



Notes d'allocution à l'intention du grand public

DIAPOSITIVE TITRE : Guide sur la protection de vos renseignements personnels

[PARTIE 1 – DIAPOSITIVE 2 : Vie privée 101]

DIAPOSITIVE 3 : Ce dont nous parlons aujourd'hui – et pourquoi

- Beaucoup de gens ont plusieurs appareils électroniques et comptes, entre autres des comptes de médias sociaux et de courriel. En outre, nous sommes nombreux à payer des produits et des services au moyen d'une carte ou même de notre téléphone.
- De plus en plus, nous menons notre vie quotidienne en ligne et utilisons la technologie. Nous communiquons donc souvent nos renseignements personnels, ce qui peut nous exposer à des risques.
- Aujourd'hui, nous allons parler des mesures à prendre pour protéger ces renseignements. Notre présentation vous renseignera sur votre droit à la vie privée et la responsabilité de protéger vos renseignements personnels qui incombe au gouvernement et aux entreprises.

DIAPOSITIVE 4 : Votre droit à la vie privée

- Combien d'entre vous font confiance aux entreprises pour protéger leur vie privée? Et le gouvernement?
- La bonne nouvelle, c'est qu'au Canada, le gouvernement et les entreprises ont l'obligation de protéger votre vie privée.
- En fait, la *Charte canadienne des droits et libertés* garantit le droit à la vie privée. Il existe aussi des lois provinciales et territoriales qui protègent ce droit.
- Le Commissariat à la protection de la vie privée du Canada veille au respect de deux lois fédérales sur la protection de la vie privée, soit la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui s'applique à certaines entreprises au Canada, et la *Loi sur la protection des renseignements personnels*, qui s'applique aux ministères et organismes fédéraux.
- Ces lois prévoient la façon dont le gouvernement et certaines entreprises traitent vos renseignements personnels. Par exemple, les entreprises doivent expliquer comment elles recueillent et utilisent vos renseignements personnels, d'ordinaire avec votre consentement. Le gouvernement et les entreprises doivent également stocker ces renseignements et procéder à leur élimination de manière responsable.
- Ressource : [Votre droit à la vie privée](#)

DIAPOSITIVE 5 : Qu'entend-on par « renseignements personnels »?

- La LPRPDE protège les renseignements concernant un individu identifiable.
- Que sont les « renseignements personnels »?



- Pensez à ce qui vous distingue des autres, par exemple vos empreintes digitales. De la même façon, il y a des renseignements qui sont du domaine de votre vie privée, comme les renseignements de votre carte de crédit et vos déclarations de revenus.

DIAPOSITIVE 6 : Exemples de renseignements personnels

- Vos renseignements personnels comprennent :
 - votre nom et les renseignements relatifs à votre race, à votre origine ethnique, à votre religion, à votre état matrimonial et le niveau d’instruction;
 - votre adresse et vos messages de courriel ainsi que votre adresse IP (protocole Internet);
 - votre âge, votre taille, votre poids, vos dossiers médicaux, votre groupe sanguin, votre code d’ADN, vos empreintes digitales et votre signature vocale (les caractéristiques de votre voix);

DIAPOSITIVE 7 : Exemples de renseignements personnels (suite)

- vos revenus, vos achats, vos habitudes de consommation, vos renseignements bancaires, les données sur les cartes de crédit ou de débit, vos rapports de prêt ou de solvabilité et vos déclarations de revenus;
 - votre numéro d’assurance sociale (NAS) ou vos autres numéros d’identification.
- Vos renseignements personnels peuvent aussi comprendre les mots que vous tapez, les sites Web que vous visitez et les photos que vous affichez en ligne.

