cours de l'année, nous avons mené des enquêtes sur plusieurs plaintes portées contre des entreprises de câblodistribution et de communications qui tentaient de recueillir des renseignements personnels sensibles auprès des personnes aux fins d'identification en ligne ou par téléphone.

Presque toutes ces plaintes concernaient des personnes qui voulaient ouvrir un nouveau compte de service, ou qui voulaient obtenir de l'information ou de l'aide relativement à des comptes existants.

Dans la plupart des cas, les personnes qui voulaient obtenir de nouveaux services (par téléphone ou en ligne) se faisaient demander de fournir des renseignements personnels aux fins d'identification. Parmi les renseignements qui étaient le plus souvent recueillis, il y avait le numéro d'assurance sociale (NAS), le numéro du permis de conduire provincial ou le numéro du passeport canadien. Les gens se faisaient aussi demander des renseignements de base, notamment leur date de naissance.

Le Commissariat a déjà statué que la collecte de renseignements sensibles pouvait être justifiée quand une organisation a besoin de vérifier la solvabilité d'un nouveau client. Réduire les risques de crédit que les organisations encourent lorsqu'elles acceptent de nouveaux clients — dont les échanges avec le fournisseur de services se font souvent uniquement en ligne ou par téléphone — constitue, à notre avis, une fin commerciale légitime. Comme l'affirment immanquablement les représentants de l'industrie des communications, l'utilisation des renseignements personnels pour faire une vérification du crédit appropriée et s'assurer que les renseignements sont exacts peut, parfois, contribuer à réduire les risques associés au crédit.

Dans les cas sur lesquels nous avons fait enquête, nous avons aussi fait remarquer que, bien que la collecte du NAS, du numéro de permis de conduire ou de passeport était une condition admise pour la prestation de services, ce n'était pas une condition absolue. Au cours de nos enquêtes, nous avons constaté que les mis en cause avaient pour politique d'offrir à leurs clients d'autres options que la collecte de renseignements personnels aux fins de la vérification du crédit. Les clients qui n'avaient pas besoin de crédit pouvaient choisir de fournir aux entreprises un numéro de carte de crédit valide ou d'effectuer un dépôt en espèces comme gage.

Malgré ce qui précède, bien qu'il puisse être raisonnable pour une entreprise de demander des

renseignements personnels sensibles *en vue de faciliter la vérification de la solvabilité*, la collecte de cette même information aux fins d'identification des clients (souvent à la suite de la création d'un compte de service) n'est peut-être pas nécessaire. Dans les cas que nous avons examinés, les plaignants ont dit à maintes reprises que les pratiques de l'industrie les préoccupaient, c'est-à-dire la pratique qui consiste à demander à un client de prouver son identité en fournissant des renseignements personnels pouvant être sensibles.

À notre avis, la collecte du NAS, du numéro de permis de conduire ou de passeport aux fins d'identification peut, dans certains cas, constituer une infraction à la LPRPDE. Non seulement ce genre de renseignements personnels n'est pas nécessaire pour offrir des services de téléphonie cellulaire, de câblodistribution ou d'Internet, mais la plupart des entreprises offrant ces services ont démontré qu'elles pouvaient authentifier l'identité de leurs clients (à la suite d'une vérification de la solvabilité et de la création d'un compte) sans les recueillir.

Dans les cas sur lesquels nous avons enquêté, les organisations mises en cause ont démontré qu'elles étaient capables d'authentifier l'identité de leurs clients actuels d'une manière qui est plus respectueuse de la vie privée. Dans la plupart des cas, les entreprises le faisaient en permettant aux clients de créer eux mêmes leur numéro d'identification personnel (NIP) ou leur mot de passe.

Évidemment, le fait pour une personne de fournir son NAS, son numéro de permis de conduire ou de passeport aux fins d'identification peut demeurer facultatif. D'ailleurs, nous sommes sensibles aux préoccupations des entreprises, qui font valoir que les clients oublient souvent leur mot de passe et que l'obligation d'utiliser un mot de passe par défaut à des fins d'identification peut engendrer de la frustration chez les consommateurs.

Mais les clients éventuels devraient être informés préalablement qu'ils ont la possibilité de fournir d'autres renseignements permettant de les identifier ou des renseignements personnels moins sensibles, et cela devrait être indiqué dans la politique de confidentialité de l'entreprise.

Lorsqu'une organisation recueille des renseignements personnels, elle doit en tout temps les conserver de manière appropriée.

RISQUE : OMISSION D'INDIQUER QU'IL Y A DE LA VIDÉOSURVEILLANCE

Les renseignements personnels recueillis dans le cadre de la défense en droit d'une entreprise relèvent de la LPRPDE

La plaignante a allégué qu'elle s'était blessée après avoir mis le pied dans une flaque d'eau dans un magasin Sobeys en novembre 2008. Elle a discuté de l'incident avec le gérant du magasin et a ultérieurement retenu les services d'un avocat.

Dans une lettre à Sobeys, l'avocat demandait divers documents, y compris des enregistrements de l'incident faits par vidéosurveillance. Il indiquait que

sa cliente avait dit que le toit du magasin coulait. La cliente a présenté une autre demande à Sobeys afin d'avoir accès à ses renseignements personnels, en invoquant la LPRPDE.

Dans la plainte déposée par la suite au Commissariat, la cliente a allégué que, au moment de l'incident, elle n'était pas consciente du fait que ses renseignements personnels étaient en train d'être recueillis sous la forme d'un enregistrement vidéo. Elle a dit que, quand elle a signalé sa chute, le gérant a négligé de lui révéler l'existence de l'enregistrement vidéo.

Dans sa plainte, la cliente alléguait que Sobeys aurait recueilli, utilisé et communiqué ses renseignements personnels à son insu et sans son consentement. Elle alléguait également que le magasin aurait refusé de façon inappropriée de lui communiquer des renseignements personnels qu'elle avait le droit de consulter en vertu de la LPRPDE.

La LPRPDE exige que toute personne soit informée de la collecte de renseignements personnels qui la concernent et y consente. Nos *Lignes directrices sur la surveillance vidéo au moyen d'appareils non dissimulés dans le secteur privé* de 2009 précisent clairement que le public doit être informé d'une telle surveillance.

Cependant, la politique de confidentialité de Sobeys ne fait aucune mention de la vidéosurveillance ou de toute collecte de renseignements personnels par ces moyens.

Sobeys a également confirmé qu'il n'y avait aucune affiche posée dans le magasin pour informer les clients du fait que les lieux étaient sous vidéosurveillance. Cependant, il y a un appareil de surveillance montrant les personnes entrant dans le magasin et en sortant, et des caméras sont suspendues au plafond, à la vue des clients. Le responsable de la protection de la vie privée de Sobeys a affirmé qu'il était évident pour quiconque dans le magasin que des caméras vidéo étaient utilisées.

À notre avis, en eux-mêmes, un appareil de surveillance situé à l'entrée et des caméras suspendues bien au-dessus des têtes n'indiquent pas clairement et suffisamment aux clients qu'un système de vidéosurveillance est utilisé.

De plus, les personnes doivent être informées de la surveillance lorsqu'elles sont encore à l'extérieur du magasin, pour qu'elles puissent choisir d'y entrer ou non. Conformément à nos lignes directrices, une affiche doit être posée à l'entrée principale pour avertir les clients potentiels. Elle devrait décrire brièvement les fins de la vidéosurveillance et indiquer un numéro de téléphone pour obtenir de plus amples renseignements ou pour permettre aux clients de demander accès à leurs renseignements personnels.

Lignes directrices sur la surveillance vidéo au moyen d'appareils non dissimulés dans le secteur privé

Dans un rapport préliminaire fourni à Sobeys en décembre 2010, nous avons recommandé que tous les magasins de la chaîne signalent adéquatement la collecte de renseignements personnels au moyen de l'utilisation de la

vidéosurveillance. Nous avons également demandé à Sobeys d'inclure une description de ses pratiques en matière de collecte de renseignements personnels au moyen de la vidéosurveillance dans sa politique de confidentialité.

En réponse à nos recommandations, Sobeys a appliqué un autocollant à l'entrée du magasin en question, où les clients peuvent également voir un appareil de surveillance en marche, de même qu'une caméra suspendue à ses côtés, ainsi que dans une autre section du magasin pour indiquer que des caméras de télévision en circuit fermé sont utilisées.

Sobeys invite également ses autres magasins à poser ces autocollants et nous a avisés depuis que ceux-ci sont en place dans tous ses magasins du Nouveau Brunswick.

À la conclusion de notre enquête, nous avons déterminé que la partie relative à la collecte des renseignements personnels de la plainte était fondée.

Cependant, nous sommes également d'avis que les autocollants, avec l'appareil de surveillance à l'entrée du magasin ainsi que la caméra suspendue à ses côtés signalaient suffisamment que le magasin est sous vidéosurveillance. En conséquence, nous avons également jugé que la question était résolue.

En plus de la question de la collecte des renseignements personnels, la plaignante a également allégué qu'elle s'est vu refuser l'accès à ses renseignements personnels.

Au début, le responsable de la protection de la vie privée de Sobeys nous avait dit que les seuls renseignements personnels que le magasin avait recueillis au sujet de la plaignante dans le cadre de ses activités commerciales étaient l'enregistrement vidéo de sécurité.

Prié de répondre à d'autres questions, le responsable a cependant affirmé que le magasin avait recueilli d'autres renseignements personnels au sujet de la plaignante, mais qu'ils avaient été produits dans le but de permettre à l'entreprise de se défendre contre une éventuelle réclamation en dommages-intérêts de la plaignante.

Étant donné que l'enregistrement vidéo a été remis à la plaignante deux jours après qu'elle a présenté une demande en vertu de la LPRPDE, nous avons rejeté cette partie de la plainte relative à l'accès aux renseignements personnels, car elle n'était pas fondée.

En ce qui concerne les rapports et les lettres créés après que la blessure est survenue, nous avons estimé que l'activité de Sobeys, qui consiste à répondre à la réclamation en responsabilité civile délictuelle d'une cliente portant sur un incident qui s'est produit dans ses locaux, se rapportait suffisamment à ses activités pour constituer une activité commerciale au sens de la *Loi*. Cette activité est, en conséquence, assujettie à la LPRPDE.

Mais nous avons aussi conclu que les documents en question étaient protégés dans le cours d'une procédure de nature judiciaire, une composante du secret professionnel liant l'avocat à son client, qui

protège les documents produits aux fins principales d'un litige ou d'un litige raisonnablement prévisible.

À notre avis, Sobeys était donc dans son droit de refuser à la plaignante l'accès aux renseignements personnels contenus dans ces documents.

Par conséquent, nous avons déterminé que la partie de la plainte relative à l'accès aux renseignements personnels se rapportant aux lettres et aux rapports n'était pas fondée.

PLAINTES NON RÉSOLUES

Nous sommes généralement en mesure de régler les problèmes de façon satisfaisante au moyen de notre processus d'enquête. La grande majorité des organisations répondent favorablement à nos recommandations.

Toutefois, lorsqu'une société refuse de suivre nos recommandations, nous pouvons demander à la Cour fédérale de rendre une ordonnance pour l'obliger à se conformer et à offrir un dédommagement, s'il y a lieu. La commissaire peut également dévoiler le nom des entreprises qui ont fait l'objet d'une enquête si elle juge qu'il est dans l'intérêt public de le faire dans les circonstances.

Le résumé de conclusions d'enquête suivant donne un exemple de plainte qui n'a pu être résolue de façon satisfaisante.

RISQUE : LES ORGANISATIONS INTERNATIONALES ET LE RESPECT DE LA LPRPDE

Le site Web de KLM au Canada ne satisfait pas aux obligations énoncées dans la LPRPDE

Le plaignant alléguait que KLM Royal Dutch Airlines (KLM) ne lui aurait pas permis d'avoir accès à ses renseignements personnels ainsi qu'à ceux des membres de sa famille, lesquels avaient été recueillis et utilisés pour des vols sur KLM. Il alléguait de plus que KLM aurait omis de lui fournir des informations concernant ses politiques et pratiques relatives à la gestion de ses renseignements personnels.

Malgré le fait que KLM soit une société aérienne internationale dont le siège social est situé à Amstelveen, aux Pays-Bas, le Commissariat a déterminé qu'il était de son ressort d'enquêter parce qu'il y avait un lien réel et substantiel entre la question en litige et les parties au Canada — un critère établi par la Cour fédérale.

Le plaignant soutenait que dans une lettre datée du 10 janvier 2009, il aurait demandé à KLM l'accès à 13 types de renseignements sur les passagers concernant deux vols que lui et sa famille avaient pris en 2005. KLM soutenait qu'elle n'avait reçu une lettre du plaignant à propos de ces renseignements que le 17 mars 2009.

Dans sa lettre du 6 mai 2009, KLM informait le plaignant que, si longtemps après les vols, les seuls renseignements sur les passagers identifiables étaient

ceux qui concernaient l'enregistrement relatif à un vol, qui ont été fournis au plaignant. N'étant pas satisfait de cette réponse, le plaignant a déposé une plainte auprès du Commissariat en date du 10 juin 2009.

La réponse de KLM, selon laquelle elle ne possédait plus de renseignements, nous a paru acceptable, car trois ans et demi s'étaient écoulés depuis les vols et la première demande du plaignant. La *Loi* stipule que les organisations ne sont tenues de conserver des renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées. À moins de circonstances atténuantes, on peut se demander pourquoi il faudrait s'attendre à ce que KLM conserve les renseignements personnels du plaignant plus longtemps.

Cependant, en ne se conformant pas au délai de réponse de 30 jours prévu dans la *Loi*, KLM avait au départ refusé au plaignant l'accès à ses renseignements personnels.

De plus, notre examen en cours d'enquête de la politique de confidentialité en ligne de KLM pour son site Web du Canada a permis d'établir que cette politique est incomplète, ne respecte pas les exigences de la LPRPDE et ne contient pas de renseignements détaillés sur les politiques et pratiques de KLM concernant la gestion des renseignements personnels.

Notre rapport d'enquête recommandait que KLM veille à ce que la politique de confidentialité destinée à la version canadienne de son site Web respecte les exigences de la *Loi* et que cette politique de confidentialité en ligne contienne soit de l'information concernant la gestion des renseignements personnels par la société soit, à tout le moins, des indications soulignant qu'il est possible d'obtenir sur demande ce type d'information.

Au départ, KLM semblait assez disposée à mettre en application notre recommandation en mettant à jour sa politique de confidentialité en ligne pour le Canada de façon à respecter les obligations que lui impose la *Loi*. Cependant, dans un courriel daté du 17 février 2011, KLM indiquait que la mise à jour prévue de sa politique de confidentialité avait été reportée à cause de difficultés techniques. Nous sommes déçus par le manque d'engagement de KLM à l'égard d'un échéancier précis en vue de la mise en application de cette recommandation.

Nous n'avions d'autre choix que de mettre fin à notre enquête avec un résultat des plus insatisfaisants. Par conséquent, nous avons conclu que la plainte était fondée.

Le rapport de conclusions complet découlant de cette enquête est disponible sur notre site Web.

4.9 ATTEINTE À LA SÉCURITÉ DES DONNÉES

Le Commissariat invite les organisations à signaler volontairement les atteintes à la protection des renseignements personnels. Ces atteintes relèvent de trois grandes catégories.

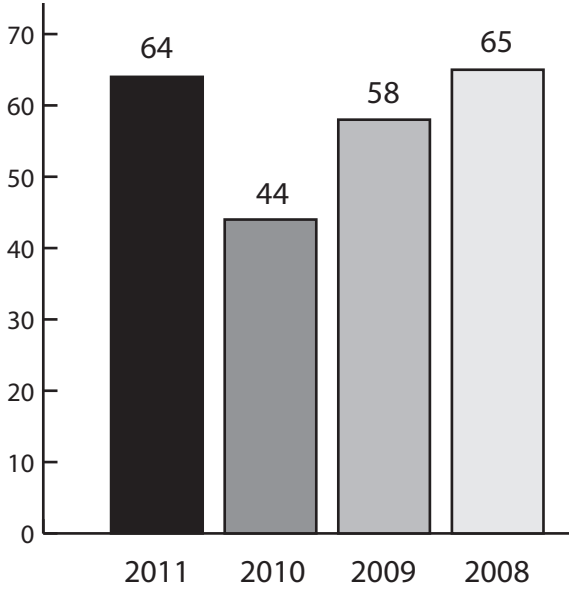
Communication accidentelle : Incidents dans le cadre desquels une organisation communique par accident des renseignements personnels à des personnes auxquelles ces renseignements ne sont pas destinés, par exemple, des relevés bancaires envoyés à la mauvaise adresse en raison d'une erreur mécanique ou humaine, ou des renseignements personnels rendus publics sur le site Web d'une organisation à la suite d'une erreur technique.

Perte : Incidents dans le cadre desquels des renseignements personnels sont perdus par une organisation, habituellement à la suite de la perte d'un ordinateur portatif, d'un CD ou de documents papier.

Accès, utilisation ou communication non autorisés : Incidents dans le cadre desquels une personne accède, utilise ou communique des renseignements personnels sans l'autorisation d'une organisation, par exemple, à la suite du vol d'un ordinateur portatif, du piratage en ligne de la base de données d'une organisation ou de l'accès ou de l'utilisation de renseignements personnels par un employé à des fins non autorisées.

En 2011, 64 atteintes à la protection des données dans le secteur privé nous ont été signalées volontairement.

Signalements volontaires des atteintes à la protection des données



Bien qu'il s'agisse d'une augmentation de 45 % par rapport au nombre d'incidents qui nous ont été signalés en 2010, cela demeure dans les limites des dernières années.

Le nombre de signalements provenant de l'industrie financière — le principal secteur à nous signaler régulièrement des atteintes — est demeuré stable, c'est-à-dire qu'il y a eu 29 incidents. Par contre, les signalements provenant de tous les autres secteurs ont plus que doublé, passant de 15 en 2010 à 35 en 2011.

Nous sommes heureux, car cela indique que la sensibilisation au fait qu'il est important de signaler les atteintes et aux avantages qui en découlent a dépassé le secteur financier et que l'ensemble du secteur privé canadien en est maintenant conscient.

L'importance du signalement des atteintes à la protection des données a davantage été mise de l'avant à la fin de 2010 et en 2011 à la suite de l'introduction en Alberta du signalement obligatoire des atteintes à la protection des données et de la préparation d'une loi fédérale visant à rendre obligatoire le signalement des atteintes à la commissaire à la protection de la vie privée.

Les responsables de la protection de la vie privée du secteur privé disent qu'ils prennent délibérément la décision de signaler préventivement les atteintes, même si la loi fédérale les obligeant à le faire n'a pas encore été adoptée. Nous les en félicitons.

Quand le Commissariat reçoit un signalement, il collabore avec le responsable de la protection de la vie privée de l'organisation pour faire en sorte que les mesures nécessaires soient prises et que les personnes touchées reçoivent de l'information pertinente et puissent faire part de leurs préoccupations. Cette collaboration peut se traduire par une diminution des plaintes adressées à la commissaire à la protection de la vie privée.

EXEMPLES D'AVIS D'INCIDENT SIGNALÉS AU CPVP

Site Web piraté

Un petit détaillant a remarqué que les numéros de carte de crédit et les adresses d'expédition de certains des clients de son site Web de commerce électronique avaient été compromis à la suite du piratage du site Web. Le détaillant a immédiatement fermé le site et avisé le Commissariat et la police. Il a aussi demandé à son fournisseur de paiements d'aviser toutes les sociétés émettrices de cartes de crédit concernées que l'intégrité des données avait été compromise. Le détaillant a de plus entrepris une vérification juricomptable, et les ventes du commerce électronique ont été suspendues jusqu'à ce que toutes les recommandations de la vérification visant à améliorer la sécurité aient été mises en œuvre.

Perte de CD contenant des données

Des CD contenant des renseignements personnels non chiffrés sur un nombre considérable de clients ont été perdus accidentellement, à l'interne, dans une institution financière. Même si rien ne laissait supposer que les données étaient tombées entre de mauvaises mains, l'institution financière a rapidement avisé le Commissariat et pris des mesures pour régler le problème. Ces mesures se rapportaient à trois aspects cruciaux de la réaction à une atteinte : a) limiter les répercussions en cherchant les CD perdus et en

mettant en place des mesures de surveillance accrue pour les comptes des clients touchés; b) aviser de l'incident tous les clients touchés; c) faire enquête et modifier les procédures pour qu'à l'avenir la politique de confidentialité de l'organisation (y compris en ce qui concerne le chiffrement) soit suivie.

Communication d'adresses de courriel

Un détaillant nous a signalé que deux de ses magasins avaient accidentellement envoyé des messages par courriel à un groupe de clients sans avoir préalablement caché les adresses de courriel de ces clients. Dans un cas, le nom et le numéro de téléphone d'un client étaient aussi indiqués dans le courriel envoyé à de nombreux autres clients. Le détaillant a réagi rapidement. Il a avisé les clients touchés quelques jours après l'incident et leur a présenté ses excuses. Le responsable de la protection de la vie privée de l'entreprise a aussi demandé à la direction régionale de faire enquête pour s'assurer que de tels courriels de masse n'étaient pas envoyés par d'autres magasins sans qu'on ait caché les adresses de courriel. La direction régionale a donné à nouveau de la formation aux employés des deux magasins concernés afin qu'ils soient bien au fait du protocole de l'entreprise pour protéger et cacher les renseignements personnels des clients lorsqu'ils communiquent par courriel.

CHAPITRE 5

Sensibiliser les Canadiennes et Canadiens

Indéniablement, le concept de protection de la vie privée est en train de se transformer, comme il l'a toujours fait au fil du temps.

La protection de la vie privée a peut-être déjà été assimilée principalement à l'exclusion, au droit de se couper du monde. Cependant, parmi la génération qui a grandi à l'ère des médias sociaux, beaucoup n'ont jamais vraiment connu l'isolement physique. Ces jeunes sont plus susceptibles d'associer la protection de la vie privée au fait de limiter l'accès que les autres ont aux renseignements qui les concernent.

La protection de la vie privée est devenue quelque chose d'assez compliqué. Il ne suffit plus de fermer une porte matérielle ou de se retirer à la campagne au fin fond des bois.

Aujourd'hui, les tentacules électroniques s'étendent jusqu'aux refuges les plus isolés. Pour trop de gens, ces tentacules sont invisibles. Elles recueillent des renseignements personnels des autos qui circulent dans les quartiers paisibles ou de logiciels malveillants installés furtivement dans leurs ordinateurs.

Comme la protection de la vie privée est plus importante que jamais et que la protection des renseignements personnels n'a jamais été aussi compliquée, le Commissariat consacre beaucoup d'efforts à la sensibilisation du public. Nous parlons aux gens de leur droit à la vie privée, de la façon dont ce droit est mis à l'épreuve et parfois même compromis, et de ce qu'ils peuvent faire pour remédier à la situation.

Nous nous adressons également aux entreprises pour les sensibiliser à leurs obligations en vertu de la LPRPDE et leur expliquer comment faire pour protéger de façon optimale les renseignements personnels des Canadiennes et Canadiens.

Les exposés que nous présentons lors de conférences et d'autres activités constituent un volet essentiel de notre programme de sensibilisation du public. En 2011, la commissaire, la commissaire adjointe et d'autres employés du CPVP ont fait plus de 140 discours et exposés. De plus, le Commissariat a présenté des expositions lors d'événements de haut niveau.

Les médias ont continué de beaucoup s'intéresser aux questions relatives à la protection de la vie privée, notamment celles qui touchent le monde virtuel. Le Commissariat essaie de remplir son mandat de sensibilisation du public par le biais des médias de masse traditionnels en acceptant autant de demandes d'entrevue qu'il le peut. En 2011, nous avons diffusé 37 communiqués de presse.

Pour ce qui est de la protection de la vie privée en ligne, nous mettons l'accent sur les compétences numériques. Nos efforts visent à aider les personnes à acquérir les compétences et les connaissances dont elles ont besoin pour protéger leurs renseignements personnels. Nous veillons également à ce que les entreprises fournissent à leurs clients les renseignements et les instruments dont ils ont besoin pour faire des choix éclairés en matière de protection de la vie privée.

Globalement, nos sites Web ont reçu 2 715 384 visites. Nous avons ajouté près de 500 abonnés à notre bulletin électronique.

Le Commissariat a créé un compte Twitter en 2010 et s'en est servi l'an dernier pour envoyer quelque 500 « gazouillis ».