DIAPOSITIVE 8 : Les entreprises ont l’obligation de vous protéger

- Qu’il s’agisse d’acheter des provisions à l’épicerie ou des vêtements en ligne ou encore de payer pour obtenir un service, par exemple des rénovations, les échanges commerciaux modernes mettent souvent en jeu des renseignements personnels. Même si vous communiquez vos renseignements personnels à une entreprise, cela ne signifie pas que vous renoncez à exercer un contrôle sur ces renseignements.
- La LPRPDE établit les règles de base qui régissent le traitement des renseignements personnels dans le cadre des activités commerciales.
- Elle s’applique aux entreprises de toutes tailles, qu’elles aient pignon sur rue ou exercent leurs activités exclusivement en ligne.
- En vertu de la LPRPDE, les organisations du secteur privé doivent recueillir, utiliser ou communiquer vos renseignements personnels de façon honnête et licite, avec votre consentement et seulement à des fins qui sont précisées et raisonnables. En gros, les entreprises peuvent recueillir uniquement les renseignements personnels essentiels pour vous fournir un produit ou un service. Si l’on sollicite d’autres renseignements, vous avez le droit d’en demander la raison et de refuser de les fournir. Vous devriez être en mesure d’effectuer une transaction même si vous avez refusé de transmettre les renseignements supplémentaires demandés.
- Trois provinces (le Québec, la Colombie-Britannique et l’Alberta) ont adopté leur propre loi, très similaire, en matière de protection de la vie privée.



- Chaque fois qu'un renseignement ne semble pas nécessaire au fonctionnement du produit ou à la prestation du service, dites « non » ou demandez plus d'information.
- Ressource : [Les entreprises et vos renseignements personnels](#)

[PARTIE 2 – DIAPOSITIVE 9 : Exercice de vos droits]

DIAPOSITIVE 10 : Accès à vos renseignements personnels

- Si vous souhaitez savoir quels renseignements personnels le gouvernement fédéral ou une entreprise privée possède à votre sujet, vous avez le droit de les consulter.
- Vous devriez avoir accès à vos renseignements personnels à un coût minime ou gratuitement.
- Le processus devrait être rapide. L'organisation est censée vous donner accès à vos renseignements personnels dans les 30 jours civils suivant la réception de votre demande. Si elle n'a pas les renseignements en mains, elle doit vous en informer avant l'expiration de ce délai.
- Dans certaines circonstances, ce délai pourrait être plus long. Par exemple, une institution fédérale peut prolonger ce délai pour une période allant jusqu'à 30 jours si :
 - le respect du délai initial peut nuire de façon déraisonnable aux activités de l'institution;
 - les consultations nécessaires pour donner suite à la demande rendent pratiquement impossible l'observation du délai initial ;
 - Le délai peut également être prorogé pour une durée raisonnable si les renseignements personnels doivent être traduits ou convertis pour être transférés sur un support de substitution.
- Des ressources en ligne du Commissariat expliquent le processus de demande de renseignements et la façon de s'y prendre pour faire corriger une erreur factuelle dans les renseignements que vous avez reçus.
 - Ressources : [Consulter vos renseignements personnels – gouvernement fédéral](#)
[Consulter vos renseignements personnels – entreprises](#)

DIAPOSITIVE 11 : Pourquoi lire les politiques de confidentialité

- Vous avez tout intérêt à prendre connaissance des politiques de confidentialité, car elles peuvent vous aider à prendre une décision éclairée concernant la communication de vos renseignements personnels. Vous pourriez être tenté de sauter cette étape, mais prenez le temps de lire l'information avant de cliquer sur « J'accepte ». Si la politique de confidentialité ne vous convient pas, évitez d'utiliser le produit ou le service.
- Comme nous l'avons mentionné, la loi oblige les organisations qui recueillent des renseignements personnels à informer les utilisateurs de leurs pratiques de protection de la vie privée.
- Une bonne politique de confidentialité devrait expliquer - dans un langage simple, avec clarté et de façon détaillée - ce que vous devriez savoir afin de bien comprendre la façon dont l'organisation traite vos renseignements personnels, notamment :
 - quels sont les renseignements qui sont recueillis;
 - à qui ces renseignements seront-ils communiqués;
 - pourquoi sont-ils recueillis, utilisés ou communiqués;



- tout risque de préjudice.
- Le Commissariat donne des conseils en ligne qui vous aideront à savoir quelle information rechercher dans une politique de confidentialité. En résumé, efforcez-vous de trouver des détails sur la collecte des renseignements, l'utilisation que l'on en fera et la période pendant laquelle ils seront conservés.
- Ressource : [Points importants à prendre en considération dans une politique de confidentialité](#)

DIAPOSITIVE 12 : La protection de votre vie privée vous inquiète? Voici ce que vous devez faire.