Nous avons aussi fait la promotion croisée de notre présence sur Internet et dans les médias sociaux, et nous avons ajouté des codes QR (carrés contenant des taches d'encre qui peuvent être lues par les téléphones intelligents) aux documents imprimés, de manière à ce que les gens aient accès encore plus facilement et rapidement à nos documents de référence.

Le Commissariat a distribué environ 12 000 publications imprimées en 2011. Parmi elles, il y avait des documents publiés durant l'année, notamment les rapports annuels exigés par la LPRPDE et la *Loi sur la protection des renseignements personnels*, trois rapports de vérification et deux publications décrites plus en détail dans le présent chapitre : *La LPRPDE et votre pratique — Guide sur la protection de la vie privée à l'intention des avocats et Sondage sur les Canadiens et la protection de la vie privée, 2011*.

Les fiches d'information sont un moyen efficace d'informer les Canadiennes et Canadiens sur les nouveaux enjeux en matière de protection de la vie privée. Parmi les sujets des nouvelles fiches d'information ou des fiches révisées que le Commissariat a rendues disponibles cette année, mentionnons l'infonuagique, les témoins, la protection des renseignements personnels sur les

appareils mobiles et la publicité comportementale en ligne.

Les dessins humoristiques confèrent une touche de légèreté aux messages sérieux concernant la protection de la vie privée, et nous continuons d'utiliser ce genre de dessins, créés exclusivement pour nous, dans nos présentations et sur nos affiches, nos cartes postales et notre populaire calendrier.

Le présent chapitre fait un résumé de quelques-unes de nos principales activités de sensibilisation en 2011. Les informations concernant nos activités de sensibilisation destinées aux enfants et aux jeunes sont présentées au chapitre 2.

5.1 BUREAU DE TORONTO

Au terme de sa première année complète de fonctionnement, nous pouvons dire que le Bureau de Toronto du CPVP a facilité l'établissement de liens avec les entreprises, les associations industrielles, les universitaires et d'autres intervenants.

Le Bureau a été ouvert à l'automne 2010, en partant du principe qu'il faut aller là où l'action se déroule. L'analyse des plaintes déposées en vertu de la LPRPDE pendant une période de deux ans a révélé que 45 % des organisations mises en cause se trouvaient, ou avaient leur siège social, dans la région du Grand Toronto.

Comme beaucoup d'organisations et d'associations industrielles ont aussi leur siège social dans cette région, nous pouvons tirer parti des réseaux qu'elles ont créés, par le biais de présentations à leurs activités et, périodiquement, de rencontres personnelles.

Par exemple, en 2011, le Bureau de Toronto a mené 48 activités de sensibilisation auprès d'organisations et d'associations industrielles.

De plus, le Bureau a organisé des séances d'information pour des intervenants afin de favoriser un débat plus approfondi sur les nouveaux enjeux en matière de protection de la vie privée. L'essor de l'économie numérique a incité les entreprises à utiliser les progrès technologiques pour trouver de nouvelles façons de joindre les consommateurs.

Dans ce contexte, les séances d'information ont permis au CPVP et aux entreprises d'échanger des renseignements sur ces innovations. Grâce à une meilleure compréhension des questions législatives sous-jacentes, les entreprises seront en mesure de faire des choix plus éclairés lorsqu'il s'agit d'adopter des pratiques responsables en matière d'innovation et de protéger les renseignements personnels de leurs clients.

Enfin, étant donné qu'un bon nombre des organisations mises en cause sont établies dans la région du Grand Toronto, nous avons mené des enquêtes à partir du Bureau de Toronto afin d'améliorer l'efficience et la rapidité des services que nous offrons à la population canadienne.

5.2 OUTIL D'AUTO-ÉVALUATION À L'INTENTION DES ORGANISATIONS

En mai 2011, poursuivant leurs efforts concertés en vue de promouvoir des pratiques harmonisées et cohérentes en matière de protection de la vie privée, le CPVP et les Commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique ont lancé conjointement un instrument pour aider les organisations à comprendre ce qu'elles devaient faire pour protéger les renseignements personnels en leur possession et à évaluer leurs pratiques en cette matière.

Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations est un instrument interactif en ligne, qui comprend 17 éléments que les organisations peuvent évaluer. Ces éléments comprennent les politiques, la gestion des documents, la sécurité des réseaux, le contrôle de l'accès, la gestion des incidents et la planification de la continuité des opérations.

L'outil aide les organisations à déterminer sur quels éléments axer leurs efforts pour s'assurer que des mesures de sécurité raisonnables sont en place et qu'elles sont adéquates compte tenu de la quantité et de la nature délicate des renseignements personnels en leur possession.

Il aidera aussi les organisations à s'assurer que les mesures de sécurité tiennent compte des risques possibles qui pèsent sur cette information et des conséquences éventuelles si un incident se produisait. À notre avis, les responsables de la protection de la vie privée trouveront que cet outil est pratique pour véhiculer, dans leurs organisations respectives, le message que les renseignements personnels sont des actifs essentiels qui doivent être protégés.

5.3 SEMAINE DE LA PME — CYBERSÉCURITÉ

Un nombre toujours croissant de petites entreprises utilisent Internet pour attirer de nouveaux clients partout dans le monde et faciliter la vie de ceux qui sont plus proches d'elles. Le Commissariat a profité de l'occasion qu'offrait la Semaine de la petite entreprise, du 16 au 22 octobre 2011, pour fournir une foule de conseils pratiques sur la protection des renseignements des consommateurs et des clients contre les cybermenaces.

La confiance est un atout majeur pour les petites entreprises, et cette confiance est ébranlée lorsque les renseignements sur les consommateurs, les clients ou les employés sont volés ou altérés. Contrairement à la croyance populaire, la plupart des systèmes informatiques ne sont pas compromis par suite d'actes audacieux perpétrés par des génies et contre lesquels monsieur et madame Tout-le-monde sont sans défense.

Comme un cambrioleur qui vérifie d'abord s'il peut pénétrer dans une maison par une porte déverrouillée ou une fenêtre ouverte avant de forcer une serrure ou de fracasser une vitre, les pirates informatiques atteignent souvent leur objectif en exploitant les vulnérabilités courantes ou les « failles connues ».

Le CPVP a produit une série d'articles sur ces vulnérabilités courantes et les mesures que les petites entreprises peuvent adopter pour protéger leurs renseignements précieux. Voici quelques-uns des conseils donnés aux entreprises :

- protégez le réseau WiFi en omettant le nom et l'adresse de l'entreprise; activez le cryptage sans fil et choisissez un mot de passe long et compliqué;

- effectuez régulièrement des mises à jour des programmes antivirus et des autres logiciels et modifiez les mots de passe pour les services en ligne après quelques semaines d'utilisation;

- cryptez toutes vos données, qu'elles soient stockées sur des disques durs, dans des bases de données ou sur des clés USB, en utilisant éventuellement les options de chiffrement gratuit offertes par les systèmes d'exploitation courants;

- restez vigilant à l'égard de l'usurpation d'identité en ligne, notamment en faisant un appel téléphonique pour confirmer l'origine de courriels suspects;

- mettez en œuvre une politique en matière de sécurité des TI dans l'ensemble de l'entreprise.

Ces mesures constituent non seulement des pratiques commerciales avisées, avons-nous rappelé aux petites entreprises, mais les organisations ont aussi la responsabilité légale de protéger les renseignements personnels qu'elles recueillent.

En plus des activités conçues expressément pour la Semaine de la petite entreprise, le Commissariat a aussi organisé des expositions à l'intention des petites et moyennes entreprises lors de 10 événements; il a affiché une série de messages destinés aux PME sur son blogue et créé une présentation sur la conformité à la LPRPDE s'adressant aux PME.

5.4 SONDAGE AUPRÈS DES ENTREPRISES

Il est essentiel que le Commissariat sache à quel point les entreprises sont au fait des questions liées à la protection de la vie privée, quels types de politiques et de pratiques elles ont mises en place dans ce domaine et dans quelle mesure elles sont au courant des nouveaux enjeux.

Pour avoir une meilleure compréhension de ces questions, le CPVP a commandé en 2011 un sondage téléphonique auprès d'environ 1 000 entreprises qui sont assujetties à la LPRPDE. L'échantillon aléatoire comprenait de petites, de moyennes et de grandes entreprises.

Les personnes interrogées étaient des représentants qui connaissaient les politiques et les pratiques de leurs entreprises respectives en matière de protection de la vie privée, par exemple des propriétaires, des présidents-directeurs généraux ou des responsables de la protection de la vie privée. Un rapport résumant les résultats du sondage sera publié en 2012.

5.5 GUIDE À L'INTENTION DES AVOCATS

Comme les avocats sont confrontés à de nombreuses difficultés liées au traitement des renseignements personnels, le Commissariat a préparé un document d'orientation intitulé *La LPRPDE et votre pratique — Guide sur la protection de la vie privée à l'intention des avocats*. Le guide a été lancé en août 2011 à la Conférence juridique canadienne et exposition de l'Association du Barreau canadien, qui ont eu lieu à Halifax (Nouvelle-Écosse).

La LPRPDE et votre pratique : Guide sur la protection de la vie privée à l'intention des avocats

Notre guide vise à aider les avocats à respecter leurs obligations aux termes de la LPRPDE, le cas échéant, et traite de questions pratiques pouvant se poser dans la gestion d'un cabinet d'avocats et dans le cadre des litiges.

Le guide explique l'application potentielle de la LPRPDE dans les travaux juridiques quotidiens; il présente les pratiques exemplaires relativement à la gestion de la collecte, de l'utilisation et de la communication des renseignements personnels, et au traitement des demandes d'accès aux renseignements personnels.

La première partie du guide est consacrée aux questions liées à la protection de la vie privée auxquelles on est susceptible d'être confronté dans le cadre de la gestion de la pratique du droit, et la dernière partie examine les questions relatives à la protection de la vie privée qui peuvent surgir dans les litiges civils.

Nous espérons que ce guide aidera les avocats à considérer la protection de la vie privée non seulement comme une obligation légale, mais aussi comme une question de comportement éthique et respectueux au nom de la profession et des clients qu'ils représentent.

5.6 JOURNÉE DE LA PROTECTION DES DONNÉES 2011

Le 28 janvier 2011, à l'instar de nombreux autres pays, le Canada a souligné la Journée de la protection des données. Reconnue par les professionnels de la protection de la vie privée, les entreprises, les fonctionnaires, le milieu universitaire et les étudiants de par le monde, la Journée de la protection des données contribue à faire connaître les incidences de la technologie sur le droit à la vie privée et à promouvoir la protection de la vie privée.

En 2011, le Commissariat a créé le slogan *Le Net a la mémoire longue. Protégez vos renseignements personnels*. Utilisé dans divers types de documents, le slogan rappelait aux Canadiennes et Canadiens que, chaque fois qu'ils vont en ligne, ils se construisent une identité au moyen des activités auxquelles ils se livrent, ainsi que des mots et des images qu'ils diffusent.

Ce message a été accentué dans notre communiqué de la Journée de la protection des données, et les médias canadiens y ont fait écho. Le Commissariat a en outre organisé un tirage de prix en ligne et partagé des ressources liées à la Journée de la protection des données, comme des affiches et des fiches d'information, avec d'autres organismes de protection de la vie privée, y compris des organismes de réglementation.

5.7 SENSIBILISATION PARTOUT AU CANADA

À l'occasion de la rencontre qui a eu lieu à Québec à l'automne, les responsables de la protection de la vie privée des gouvernements fédéral, provinciaux et territoriaux ont convenu de se réunir régulièrement pour discuter de leurs activités de sensibilisation respectives.

Le matériel conçu pour la Journée de la protection des données a été envoyé aux Commissariats à la protection de la vie privée des provinces et des territoires qui, à leur tour, l'ont transmis à des institutions telles que des écoles et des autorités sanitaires régionales.

Le personnel du CPVP qui a voyagé à l'extérieur de la région d'Ottawa en 2011 a fait de grands efforts pour rencontrer les représentants des Commissariats à la protection de la vie privée des provinces et territoires. Lors d'activités comme des rencontres avec des chambres de commerce, nous nous sommes efforcés de faire participer nos homologues.

5.8 PROGRAMME DES CONTRIBUTIONS

Créé en 2004, le Programme des contributions s'est avéré très utile en fournissant des fonds à des projets de recherche de pointe et de sensibilisation du public portant sur la protection de la vie privée. Doté d'un budget annuel de 500 000 $, le Programme accorde jusqu'à 50 000 $ par projet.

En plus de faire progresser les connaissances, le Programme vise à aider les personnes et les organisations à mieux connaître et comprendre leurs droits et obligations en matière de protection de la vie privée, et à faciliter l'application pratique des résultats des recherches par les utilisateurs finals concernés.

En 2011, nous avons financé un large éventail de projets d'intérêt pour la population canadienne, notamment :

- une étude sur la façon dont les entreprises privées de sécurité utilisent les systèmes de caméras de surveillance, qui peuvent être installés pour des événements précis ou, pendant une certaine période, dans des points névralgiques (systèmes pouvant être déplacés); l'étude sera axée sur la collaboration entre les entreprises du secteur privé qui font de la collecte de données et les autorités responsables de l'application de la loi.

- la création d'un jeu multimédia, qui mettra à profit les espaces physiques et numériques pour renseigner les enfants canadiens sur la protection de la vie privée;

- la création d'une trousse interactive et éducative sur la protection des renseignements personnels à l'intention des enseignants;

- une étude sur les attentes en matière de protection de la vie privée des utilisateurs de sites de réseautage social, qui examinera dans quelle mesure ils estiment que les réseaux sociaux en ligne constituent vraiment des espaces « privés ».

Les recherches financées par le Programme des contributions sont menées indépendamment du CPVP.

Nous avons récemment adopté une nouvelle stratégie quinquennale pour le Programme en vue d'accroître ses retombées parmi les intervenants et au Canada en général. La stratégie repose sur ces six points :

1) **Augmenter notre influence grâce aux partenariats**
   Le CPVP invitera plusieurs organismes de financement gouvernementaux à s'associer à lui pour mieux utiliser les ressources financières disponibles et accroître l'incidence du financement. Ces partenariats permettront d'élargir le bassin de demandeurs potentiels dans différentes disciplines.

2) **Permettre le transfert et la mise en application des connaissances**
   Les demandeurs de financement seront invités à prévoir l'intégration d'initiatives de transfert

de connaissances dans leurs propositions de recherches. Le CPVP prévoit également organiser des symposiums sur le transfert des connaissances dans le cadre des prochaines années, dans le cadre desquels on présentera les recherches menées dans le cadre du Programme.

3) **Améliorer l'évaluation par des pairs**
Un système plus rigoureux d'évaluation par des pairs, auxquels s'ajouteraient des évaluateurs externes, sera établi pour faire en sorte que l'évaluation des projets de recherche et, au bout du compte, les recherches financées par le Programme soient de meilleure qualité.

4) **Faciliter l'accès par des améliorations techniques**
Des améliorations techniques, comme un système de demande en ligne et une base de données interrogeable pour les recherches, aideront les demandeurs et les utilisateurs à présenter une demande de financement ou à avoir accès aux connaissances obtenues grâce au Programme plus facilement.

5) **Évaluer le succès du Programme**
Un processus d'évaluation systématique sera mis en place afin de déterminer la pertinence des résultats des recherches et la fréquence de leur utilisation par les chercheurs, les médias et les autres intervenants.

6) **Renouveler notre stratégie de communication avec le public**
Le renouvellement de la stratégie de communication du Programme des contributions contribuera au retentissement des recherches et des connaissances émanant du Programme.

En mettant cette stratégie en œuvre, nous espérons que le Programme continuera de répondre aux besoins du CPVP et de la population canadienne en matière de recherche de pointe sur la promotion et la protection de la vie privée.

5.9 ALLOCUTIONS

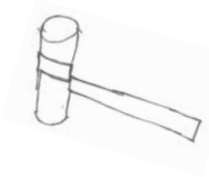
Les allocutions représentent un volet essentiel de la sensibilisation du public. Elles offrent au CPVP l'occasion de traiter directement de sujets qui intéressent plus particulièrement des groupes d'entreprises, des professionnels de la protection de la vie privée, des décideurs, des étudiants et d'autres segments de la population canadienne. Par ailleurs, les discours permettent à la commissaire, à la commissaire adjointe et au personnel de répondre directement aux questions qui préoccupent ces auditoires.

En 2011, nous avons participé à 143 activités. Nous étions présents au Sommet canadien sur la protection

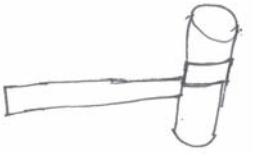
de la vie privée 2011, organisé par l'International Association of Privacy Professionals, à la Conférence Canada 3.0, organisée par le Canadian Digital Media Network, à la Conférence juridique canadienne et exposition de l'Association du Barreau canadien et à la Conférence sur le marketing et le droit, organisée par l'Association canadienne des annonceurs. Nous avons aussi pris la parole devant plusieurs groupes d'entreprises et à l'occasion d'événements organisés pour les petites et moyennes entreprises.

De nombreux discours sont disponibles sur notre site Web.

CHAPITRE 6



Devant les tribunaux



En 2011, le Commissariat a continué d'intervenir devant les tribunaux dans plusieurs causes de longue date.

Selon l'article 14 de la LPRPDE, un plaignant peut, après avoir reçu un rapport du Commissariat, demander une audience à la Cour fédérale pour toute question évoquée dans sa plainte ou dans le rapport de la commissaire, sous réserve de certaines restrictions.

La commissaire à la protection de la vie privée peut, avec le consentement du plaignant, comparaître en son nom, ou demander directement une audience à la Cour fédérale concernant cette même affaire (article 15 de la LPRPDE). La commissaire peut aussi demander à la Cour fédérale l'autorisation de comparaître comme partie à toute audience demandée par un plaignant.

Cette année, le Commissariat est parvenu à régler deux demandes émanant de la commissaire qui avaient été présentées au cours des dernières années. Une autre demande présentée aux termes de l'article 15 dans une année antérieure est toujours examinée par la Cour fédérale.

La commissaire à la protection de la vie privée intente régulièrement des poursuites lorsqu'une organisation refuse d'adopter ses recommandations à la suite de plaintes jugées fondées. Nous avons constaté que cela entraîne un degré élevé de conformité aux recommandations.

Conformément à l'esprit de notre mandat, nous avons respecté la vie privée des plaignants en ne mentionnant pas leur nom dans ce rapport.

DEMANDES DÉPOSÉES PAR LA COMMISSAIRE (ARTICLE 15 DE LA LPRPDE)

Numéro de dossier de la Cour fédérale : T-1275-10
Commissaire à la protection de la vie privée du Canada c. Association of American Medical Colleges

La commissaire à la protection de la vie privée a demandé une audience à la Cour fédérale en raison du refus de l'Association of American Medical Colleges (AAMC) de mettre un terme à la collecte de renseignements biométriques sensibles (empreintes digitales numériques, photographie numérique et renseignements sur le permis de

conduire) sur les candidats au Medical College Admissions Test (MCAT).

L'AAMC recueille ces renseignements pour garantir l'intégrité du MCAT et en raison d'allégations de fraude aux États-Unis et au Canada. L'AAMC, par l'entremise d'un tiers, recueille des empreintes digitales numériques et d'autres renseignements personnels sur les candidats au MCAT dans les centres d'examen. Les empreintes digitales sont converties en modèle numérique, mais les images sont conservées au cas où le modèle deviendrait corrompu.

Notre enquête portait sur la communication des motifs, la collecte, la conservation et les mesures de sécurité. Compte tenu des renseignements fournis en cours d'enquête, la commissaire a estimé qu'il existait des moyens portant moins atteinte à la vie privée de répondre aux besoins de l'AAMC en l'espèce.

En réponse au rapport de conclusions d'enquête préliminaire du Commissariat, l'AAMC a déclaré qu'elle réviserait le libellé de l'avis et du consentement en fonction de modifications à venir au sujet de l'utilisation des renseignements personnels. Elle a cependant ajouté qu'elle continuerait de recueillir les empreintes digitales des candidats et de scanner leur permis de conduire et leur photographie.

Le Commissariat a donc conclu que la plainte était fondée et résolue sur le plan de la communication des motifs, mais qu'elle restait fondée sur le plan de la collecte de renseignements.

En août 2010, la commissaire a déposé un avis de requête à la Cour fédérale pour lui demander à titre de redressement une ordonnance enjoignant à l'AAMC de trouver des moyens moins envahissants sur le plan de la protection de la vie privée de garantir l'intégrité de cet examen aux enjeux importants. Les parties ont déposé leurs affidavits et leurs pièces documentaires à la Cour à l'automne et à l'hiver 2010.

Au moment de la rédaction du présent rapport, l'affaire était toujours en instance devant la Cour fédérale.

Nota : Nous avons fait mention de cette affaire dans le rapport annuel de 2010.

Numéro de dossier de la Cour fédérale : T-1885-10
Commissaire à la protection de la vie privée c. Autorité aéroportuaire du Grand Toronto

La commissaire à la protection de la vie privée a présenté cette demande, qui concerne la collecte indue de renseignements personnels par une employée de l'Autorité aéroportuaire du Grand Toronto (GTAA) et le refus de la GTAA d'octroyer au plaignant l'accès aux renseignements personnels le concernant qui se trouvent sous le contrôle de celle-ci.

Le plaignant allègue notamment que son ex-épouse, une employée de la GTAA, aurait fait une utilisation inappropriée de l'équipement de la GTAA pour recueillir des photographies de lui et de sa famille alors qu'ils se trouvaient à l'aéroport international Pearson de Toronto. Le plaignant a fait

part à la GTAA de ses préoccupations concernant la protection de sa vie privée, et celle-ci a mené sa propre enquête interne. Le plaignant a également demandé à la GTAA l'accès à ses renseignements personnels. Insatisfait de la manière dont la GTAA a mené l'enquête et répondu à sa demande d'accès, le plaignant a porté plainte auprès du Commissariat. Nous avons jugé que la plainte était fondée et avons fait une requête en vertu de l'article 15 de la LPRPDE.

La demande adressée à la Cour soulevait, entre autres, la question de savoir si la GTAA avait omis de respecter ses obligations en vertu de la LPRPDE lorsque son employée avait recueilli et utilisé des renseignements personnels sur le plaignant à l'insu de celui-ci et sans son consentement. Elle soulevait également la question de savoir si la GTAA avait permis au plaignant d'avoir accès à tous les renseignements personnels le concernant qu'elle avait en sa possession.

En novembre 2011, nous avons conclu avec la GTAA un règlement négocié en vertu duquel la GTAA a fourni tous les renseignements personnels que lui avait demandés le plaignant. De plus, la GTAA a mis en place une procédure pour l'utilisation des caméras internes et rédigé un manuel sur leur utilisation.

Le Commissariat est heureux que la GTAA ait accepté de prendre des mesures pour garantir que le droit des passagers de l'aéroport à la protection de leur vie privée soit respecté.

Le plaignant a déposé un avis de requête distinct pour obtenir une audience devant la Cour fédérale concernant cette affaire, en vertu du paragraphe 14(1) de la LPRPDE. Le plaignant demandait diverses réparations, dont des dommages-intérêts. Au moment de la rédaction du présent rapport, ce dossier distinct n'était pas encore réglé.

Nota : Nous avons fait mention de cette affaire dans le rapport annuel de 2010.

Numéro de dossier de la Cour fédérale : T-243-10
Commissaire à la protection de la vie privée du Canada c. Sobeys

La commissaire à la protection de la vie privée s'est adressée à la Cour fédérale à la suite d'une plainte concernant la pratique de Sobeys de demander à tous les clients qui achètent des produits du tabac de présenter une pièce d'identité, quel que soit leur âge apparent.

En cours d'enquête, Sobeys a expliqué qu'elle avait adopté cette politique en Ontario afin de respecter les dispositions de la *Loi favorisant un Ontario sans fumée*. Cette loi interdit de vendre des produits du tabac aux personnes de moins de 19 ans et exige que les détaillants demandent une pièce d'identité aux personnes qui semblent avoir moins de 25 ans.

Le Commissariat a recommandé à Sobeys d'adopter d'autres procédures n'exigeant pas la production d'une pièce d'identité lorsque les clients ont manifestement

plus de 25 ans. Le Commissariat a par la suite déposé une demande auprès de la Cour fédérale réclamant une ordonnance selon laquelle Sobeys serait tenue de se conformer à sa recommandation.