- Il est possible que vous soyez préoccupé par la façon dont une organisation traite vos renseignements personnels.
- Si c'est le cas, commencez par faire part de vos préoccupations directement à l'entreprise. Les entreprises peuvent souvent résoudre le problème rapidement.
- Si vous n'êtes pas satisfait de la réponse obtenue, vous avez parfaitement le droit de déposer une plainte auprès du Commissariat. Il n'est pas nécessaire d'avoir recours à un avocat ou à un consultant. Vous trouverez sur le site Web du Commissariat un guide sur le traitement des plaintes. Vous pouvez aussi utiliser la ligne téléphonique d'information du Commissariat pour parler avec des agents qui répondront à vos questions sur les enjeux liés à la protection de la vie privée.
- Ressource : [Signaler un problème](#)

DIAPOSITIVE 13 : Posez des questions et exprimez-vous!

- Lorsque vous consultez une politique de confidentialité, recherchez les coordonnées des personnes-ressources au cas où vous auriez des questions particulières. Les coordonnées du responsable de la protection de la vie privée sont parfois indiquées. En cas de doute, n'hésitez pas à poser des questions à l'organisation.
- Si vous estimez que l'on ne traite pas correctement vos renseignements personnels, n'oubliez pas que vous avez le droit de le signaler. Faites part de vos préoccupations directement à l'organisation ou déposez une plainte officielle auprès du Commissariat.
- Vous serez peut-être nerveux à l'idée d'exprimer ainsi vos préoccupations, mais ne vous en faites pas. C'est votre droit. Le Commissariat met à votre disposition de nombreuses ressources qui vous aideront à communiquer avec la bonne personne, à avoir un dialogue constructif et à vous protéger.
- Ressource : [Conseils pour faire part de vos préoccupations concernant la protection de la vie privée à une entreprise](#)

DIAPOSITIVE 14 : Vous êtes prêt à communiquer vos renseignements? Pensez-y deux fois!

- Que ce soit en ligne ou en personne, on nous demande constamment de communiquer des renseignements personnels.
- Ne fournissez pas les vôtres aveuglément.



- Demandez-vous pourquoi ces renseignements sont nécessaires, qui les utilisera et comment. En cas de doute, posez des questions.
- Si la réponse ne vous satisfait pas, faites-le savoir à l'organisation et ne lui communiquez pas vos renseignements personnels. Toutefois, vous devrez peut-être renoncer à obtenir le produit ou le service fourni par l'organisation.
- Ressource : [Dix conseils à suivre pour protéger vos renseignements personnels](#)

[PARTIE 3 – DIAPOSITIVE 15 : D'autres moyens de vous protéger]

DIAPOSITIVE 16 : Réglez les paramètres de confidentialité de manière à vous protéger

- Avant de vous inscrire à un service ou de télécharger une application, renseignez-vous sur les renseignements personnels recueillis et les contrôles proposés en matière de confidentialité. Si vous n'êtes pas à l'aise, ne vous inscrivez pas au service.
- Le meilleur moyen de contrôler vos renseignements personnels en ligne est de ne pas les transmettre en premier lieu.
- Évidemment, il peut ne pas être pratique ou possible de s'abstenir de divulguer des renseignements, un moyen d'essayer de limiter les implications potentielles sur la vie privée consiste à utiliser les paramètres de confidentialité.
- Sans être une solution miracle, les paramètres de confidentialité peuvent certainement vous aider à exercer un contrôle sur vos renseignements personnels. Il est important de savoir que les paramètres par défaut peuvent vous exposer à des risques.
- Les paramètres de confidentialité vous aident à indiquer si vous consentez ou non à la collecte, à l'utilisation et à la communication de vos renseignements personnels. C'est pourquoi il est important de choisir et de définir des paramètres de confidentialité avec lesquels vous êtes à l'aise sur tous les comptes de médias sociaux, les services en ligne, les appareils et les navigateurs que vous utilisez.
- Sachez que vous avez le droit de refuser de fournir des renseignements personnels qui ne sont pas essentiels au produit ou au service. Recherchez les options vous permettant de désactiver certaines fonctions, par exemple l'accès à votre microphone ou votre géolocalisation, s'ils ne sont pas nécessaires pour l'utiliser.
- On doit vérifier souvent les paramètres de confidentialité – il ne suffit pas de le faire une seule fois sans y penser par la suite. Comme de nombreux sites modifient fréquemment les options offertes à cet égard, vérifiez souvent ces paramètres pour vous assurer d'être toujours à l'aise avec les renseignements que vous communiquez.
- Ressource : [Conseils pour utiliser les paramètres de confidentialité](#)