À la suite des discussions ayant eu cours entre les parties, Sobeys a modifié sa politique sur les ventes de tabac en Ontario de sorte que les personnes qui ont visiblement l'âge légal pour acheter des produits du tabac seront, dans les circonstances appropriées, exemptées de l'exigence de présenter une pièce d'identité. Sobeys avisera ses clients en Ontario, au moyen d'un message sur son site Web public, qu'ils peuvent faire part au gérant du magasin de toute préoccupation relative aux exigences d'identification de la politique de l'entreprise.

La commissaire à la protection de la vie privée a déposé son avis de désistement le 31 mai 2011.

Nota : Nous avons fait mention de cette affaire dans le rapport annuel de 2010.

DEMANDES DE CONTRÔLE JUDICIAIRE PRÉSENTÉES EN VERTU DE L'ARTICLE 18.1 DE LA *LOI SUR LES COURS FÉDÉRALES*

Numéros de dossier de la Cour fédérale :
T-1587-11 et T-1588-11
X c. Commissaire à la protection de la vie privée du Canada

Le 27 septembre 2011, le requérant a présenté deux demandes de contrôle judiciaire, dans lesquelles il demandait la révision de deux rapports de conclusions rédigés par le Commissariat, qui concernaient ses plaintes.

Le requérant s'était plaint au Commissariat que le fournisseur de services d'orientation de son ancien employeur avait communiqué des renseignements à son employeur qui, à son tour, les avait communiqués aux autres employés, au médecin du requérant et à un médecin examinateur indépendant.

L'enquête du Commissariat a révélé que les plaintes n'étaient pas fondées. Le Commissariat a conclu que la communication de renseignements à l'employeur par le fournisseur de services d'orientation était autorisée aux termes d'un protocole d'entente que le requérant avait signé. En ce qui concerne la communication de renseignements par l'employeur, l'enquête a démontré que le requérant avait donné son consentement explicite ou implicite.

Le requérant allègue que la commissaire n'a pas observé les principes d'équité procédurale, qu'elle a rendu une décision fondée sur une conclusion de fait erronée et qu'elle a agi ou omis d'agir en raison d'une fraude ou de faux témoignages.

Au moment de la rédaction du présent rapport, l'affaire était toujours en instance devant la Cour fédérale.

CHAPITRE 7

Lois provinciales et territoriales essentiellement similaires à la loi fédérale

En vertu de l'alinéa 26(2)*b)* de la LPRPDE, le gouverneur en conseil peut exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la LPRPDE à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels dans une province dotée d'une loi essentiellement similaire à la LPRPDE.

Selon le paragraphe 25(1) de la LPRPDE, le Commissariat doit remettre tous les ans au Parlement un rapport sur « la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la loi fédérale.

Dans les rapports annuels antérieurs, nous avons rendu compte des lois du Québec, de l'Ontario (pour les renseignements personnels sur la santé), de l'Alberta et de la Colombie-Britannique, qui ont été déclarées essentiellement similaires.

Selon Industrie Canada, pour être reconnue comme étant essentiellement similaire, une loi provinciale ou territoriale doit :

- inclure les dix principes énoncés à l'annexe 1 de la LPRPDE;
- prévoir un mécanisme de surveillance et de recours indépendant et efficace comprenant le pouvoir d'enquêter;
- restreindre la collecte, l'utilisation et la communication de renseignements personnels à des fins appropriées ou légitimes.

Le 17 novembre 2011, la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (LAPRPS) du Nouveau-Brunswick a été déclarée essentiellement similaire à la LPRPDE. Par conséquent, les dépositaires de renseignements personnels sur la santé visés par la LAPRPS sont exclus de l'application de la partie 1 de la LPRPDE en ce qui concerne la collecte, l'utilisation et la communication de renseignements personnels sur la santé au Nouveau-Brunswick.

La LAPRPS a reçu la sanction royale le 19 juin 2009. Elle est entrée en vigueur le 1er septembre 2010.

La *Personal Health Information Act* (PHIA) de Terre-Neuve-et-Labrador, qui est entrée en vigueur le 1er avril 2011, n'avait pas, à la fin de 2011, été déclarée essentiellement similaire à la loi fédérale.

CHAPITRE 8

L'année à venir

« Il faut courir aussi vite que tu peux pour rester à la même place. » Ainsi se plaignait la Reine Rouge dans le conte de Lewis Carroll *De l'autre côté du miroir*.

La science s'est approprié cette image fantaisiste de l'hypothèse de l'évolution plus formelle de la Reine Rouge, qui soutient que l'adaptation continue d'une espèce est nécessaire pour lui permettre de conserver sa valeur sélective par rapport aux systèmes qui évoluent en parallèle.

Le CPVP peut être considéré comme un exemple concret de l'hypothèse de la Reine Rouge.

Le Commissariat doit continuer de courir le plus vite possible s'il veut seulement suivre le rythme de l'évolution rapide des technologies des communications et des pratiques sociétales qui génèrent de nouveaux défis en matière de protection de la vie privée et des renseignements personnels.

Au cours de la prochaine année, nous continuerons de raffermir notre compréhension des questions relatives à la protection de la vie privée soulevées dans le monde numérique en ligne, où de plus en plus de Canadiennes et Canadiens mènent une partie de leurs activités. Nous appliquerons cette expertise durement acquise pour aider les Canadiennes et Canadiens à acquérir de solides compétences numériques. Nous augmenterons notre utilisation des outils en ligne et d'autres moyens de communication pour sensibiliser le grand public sur le droit à la vie privée.

Voici quelques exemples concrets de notre évolution continue en 2012 :

INITIATIVES DE SENSIBILISATION DES JEUNES

Bande dessinée romanesque

Durant nos consultations de 2010, nous avons appris que les jeunes ont besoin d'une attention particulière parce qu'ils utilisent Internet de plus en plus jeunes et qu'ils fournissent des renseignements personnels sans savoir clairement comment et pourquoi ils seront utilisés. Le Commissariat a donc

convenu d'élaborer des manières créatives et novatrices de joindre les jeunes, ce qui a mené à l'idée d'une bande dessinée.

La bande dessinée comprendra entre 12 et 16 pages, en français et en anglais. Elle traitera de quelques enjeux concernant la protection de la vie privée, présentés sous forme de pages simples illustrées et d'impressions sur plusieurs pages. La bande dessinée ne portera pas seulement sur la protection de la vie privée dans le monde numérique; elle présentera des concepts et des idées nécessaires pour comprendre le fonctionnement de nos interfaces numériques et la façon dont celles-ci peuvent poser des problèmes technologiques qui risquent de nuire à la protection de la vie privée en ligne.

Le CPVP a embauché un auteur et un graphiste/illustrateur pour conjointement produire la bande dessinée, qui sera publiée, en ligne et en format papier, en 2012.

Des groupes de discussion formés de jeunes de 12 à 17 ans diront ce qu'ils pensent de la version préliminaire de la bande dessinée dans le cadre de séances organisées par un cabinet spécialisé en recherches sur l'opinion publique. On demandera également aux jeunes de dire ce qu'ils pensent du site Web du Commissariat destiné aux jeunes et, plus généralement, de la protection de la vie privée.

Davantage pour les jeunes

À la suite du lancement réussi de nos deux trousses de présentation pour les jeunes destinées aux élèves de 7e et 8e année ainsi qu'aux élèves de la 9e à la 12e année[2], nous lancerons une troisième trousse destinée aux élèves de la 4e à la 6e année.

2 Secondaire I et II et secondaire III à V au Québec.

Comme les premières trousses, celle-ci offrira les outils nécessaires pour permettre aux enseignants ou à d'autres adultes de présenter des exposés efficaces et attrayants dans les écoles ou la collectivité. L'objectif est d'expliquer aux jeunes des trois groupes d'âge que la technologie peut avoir une incidence sur leur vie privée, ainsi que de leur montrer comment se construire une identité en ligne de manière sécuritaire tout en protégeant leurs renseignements personnels.

En janvier 2012, le Commissariat a également lancé une version vidéo de la trousse, destinée aux élèves de la 8e à la 12e année, qui peut être consultée sur notre site Web principal, notre site Web conçu principalement pour les jeunes et notre canal YouTube.

Des vidéos sur la protection de la vie privée de nature différente seront à l'honneur en mars, lorsque des élèves de diverses écoles canadiennes qui participent au programme Rencontres du Canada voteront pour choisir les gagnants du quatrième concours national de vidéo *Ma vie privée et moi* à l'intention des jeunes. Ce concours invite les élèves de 12 à 18 ans à produire un message vidéo d'intérêt public d'une à deux minutes sur les questions relatives à la protection de la vie privée associées aux réseaux sociaux, aux appareils mobiles, au jeu en ligne ou à la cybersécurité.

Des prix sont remis à la meilleure vidéo pour chacun des quatre thèmes.

LOI ANTIPOURRIEL DU CANADA

Nous continuerons de collaborer avec Industrie Canada et nos partenaires d'application de la loi pour nous préparer à l'entrée en vigueur de la nouvelle loi. Par ailleurs, nous améliorerons nos capacités techniques et d'enquête à l'interne pour relever les défis liés à l'application de la loi.

LABORATOIRE TECHNOLOGIQUE

En 2012, le laboratoire technologique augmentera ses capacités en ajoutant du matériel et du personnel, principalement dans le but de relever les défis que pose la mise en œuvre de la nouvelle loi canadienne visant l'élimination des pourriels. En vertu de cette loi, le Commissariat a la responsabilité de faire enquête sur la collecte non autorisée de renseignements personnels, plus particulièrement la collecte d'adresses électroniques, et la collecte de renseignements personnels par le biais de l'accès illégal à des systèmes informatiques.

JOURNÉE DE LA PROTECTION DES DONNÉES

Fort du succès de l'édition de 2011, le CPVP insistera, à l'occasion de la Journée de la protection des données 2012, sur l'importance de limiter la quantité de renseignements personnels communiqués en ligne. Pendant la semaine qui précède le 28 janvier, nous participerons à diverses activités, y compris le lancement de nouveaux outils, ainsi que des exposés à l'intention des jeunes, des fonctionnaires, des entreprises et des employés. Le Commissariat élaborera de nouvelles ressources,

comme des affiches et des graphiques, qui peuvent favoriser la sensibilisation aux questions de protection des renseignements personnels dans toutes les organisations.

DISPOSITIONS LÉGISLATIVES TOUCHANT LA PROTECTION DE LA VIE PRIVÉE

Le deuxième examen parlementaire de la LPRPDE est prévu pour 2012. Des modifications nous permettraient de nous assurer que la *Loi* reste un moyen efficace de protéger la vie privée des Canadiennes et Canadiens.

ENQUÊTES

Le traitement des plaintes en vertu de la LPRPDE est au cœur du mandat du Commissariat. Nous avons déjà grandement accéléré le traitement des centaines de plaintes reçues chaque année.

Désormais, à compter de janvier 2012, nous adopterons des décisions modifiées avec des définitions actualisées. Ces nouvelles décisions refléteront plus fidèlement l'obligation des organisations de faire preuve de responsabilité en vertu de la *Loi*, tandis que les nouvelles définitions présenteront, en langage clair, la signification de chaque décision.

La principale modification est une approche révisée de la façon de déterminer qu'une question est « résolue ». À compter du 1er janvier 2012, nous réserverons l'utilisation de la conclusion « fondée et résolue » aux affaires où la plainte était fondée et où l'organisation a, au moment où une conclusion est rendue, pris la mesure corrective qui s'impose.

La conclusion « résolue » sera éliminée afin d'éviter la confusion entre cette conclusion et les décisions « réglée en cours d'enquête » et « réglée rapidement ».

Parallèlement, la nouvelle conclusion « fondée et conditionnellement résolue » s'appliquera désormais aux dossiers pour lesquels une organisation a pris un engagement ferme de démontrer sa mise en œuvre des mesures correctives dans un délai prescrit après la publication des conclusions du Commissariat. Ce libellé reflète que, dans certains cas, une organisation s'engage à traiter les questions relevées par le Commissariat, mais que tous les changements nécessaires ne peuvent pas être apportés immédiatement.

Lorsque nous utilisons cette conclusion, nous nous engageons à demander au mis en cause de nous informer, selon un calendrier établi après l'enquête, si une mesure corrective a été prise, à des fins d'évaluation.

Par ailleurs, nous demanderons aux entreprises de confirmer si elles se sont conformées à nos recommandations. À cette fin, elles devront faire réaliser à leurs frais par une tierce partie une vérification indépendante en respectant un échéancier précis.

Voici les nouvelles décisions et leurs définitions :

Non fondée : L'enquête n'a pas permis de déceler les éléments de preuve donnant à penser qu'une

organisation a enfreint la LPRPDE ou de déceler assez d'éléments de preuve à cette fin.

Fondée et conditionnellement résolue : La commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE. L'organisation s'est engagée à mettre en œuvre les recommandations formulées par la commissaire et à faire la démonstration de cette mise en œuvre dans les délais prescrits.

Fondée et résolue : La commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE. L'organisation a démontré qu'elle avait pris des mesures correctives satisfaisantes pour remédier à la situation, soit de sa propre initiative, soit à la suite de recommandations formulées par la commissaire, au moment où la conclusion a été rendue.

Fondée : La commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE.

Réglée rapidement : Le Commissariat a aidé à négocier une solution satisfaisante pour toutes les parties concernées sans qu'une enquête officielle n'ait été entreprise. La commissaire ne produit pas de rapport.

Réglée en cours d'enquête : Le Commissariat aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. La commissaire ne produit pas de rapport.

Mettre fin à l'examen : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. À sa discrétion, la commissaire peut mettre fin à l'examen de la plainte pour un motif prévu au paragraphe 12.2(1) de la LPRPDE, à la demande du plaignant ou lorsqu'il a renoncé à la plainte.

Refus d'enquêter : La commissaire a refusé de procéder à une enquête relative à une plainte parce qu'elle était d'avis que le plaignant aurait d'abord dû épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; que la plainte pourrait avantageusement être instruite selon des procédures prévues par le droit fédéral ou le droit provincial; que la plainte n'a pas été déposée dans un délai raisonnable après que son objet a pris naissance, conformément au paragraphe 12(1) de la LPRPDE.

Hors du champ d'application : À la lumière des données préliminaires recueillies, on a déterminé que la LPRPDE ne s'appliquait pas à l'organisation ou à l'activité faisant l'objet de la plainte. La commissaire ne produit pas de rapport.

DÉMÉNAGEMENT EN 2013

Au cours des 18 prochains mois, le CPVP préparera le déménagement, durant l'été 2013, de ses bureaux du centre-ville d'Ottawa à Gatineau, de l'autre côté de la rivière, au Québec. Nos bureaux d'Ottawa accueillent actuellement 95 % de nos employés. Ce déménagement est l'occasion de s'installer dans un nouvel immeuble à la fine pointe de la technologie et ayant obtenu une certification environnementale.

Annexe 1

DÉFINITIONS

DÉFINITIONS DES TYPES DE PLAINTES DÉPOSÉES EN VERTU DE LA LPRPDE

Les plaintes adressées au Commissariat sont réparties selon les principes et les dispositions de la LPRPDE qui auraient été enfreints :

Accès. Une personne s'est vu refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements, soit en raison d'une exception dont l'organisation s'est prévalue pour retrancher les renseignements.

Collecte. Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.

Consentement. Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans un consentement valable de la personne concernée ou elle a exigé que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels comme condition à l'obtention des biens ou des services.

Conservation. Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins qu'une organisation a déclarées au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.

Correction/Annotation. L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.

Délais. Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la *Loi*.

Exactitude. Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont exacts, complets et à jour.

Frais. Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.

Mesures de sécurité. Une organisation n'a pas protégé les renseignements personnels qu'elle détient par des mesures de sécurité appropriées.

Possibilité de porter plainte. Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la *Loi* ou elle a enfreint ses propres procédures et politiques.

Responsabilité. Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou dont elle a la garde ou elle a omis de désigner une personne responsable d'assurer le respect de la *Loi*.

Transparence. Une organisation a omis de rendre facilement accessibles aux personnes des renseignements précis sur ses pratiques et politiques en matière de gestion des renseignements personnels.

Utilisation et communication. Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles pour lesquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la *Loi*.

DÉFINITIONS DES CONCLUSIONS ET AUTRES DÉCISIONS

Le Commissariat a élaboré des définitions de conclusions et de décisions afin d'expliquer les résultats des enquêtes effectuées conformément à la LPRPDE. Les définitions en place à la fin de 2011 figurent ci-dessous.

À compter de janvier 2012, nous adopterons des décisions modifiées avec des définitions actualisées. Ces nouvelles décisions refléteront plus fidèlement l'obligation des organisations de faire preuve de responsabilité en vertu de la *Loi*, tandis que les nouvelles définitions présenteront, en langage clair, la signification de chaque décision. Pour une description du nouvel ensemble de décisions et définitions, veuillez vous reporter au chapitre « L'année à venir ».

Non fondée. L'enquête n'a pas permis de déceler les éléments de preuve donnant à penser qu'une organisation a enfreint la LPRPDE ou de déceler assez d'éléments de preuve à cette fin.

Fondée. L'organisation a contrevenu à une disposition de la LPRPDE.

Résolue. L'enquête a corroboré les allégations, mais avant la fin de l'enquête, l'organisation a pris des mesures correctives pour remédier à la situation, à la satisfaction du Commissariat, ou s'est engagée à prendre ces mesures.

Fondée et résolue. La commissaire est d'avis, au terme de son enquête, que les allégations semblent fondées sur des preuves, mais fait une recommandation à l'organisation concernée avant de rendre ses conclusions, et l'organisation prend ou s'engage à prendre les mesures correctives recommandées.

Réglée en cours d'enquête. Le Commissariat aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. Aucune conclusion n'est rendue.

Mettre fin à l'examen. Il s'agit d'une enquête qui a pris fin avant que toutes les allégations ne soient pleinement examinées. Une enquête peut être abandonnée à la demande du plaignant ou lorsqu'il a renoncé à la plainte. **Par ailleurs,** en date du 1er avril 2011, date de l'entrée en vigueur des modifications à la LPRPDE, une enquête peut être abandonnée à la discrétion de la commissaire pour un motif prévu au paragraphe 12.2(1) de la LPRPDE.

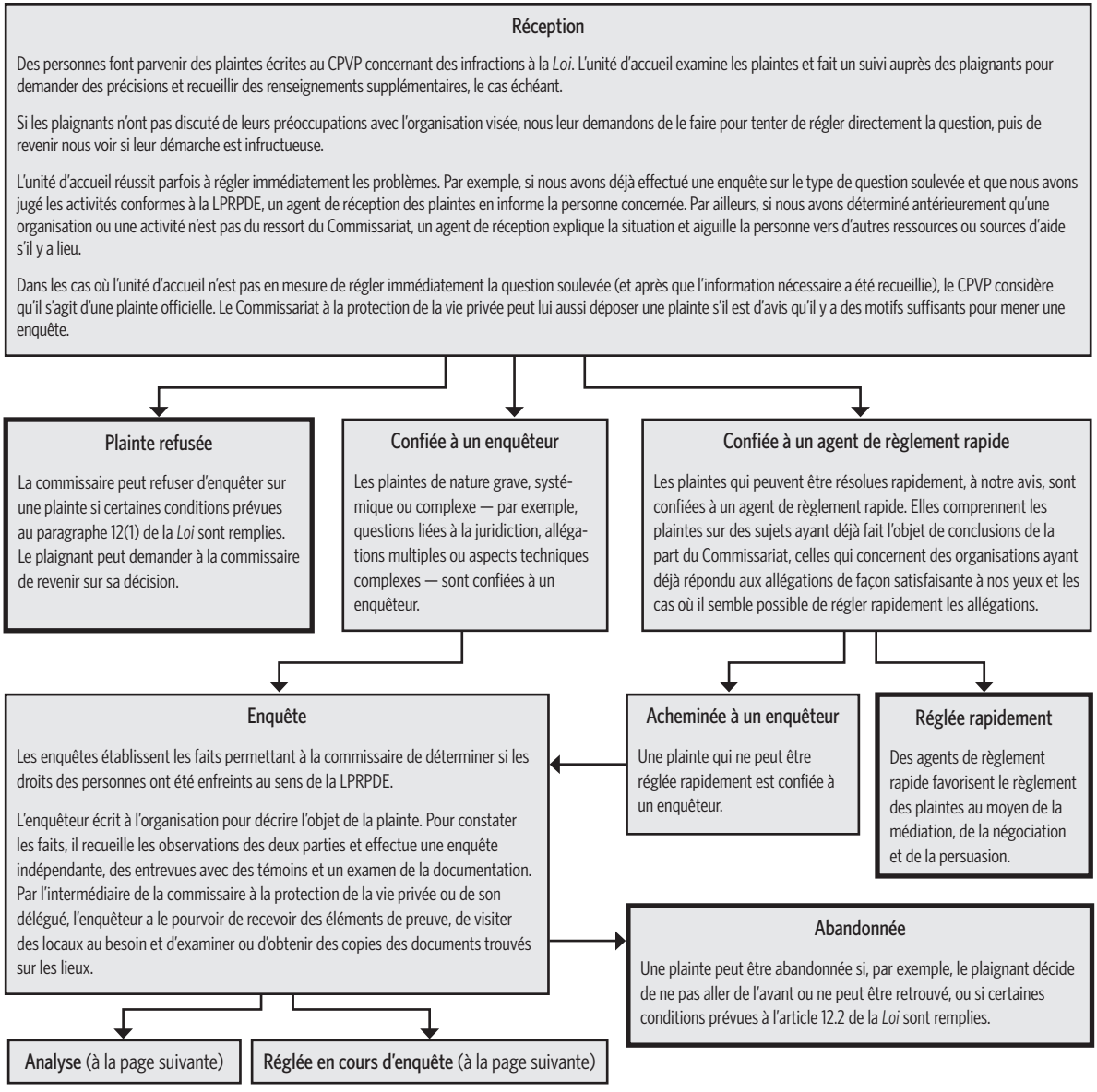
Hors du champ d'application. L'enquête a démontré que la LPRPDE ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.

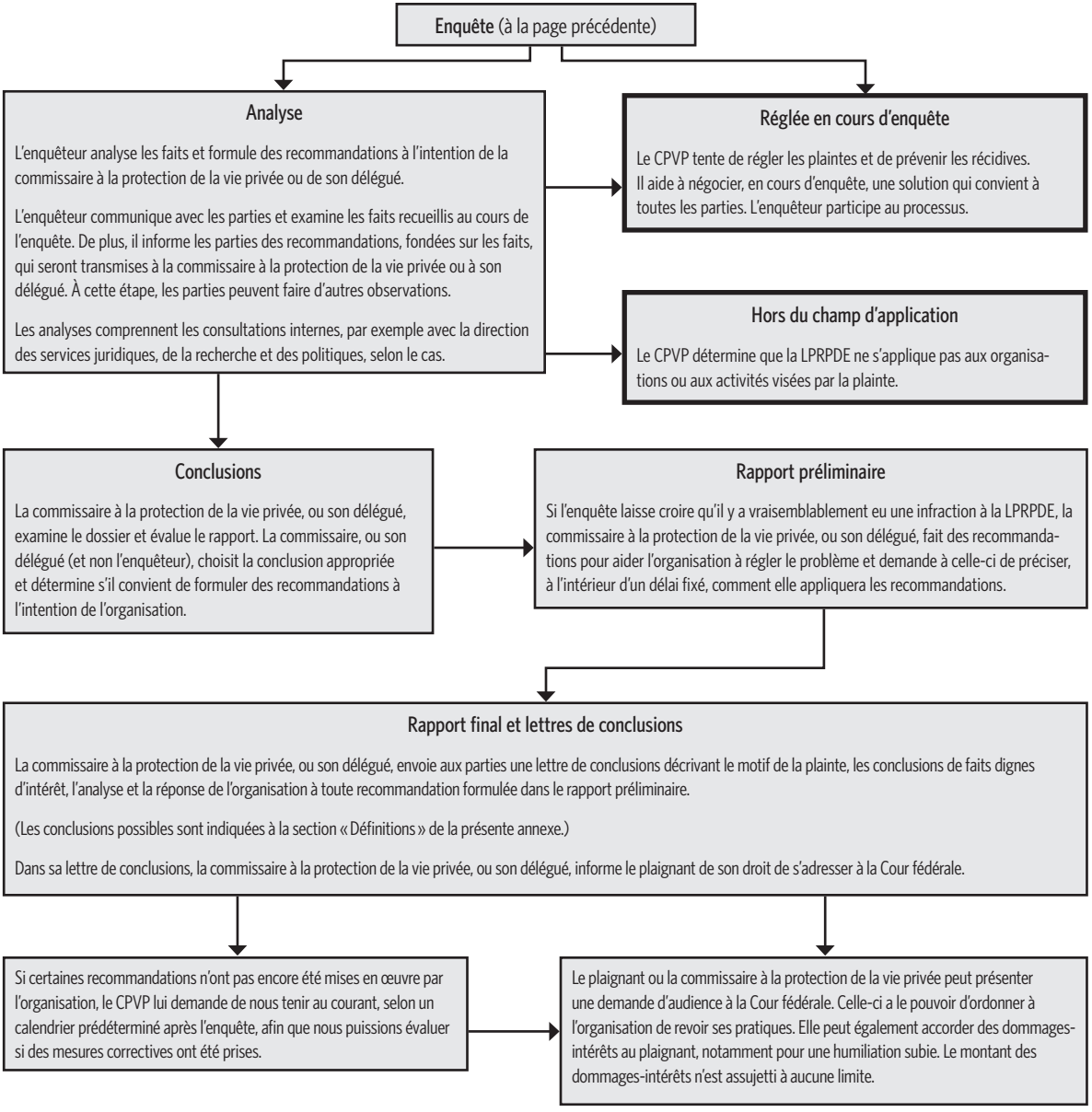
Réglée rapidement. Situation dans laquelle l'affaire est réglée avant même qu'une enquête officielle ne soit entreprise. À titre d'exemple, si une personne dépose une plainte concernant un sujet qui a déjà fait l'objet d'une enquête par le Commissariat et qui a été jugé conforme à la LPRPDE, nous lui fournirons les explications nécessaires. Cette conclusion s'applique également lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du Commissariat.