DIAPOSITIVE 17 : N'oubliez pas vos appareils électroniques

- Choisissez des mots de passe difficiles à deviner. Si vous oubliez votre téléphone quelque part et que des gens le trouvent, ils pourront beaucoup plus difficilement avoir accès à vos renseignements personnels.



- Vous pouvez aussi installer des logiciels antivirus et de sécurité sur vos appareils électroniques. Assurez-vous de garder ces logiciels à jour.
- Supprimez tous les renseignements personnels stockés sur vos anciens appareils (téléphone, ordinateur portable ou tablette électronique) avant de vous en débarrasser, de les recycler ou de les vendre. Il est important de savoir que la restauration des paramètres par défaut ne supprime pas les données en permanence. Vérifiez auprès du fabricant de l'appareil.
- Le Commissariat peut vous fournir de l'information concernant la gestion de la confidentialité sur vos appareils mobiles.

DIAPOSITIVE 18 : Naviguez en toute sécurité

- Des outils intégrés à votre navigateur Internet aident à protéger vos renseignements personnels. Prenez le temps de vous renseigner sur les paramètres de sécurité et de confidentialité de votre navigateur et tenez-les à jour. Si vous utilisez plusieurs navigateurs (comme Chrome et Safari), vérifiez les paramètres de chacun.
- Recherchez l'icône de verrouillage (cadenas), le protocole HTTPS ou la surbrillance verte dans la barre d'adresse. Sans être infaillibles, tous ces éléments indiquent que le site est probablement sécurisé.
- N'effectuez pas de transactions de nature délicate, par exemple des opérations bancaires, sur un réseau Wi-Fi public. On pourrait intercepter les données que vous transmettez, car ces connexions ne sont pas sécurisées.
- Vous devriez également désactiver les fonctions Wi-Fi et Bluetooth lorsque vous ne les utilisez pas. En laissant votre appareil électronique ouvert par défaut, vous permettez aux autres d'avoir accès à vos données, à votre insu et sans votre consentement, quand vous passez dans un café ou un autre endroit qui offre un réseau sans fil ouvert au public.

DIAPOSITIVE 19 : Gestion des mots de passe

- Les mots de passe sont essentiels pour protéger vos renseignements personnels. Des mots de passe faciles à deviner ou les mots de passe par défaut peuvent vous exposer à des risques.
- Il est tentant d'utiliser un seul mot de passe pour tout, mais vous pourriez ainsi mettre en péril vos renseignements personnels : si une personne obtenait votre mot de passe, elle pourrait avoir accès à tous vos comptes.
- Évitez de choisir comme mot de passe le nom de famille de votre mère, le prénom de votre enfant, le nom de votre animal de compagnie ou d'autres références que quelqu'un pourrait deviner à partir de renseignements que vous avez publiés ailleurs.

DIAPOSITIVE 20 : Un conseil d'ami

- Choisissez des mots de passe que vous retiendrez facilement, mais qui sera difficile à deviner pour quelqu'un d'autre. Assurez-vous qu'ils comptent huit caractères ou plus.