Aucun rapport produit aux termes du paragraphe 13(2). ***Nota : Cette décision était seulement appliquée aux enquêtes terminées avant le 1er avril 2011, au moment où le paragraphe 13(2) de la LPRPDE a été abrogé.*** La commissaire n'est pas tenue de rédiger un rapport si certaines conditions sont remplies : a) le plaignant devrait d'abord épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; b) la plainte pourrait être avantageusement instruite, dans un premier temps ou à toutes les étapes, selon des procédures prévues par le droit fédéral ou le droit provincial; c) le délai écoulé entre la date où l'objet de la plainte a pris naissance et celle du dépôt de celle-ci est tel que le rapport serait inutile; d) la plainte est futile, vexatoire ou entachée de mauvaise foi. Si la commissaire décide de ne pas rédiger de rapport, elle en informe le plaignant et l'organisation, en précisant les motifs.

Refus d'enquêter. ***Nota : Cette décision n'a été utilisée que pour les plaintes reçues après le 1er avril 2011, date d'entrée en vigueur du paragraphe 12(1) révisé de la LPRPDE.*** La commissaire a refusé de procéder à une enquête relative à une plainte parce qu'elle était d'avis que le plaignant aurait d'abord dû épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; que la plainte pourrait avantageusement être instruite selon des procédures prévues par le droit fédéral ou le droit provincial; que la plainte n'a pas été déposée dans un délai raisonnable après que son objet a pris naissance, conformément au paragraphe 12(1) de la LPRPDE.

PROCESSUS D'ENQUÊTE




Enquête (à la page précédente)
Analyse
L'enquêteur analyse les faits et formule des recommandations à l'intention de la commissaire à la protection de la vie privée ou de son délégué.
L'enquêteur communique avec les parties et examine les faits recueillis au cours de l'enquête. De plus, il informe les parties des recommandations, fondées sur les faits, qui seront transmises à la commissaire à la protection de la vie privée ou à son délégué. À cette étape, les parties peuvent faire d'autres observations.
Les analyses comprennent les consultations internes, par exemple avec la direction des services juridiques, de la recherche et des politiques, selon le cas.
Réglée en cours d'enquête
Le CPVP tente de régler les plaintes et de prévenir les récidives. Il aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. L'enquêteur participe au processus.
Hors du champ d'application
Le CPVP détermine que la LPRPDE ne s'applique pas aux organisations ou aux activités visées par la plainte.
Conclusions
La commissaire à la protection de la vie privée, ou son délégué, examine le dossier et évalue le rapport. La commissaire, ou son délégué (et non l'enquêteur), choisit la conclusion appropriée et détermine s'il convient de formuler des recommandations à l'intention de l'organisation.
Rapport préliminaire
Si l'enquête laisse croire qu'il y a vraisemblablement eu une infraction à la LPRPDE, la commissaire à la protection de la vie privée, ou son délégué, fait des recommandations pour aider l'organisation à régler le problème et demande à celle-ci de préciser, à l'intérieur d'un délai fixé, comment elle appliquera les recommandations.
Rapport final et lettres de conclusions
La commissaire à la protection de la vie privée, ou son délégué, envoie aux parties une lettre de conclusions décrivant le motif de la plainte, les conclusions de faits dignes d'intérêt, l'analyse et la réponse de l'organisation à toute recommandation formulée dans le rapport préliminaire.
(Les conclusions possibles sont indiquées à la section « Définitions » de la présente annexe.)
Dans sa lettre de conclusions, la commissaire à la protection de la vie privée, ou son délégué, informe le plaignant de son droit de s'adresser à la Cour fédérale.
Si certaines recommandations n'ont pas encore été mises en œuvre par l'organisation, le CPVP lui demande de nous tenir au courant, selon un calendrier prédéterminé après l'enquête, afin que nous puissions évaluer si des mesures correctives ont été prises.
Le plaignant ou la commissaire à la protection de la vie privée peut présenter une demande d'audience à la Cour fédérale. Celle-ci a le pouvoir d'ordonner à l'organisation de revoir ses pratiques. Elle peut également accorder des dommages-intérêts au plaignant, notamment pour une humiliation subie. Le montant des dommages-intérêts n'est assujetti à aucune limite.

Annexe 2

STATISTIQUES SUR LES ENQUÊTES LIÉES À LA LPRPDE POUR 2011

Nota : Les pourcentages ayant été arrondis, leur somme peut ne pas être égale à 100.

Dans l'ensemble de 2011, le Commissariat a accepté 281 plaintes officielles, une augmentation de 35 % par rapport aux 207 plaintes reçues en 2010. Cette augmentation est probablement liée à divers facteurs, comme la complexité croissante des enjeux en matière de protection de la vie privée auxquels sont confrontés les Canadiennes et Canadiens (ce qui mène à un plus grand nombre de plaintes officielles), une possible sensibilisation accrue parmi les Canadiennes et Canadiens à leur droit à la vie privée ou des changements à la façon dont les personnes interagissent avec les entreprises dans l'économie de plus en plus numérique.

Plaintes reçues par secteur d'activité

	2011		2010		2009	
Secteur	**Nombre**	**Pourcentage**	**Nombre**	**Pourcentage**	**Nombre**	**Pourcentage**
Secteur financier	62	22 %	45	22 %	55	24 %
Transport	34	12 %	13	6 %	15	6 %
Télécommunications	30	11 %	19	9 %	42*	18 %
Services	28	10 %	35	17 %	9	4 %
Assurance	25	9 %	27	13 %	41	18 %
Hébergement	24	9 %	6	3 %	7	3 %
Internet	18	6 %	19	9 %	—	—
Vente/Détail	16	6 %	18	9 %	25	11 %
Divertissement	8	3 %	2	1 %	0	0 %
Services professionnels	7	3 %	6	3 %	10	4 %
Santé	4	>1 %	4	2 %	8	3 %
Autres	25	9 %	13	6 %	19	8 %
Total	281		207		231	

*En 2010, nous avons commencé à comptabiliser les plaintes relatives à Internet comme un secteur distinct. Antérieurement, les plaintes relatives à Internet étaient comptabilisées sous le secteur des télécommunications.

Les plaintes liées au secteur financier continuent de représenter la plus importante proportion de plaintes officielles que nous acceptons, environ une sur cinq.

Les plaintes dans le secteur des transports ont grimpé cette année comparativement aux années précédentes. Nous entendons examiner cette tendance possible de près au cours des prochains mois.

Les plaintes relevant du secteur de l'assurance ont baissé au cours des deux dernières années. Cela peut s'expliquer par le fait que, durant cette période, nous avons constaté une augmentation de la clarté et des connaissances en ce qui concerne les règles de protection de la vie privée dans le secteur de l'assurance.

DÉFINITIONS DES SECTEURS D'ACTIVITÉ

- **Secteur financier :** banques, intermédiation financière (p. ex. société émettrice de cartes de crédit, financement des ventes, prêts à la consommation, courtiers hypothécaires, activités de traitement des transactions financières), investissement financier et activités connexes, planification et investissement financiers, autorités monétaires.

- **Services :** organisations civiques et professionnelles, services de soins personnels, services de réparation et de maintenance, programmes de récompense, services administratifs et de soutien (comprend les agences de recouvrement et les agences d'évaluation du crédit), services éducatifs et aide sociale.

- **Internet :** traitement des données, hébergement Web et services connexes, fournisseurs de services Internet, réseaux sociaux et portails de recherche Web.

- **Assurance :** sociétés d'assurance (responsabilité, vie, maladie, dommages et décès).

- **Vente/Détail :** concessionnaires d'automobiles, vente de matériaux de construction et de fournitures, marketing direct, commerce électronique, vente au détail (en magasin et en ligne).

- **Services professionnels :** comptabilité, préparation de déclarations de revenus tenue de comptes et services de la paie, services juridiques, autres services professionnels, scientifiques et techniques.

- **Transport :** aérien, ferroviaire, transport en commun et transport terrestre de voyageurs, camionnage, transport par voie d'eau.

- **Télécommunications :** applications mobiles, entreprises de télécommunications par satellite, équipement de télécommunications, entreprises de télécommunications câblées ou sans fil.

- **Hébergement :** associations de condominiums, coopératives d'habitation, services immobiliers, logements locatifs et hébergement des voyageurs.

- **Santé :** médecins, dentistes, pharmaciens et autres professionnels de la santé.

- **Divertissement :** industries du divertissement, du jeu et des loisirs et autres services de divertissement.

- **Autres :** industries manufacturières, agriculture, services publics, hors du champs d'application, diffuseurs (excepté Internet), alimentation et boissons, et entités gouvernementales qui relèvent du champ d'application de la LPRPDE.

Plaintes reçues par type de plainte

	2011		2010		2009	
Type	**Nombre**	**Pourcentage**	**Nombre**	**Pourcentage**	**Nombre**	**Pourcentage**
Utilisation et communication	89	32 %	56	27 %	59	26 %
Accès	74	26 %	50	24 %	64	28 %
Collecte	57	20 %	33	16 %	33	14 %
Consentement	19	7 %	30	14 %	22	10 %
Correction/Annotation	14	5 %	1	>1 %	1	>1 %
Conservation	10	4 %	10	5 %	3	1 %
Mesures de sécurité	9	3 %	13	6 %	21	9 %
Responsabilité	4	1 %	—	—	—	—
Exactitude	3	1 %	4	2 %	9	4 %
Possibilité de porter plainte	1	>1 %	2	1 %	2	>1 %
Frais	1	>1 %	—	—	—	—
Transparence	0	0 %	3	1 %	4	2 %
Détermination des fins de la collecte	0	0 %	2	1 %	0	0 %
Fins appropriées	0	0 %	1	>1 %	0	0 %
Autres	—	—	2	1 %	13	6 %
Total	281		207		231	

L'utilisation et la communication de renseignements personnels, l'accès aux renseignements personnels et la collecte de renseignements personnels ont été, une fois de plus, les trois principales questions soulevées dans les plaintes adressées au Commissariat.