- Vous pouvez utiliser une phrase comme mot de passe, composé de la première lettre de chaque mot. Par exemple, si je dis « Je joue au tennis avec 2 amis le jeudi à 4 h », le mot de passe sera « Jjata2alja4h. ».
- Si vous devez prendre en note vos mots de passe pour vous en souvenir, conservez-en une copie hors ligne dans un lieu sûr, comme un classeur verrouillé. Ne les affichez pas à la vue ou dans un endroit où quelqu'un pourrait les trouver.
- N'activez pas la fonction « se souvenir du mot de passe » sur votre navigateur ou appareil. L'ouverture de session automatique peut être utile, mais elle est contre-indiquée si vous partagez un ordinateur.
- Ne conservez pas le mot de passe par défaut ou celui programmé par le fabricant d'un nouvel appareil électronique ou d'un nouveau compte. En outre, vous devriez toujours utiliser la fonction de verrouillage automatique de vos appareils électroniques (c'est-à-dire régler votre téléphone pour qu'il se verrouille après un certain temps et qu'il vous oblige à ouvrir une nouvelle session).
- **Vous avez des enfants?** Nous avons un conseil pour vous : Si vous demandez à vos enfants de vous dévoiler leurs mots de passe, faites-leur bien comprendre qu'il s'agit d'un cas d'exception entre vous. Ils ne devraient communiquer leurs mots de passe à personne d'autre, pas même à leurs amis.
- Le Commissariat peut vous donner d'autres excellents conseils qui vous aideront à choisir et à utiliser vos mots de passe de manière efficace.
- Ressource : [Conseils pour créer et gérer vos mots de passe](#)

DIAPOSITIVE 21 : Évitez le vol d'identité

- Il y a vol d'identité lorsque quelqu'un utilise les renseignements personnels d'une autre personne afin de se faire passer pour elle à des fins frauduleuses.
- Chaque année, des milliers de personnes sont victimes d'un vol d'identité. Un fraudeur peut utiliser votre nom, votre date de naissance, votre adresse, votre numéro de carte de crédit, votre numéro d'assurance sociale (NAS) et vos autres numéros d'identification personnels pour demander une carte de crédit, ouvrir un compte bancaire, réacheminer votre courrier, s'abonner à des services de téléphonie cellulaire et louer des véhicules, de l'équipement ou encore un logement ou des chambres d'hôtel, voire obtenir un emploi.
- Les conséquences d'un vol d'identité peuvent être graves pour la victime. Par exemple, on peut lui refuser un permis de conduire ou des services de téléphonie cellulaire. Il faut parfois des années pour réparer les dommages.
- Les voleurs d'identité utilisent plusieurs moyens pour s'approprier les renseignements personnels. De votre côté, vous disposez d'une panoplie de moyens pour vous protéger.
- En ligne, utilisez des mots de passe difficiles à deviner et des paramètres de confidentialité sécuritaires.
- Examinez tous vos relevés de carte de crédit et vos relevés bancaires pour vous assurer qu'aucun achat non autorisé n'y figure.
- Ne communiquez pas votre numéro de carte de crédit ni d'autres renseignements personnels par téléphone, à moins que votre interlocuteur soit une personne de confiance ou que vous ayez vous-même fait l'appel.



- Portez sur vous uniquement les pièces d'identité essentielles, comme votre permis de conduire et votre carte d'assurance maladie. Laissez votre carte d'assurance sociale, votre passeport et votre certificat de naissance en lieu sûr à la maison.
- Éliminez de façon sécuritaire les documents qui renferment des renseignements personnels. Déchiquez les factures, les relevés ou les autres documents qui ne sont plus utiles.
- Ressource : [Le vol d'identité et vous](#)

DIAPOSITIVE 22 : Les pourriels – une menace qui ne se limite pas à votre boîte de réception