Plaintes fermées par type de plainte et décision

	Réglée rapidement	Non fondée	Hors du champ d'application	Abandonnée	Fondée et résolue	Fondée	Résolue	Réglée en cours d'enquête	Aucun rapport produit aux termes du paragr. 13(2)	Refus d'enquêter	**Total**	**Pourcentage**
Accès	33	11	6	5	4	2	4	1	2	1	**69**	**29 %**
Utilisation et communication	38	7	7	4	3	3	2	1	1	0	**66**	**28 %**
Collecte	23	5	4	5	3	2	1	1	0	0	**44**	**19 %**
Consentement	5	7	0	2	2	2	2	1	0	0	**21**	**9 %**
Mesures de sécurité	8	2	1	1	1	1	3	0	0	0	**17**	**7 %**
Conservation	5	0	0	0	0	0	0	0	0	0	**5**	**2 %**
Correction/ Annotation	4	0	0	0	0	0	0	1	0	0	**5**	**2 %**
Exactitude	0	0	0	0	2	1	0	1	0	0	**4**	**2 %**
Possibilité de porter plainte	0	3	0	0	0	0	0	0	0	0	**3**	**1 %**
Détermination des fins de la collecte	0	0	0	0	0	1	0	0	0	0	**1**	**>1 %**
Transparence	0	0	0	0	0	1	0	0	0	0	**1**	**>1 %**
Total	**116**	**35**	**18**	**17**	**15**	**13**	**12**	**6**	**3**	**1**	**236**	
Pourcentage	**49 %**	**15 %**	**8 %**	**7 %**	**6 %**	**6 %**	**5 %**	**3 %**	**1 %**	**>1 %**		

En 2011, nous avons traité 125 dossiers pour règlement rapide. Nous avons résolu de façon satisfaisante 116 de ces dossiers. Les neuf autres dossiers ont été transférés pour enquête officielle. Nous sommes ravis d'avoir conservé un très haut taux de résolution, soit plus de 90 %.

Nous avons enregistré une augmentation notable du nombre de plaintes traitées par le biais de ce processus — près de la moitié de toutes les plaintes officielles, contre environ le quart en 2010.

Nous avons également effectué 120 enquêtes sur des plaintes. Le nombre de plaintes conclues est nettement moins élevé qu'en 2010, année durant laquelle nous avons terminé 249 enquêtes, dans le cadre de notre projet de deux ans pour éliminer l'arriéré de plaintes.

Plaintes fermées par secteur d'activité et décision

	Réglée rapidement	Non fondée	Hors du champ d'application	Abandonnée	Fondée et résolue	Fondée	Résolue	Réglée en cours d'enquête	Aucun rapport produit aux termes du paragr. 13(2)	Refus d'enquêter	**Total**	**Pourcentage**
Secteur financier	20	13	0	6	3	4	3	2	1	0	**52**	**22 %**
Assurance	10	4	9	2	1	1	2	0	2	1	**32**	**14 %**
Services	10	5	2	2	3	1	2	1	0	0	**26**	**11 %**
Télécommunications	16	4	0	2	0	0	0	0	0	0	**22**	**9 %**
Transport	13	1	0	0	1	2	3	1	0	0	**21**	**9 %**
Vente/Détail	11	2	1	0	5	0	1	0	0	0	**20**	**8 %**
Internet	5	6	0	4	0	4	1	0	0	0	**20**	**8 %**
Hébergement	10	0	0	0	2	0	0	0	0	0	**12**	**5 %**
Services professionnels	4	0	3	0	0	0	0	0	0	0	**7**	**3 %**
Santé	3	0	0	0	0	0	0	0	0	0	**3**	**1 %**
Divertissement	2	0	0	0	0	0	0	1	0	0	**3**	**1 %**
Autres	12	0	3	1	0	1	0	1	0	0	**18**	**8 %**
Total	**116**	**35**	**18**	**17**	**15**	**13**	**12**	**6**	**3**	**1**	**236**	
Pourcentage	**49 %**	**15 %**	**8 %**	**7 %**	**6 %**	**6 %**	**5 %**	**3 %**	**1 %**	**>1 %**		

Dans la majorité des enquêtes, nous avons réussi à trouver une solution satisfaisante. Seulement 6 % des enquêtes officielles ont été jugées fondées (mais non résolues), ce qui signifie que nous n'avons pu trouver de solution acceptable.

Nous avons noté une importante diminution de la proportion des cas jugés résolus ou fondés et résolus. Ces dossiers ont diminué des deux tiers, passant de 33 % de tous les cas en 2010 à seulement 11 % en 2011. Cette diminution était presque complètement compensée par l'augmentation de la proportion des cas résolus par règlement rapide, qui a plus que doublé, passant de 24 % en 2010 à 49 % en 2011.

En 2011, nous avons enregistré une augmentation du nombre de plaintes pour lesquelles nous avons conclu que la LPRPDE ne s'appliquait pas à l'organisation ou à l'activité faisant l'objet de la plainte, soit 8 % des plaintes par rapport à 2 % l'année précédente.

Cette hausse est en partie attribuable à une décision de la Cour fédérale en 2010 sur la portée de l'application de la LPRPDE lorsque les renseignements personnels sont recueillis pour défendre une personne assurée dans une réclamation en responsabilité civile découlant d'un accident d'automobile. Par la suite, quelques plaintes ont été fermées parce qu'elles avaient été reçues avant cette décision et concernaient des activités pour lesquelles la Cour a déterminé que la LPRPDE ne s'applique pas.

DÉLAIS DE TRAITEMENT

Délais de traitement moyens par type de plainte et de règlement

	Règlement rapide		Plaintes officielles	
Type de plainte	**Nombre**	**Délai de traitement moyen en mois**	**Nombre**	**Délai de traitement moyen en mois**
Accès	33	2	36	17
Exactitude	0	—	4	18
Possibilité de porter plainte	0	—	3	13
Collecte	23	2	21	12
Consentement	5	2	16	11
Correction/Annotation	4	2	1	3
Détermination des fins de la collecte	0	—	1	12
Transparence	0	—	1	21
Conservation	5	2	0	—
Mesures de sécurité	8	3	9	19
Utilisation et communication	38	1	28	13
	Total 116	**Moyenne pondérée* 2,0**	**Total 120**	**Moyenne pondérée* 14,3**

*Une moyenne pondérée est calculée en multipliant le nombre de plaintes de chaque type par le délai de traitement moyen pour ce type de plainte, en additionnant ces chiffres et en divisant le total par le nombre total de plaintes. La moyenne pondérée constitue une statistique représentative des délais de traitement globaux.

En 2011, compte tenu de l'élimination de notre arriéré de plaintes et du recours accru au règlement rapide, nous avons pu retourner à nos niveaux de dotation de 2008 et quand même accélérer le règlement de nos enquêtes.

Le délai moyen des enquêtes officielles a baissé de plusieurs mois pour atteindre 14 mois. Par ailleurs, les plaintes résolues par règlement rapide ont été réglées dans un délai de deux mois suivant leur acceptation.

Dans l'ensemble, le délai de traitement moyen pour toutes les plaintes acceptées a diminué pour atteindre un peu plus de huit mois, ce qui est nettement inférieur à la période de 12 mois énoncée dans la LPRPDE.

Délais de traitement moyens par décision

Décision	Nombre	Délai de traitement moyen (en mois)
Réglée rapidement	116	2
Réglée en cours d'enquête	6	6
Abandonnée	17	7
Refus d'enquêter	1	3
Hors du champ d'application	18	23
Aucun rapport produit aux termes du paragr. 13(2)	3	23
Non fondée	35	14
Fondée et résolue	15	15
Résolue	12	13
Fondée	13	16
Total	**236**	**Moyenne pondérée 8,2**

Tel que nous dans le rapport annuel de 2010, nous utilisons une nouvelle définition de délai de traitement dans le présent rapport. Les délais de traitement sont désormais calculés à compter de la date d'acceptation d'une plainte et jusqu'à ce qu'une conclusion soit tirée ou que la plainte soit réglée. La date d'acceptation d'une plainte est la date à laquelle nous recevons une plainte complète (c'est-à-dire une plainte dans laquelle on retrouve suffisamment de renseignements pour entreprendre une enquête).

Antérieurement, nous mesurions le délai de traitement à compter de la date à laquelle une plainte était reçue pour la première fois, et non quand le dossier était suffisamment complet pour entreprendre une enquête. Cette ancienne définition avait toutefois pour conséquence d'établir des délais de traitement artificiellement élevés lorsque les plaintes n'étaient pas accompagnées de tous les renseignements pertinents pour entreprendre une enquête.

Nous sommes heureux de constater que, conformément à la priorité liée à la prestation de services aux Canadiennes et Canadiens de la commissaire, le délai de traitement des plaintes en 2011 a chuté considérablement pour atteindre 8,2 mois.

À des fins de comparaison, si les délais de traitement étaient cette année calculés de la même façon que l'an dernier (à compter de la date de réception plutôt qu'à compter de la date d'acceptation), le délai de traitement moyen en 2011 serait tout-de-même de 9,3 mois, une baisse par rapport aux 15,6 mois enregistrés l'année précédente.

Signalements volontaires des atteintes à la protection des données — par secteur d'activité et type d'incident

Secteur	Type d'atteinte					2011		2010	
	Communication accidentelle	Perte	Accès, utilisation ou communication non autorisés	Total	Pourcentage	Total	Pourcentage	Total	Pourcentage
Secteur financier	12	3	14	**29**	**45 %**	**29**	**45 %**	**29**	**66 %**
Services	0	0	8	**8**	**13 %**	**8**	**13 %**	**2**	**5 %**
Assurance	0	2	5	**7**	**11 %**	**7**	**11 %**	**2**	**5 %**
Vente/Détail	2	0	3	**5**	**8 %**	**5**	**8 %**	**1**	**2 %**
Télécommunications	1	0	2	**3**	**5 %**	**3**	**5 %**	**2**	**5 %**
Internet	0	0	3	**3**	**5 %**	**3**	**5 %**	**1**	**2 %**
Divertissement	1	0	1	**2**	**3 %**	**2**	**3 %**	**2**	**5 %**
Hébergement	0	0	1	**1**	**2 %**	**1**	**2 %**	**1**	**2 %**
Autres	2	0	4	**6**	**9 %**	**6**	**9 %**	**1**	**2 %**
Santé	0	0	0	**0**	**0 %**	**0**	**0 %**	**1**	**2 %**
Services professionnels	0	0	0	**0**	**0 %**	**0**	**0 %**	**1**	**2 %**
Transport	0	0	0	**0**	**0 %**	**0**	**0 %**	**1**	**2 %**
Total	**18**	**5**	**41**	**64**		**64**		**44**	
Pourcentage	**28 %**	**8 %**	**64 %**						

*Depuis 2011, les incidents de vol de renseignements personnels sont signalés sous la catégorie Accès, utilisation ou communication non autorisés. Cette mesure a été prise parce que le vol est une forme d'accès non autorisé, et qu'il ne relève pas du mandat du Commissariat de déterminer si un incident d'accès non autorisé constitue un vol ou non.

En 2011, 64 atteintes à la protection des données dans le secteur privé nous ont été signalées volontairement. Même s'il s'agit d'une augmentation de 45 % par rapport au nombre d'incidents signalés en 2010, ce nombre se situe dans la moyenne des dernières années.

Les signalements des atteintes à la protection des données dans l'industrie financière — le principal secteur qui nous signale couramment des incidents — sont demeurés stables avec 29 incidents. À titre de comparaison, le signalement des atteintes à la protection des données dans tous les autres secteurs a plus que doublé, passant de 15 en 2010 à 35 en 2011.

Cela suggère une sensibilisation accrue au signalement des atteintes à la protection des données. Ses avantages ont largement dépassé le secteur financier pour atteindre le plus vaste secteur privé du Canada.

L'importance du signalement des atteintes à la protection des données a davantage été mise de l'avant à la fin de 2010 et en 2011 à la suite de l'introduction en Alberta du signalement obligatoire des atteintes à la protection des données et de la préparation d'une loi fédérale visant à rendre obligatoire le signalement des atteintes à la commissaire à la protection de la vie privée.

DÉFINITIONS DES TYPES D'ATTEINTES À LA PROTECTION DES DONNÉES :

Communication accidentelle : incidents dans le cadre desquels une organisation communique par accident des renseignements personnels à des personnes auxquelles ces renseignements ne sont pas destinés, par exemple, des relevés bancaires envoyés à la mauvaise adresse en raison d'une erreur mécanique ou humaine, ou des renseignements personnels rendus publics sur le site Web d'une organisation à la suite d'une erreur technique.

Perte : incidents dans le cadre desquels des renseignements personnels sont perdus par une organisation, habituellement à la suite de la perte d'un ordinateur portatif, d'un CD ou de documents papier.

Accès, utilisation ou communication non autorisés : incidents dans le cadre desquels une personne accède, utilise ou communique des renseignements personnels sans l'autorisation d'une organisation, par exemple, à la suite du vol d'un ordinateur portatif, du piratage en ligne de la base de données d'une organisation ou de l'accès ou de l'utilisation de renseignements personnels par un employé à des fins non autorisées.