- Non seulement les pourriels sont insupportables, mais sachez qu'ils peuvent aussi constituer une véritable menace pour votre vie privée. En effet, les pourriels et les messages textes indésirables peuvent renfermer des logiciels malveillants ou espions permettant d'avoir accès à vos renseignements personnels.
- Une façon simple d'éviter les pourriels est de vous abstenir de publier votre adresse de courriel en ligne à la vue de tous. La diffusion des pourriels commence par l'utilisation de logiciels recueillant sans discernement des adresses de courriel qui sont ensuite vendues à des polluposteurs.
- Vous pouvez également créer un compte de courriel distinct, qui servira uniquement à participer à des groupes en ligne ou à remplir des formulaires, tout en continuant d'utiliser un compte principal pour vos communications avec des personnes de confiance. De cette façon, vous pourrez facilement remplacer les comptes secondaires si des pirates recueillent l'adresse de courriel correspondante et que vous commencez à recevoir des pourriels.
- La protection contre les pourriels ne se limite pas à votre boîte de réception. Protégez tous vos appareils électroniques – ordinateur, téléphone et tablette électronique – au moyen de logiciels de sécurité (antivirus et antimaliciels) téléchargés à partir d'une source digne de confiance. Assurez-vous de garder ces logiciels à jour.
- Ressource : [Dix conseils pratiques pour protéger votre boîte de courriels, votre ordinateur et votre appareil mobile](#)

DIAPOSITIVE 23 : Conseils pour se protéger contre les pourriels

- N'ouvrez aucun courriel dont vous ne connaissez pas l'expéditeur. En supprimant ce type de courriel, vous pourrez prévenir de nombreux problèmes.
- Si vous ouvrez un pourriel par mégarde, n'y répondez pas. Une réponse confirmerait que votre adresse de courriel est active, si bien que vous pourriez ensuite recevoir encore plus de pourriels. Pour la même raison, ne cliquez jamais sur un lien comme « Supprimer », ou « Désinscrivez-vous » dans un message de nature douteuse pouvant être un pourriel. Vous pourriez vous « abonner » sans le savoir et là encore recevoir par la suite encore plus de pourriels.
- Ne cliquez jamais sur un hyperlien ou une pièce jointe faisant partie d'un courriel suspect. Vous pourriez lancer un logiciel malveillant susceptible de porter atteinte à votre vie privée ou d'endommager votre appareil.
- Vous pouvez signaler au Centre de notification des pourriels (www.combattrelepourriel.gc.ca) les courriels non sollicités renfermant des pièces jointes ou un contenu suspects.



DIAPOSITIVE 24 : Protégez-vous dans les médias sociaux

- Combien d'entre vous utilisent les médias sociaux? Levez la main. Si vous les utilisez plus d'une fois par jour, gardez la main levée. Les utilisez-vous deux fois par jour? Cinq fois par jour? Encore plus?
- Les médias sociaux peuvent être formidables pour rester en contact avec vos amis et votre famille ou partager des photos et des vidéos. Mais ils peuvent aussi mettre en péril vos renseignements personnels.
- Assurez-vous de bien comprendre et gérer les différents paramètres de confidentialité de tous vos comptes de médias sociaux. Prenez connaissance de la politique de confidentialité avant de vous inscrire et vérifiez périodiquement le réglage des paramètres de confidentialité pour vous assurer d'être toujours à l'aise avec les options que vous avez choisies.
- Choisissez des mots de passe difficiles à deviner qui sont différents pour chacun de vos comptes de médias sociaux.
- Déconnectez-vous de vos comptes lorsque vous ne les utilisez pas. Si vous ne vous servez plus d'un compte, demandez à l'entreprise de supprimer votre compte et vos données. Il n'est pas suffisant de désactiver un compte ou de supprimer une application de votre appareil électronique, car toutes vos données resteront sur les serveurs de l'entreprise.
- Faites attention au contenu que vous publiez, notamment les photos qui pourraient renfermer des renseignements personnels. En outre, faites preuve de respect envers les autres personnes. Avant de publier des photos ou des vidéos où elles figurent ou encore des renseignements les concernant, demandez-leur si elles sont à l'aise que vous les partagiez.
- N'oubliez pas de peser les répercussions que vos publications en ligne pourraient avoir dans le monde hors ligne. Pensez-y deux fois avant de publier des commentaires ou des images qui pourraient nuire à votre propre réputation ou à celle d'autres personnes.
- Ressource : [Utilisation sécuritaire des médias sociaux](#)

DIAPOSITIVE 25 : Résumé

- Connaissez vos droits en matière de protection de la vie privée.
- Posez des questions lorsqu'une entreprise vous demande des renseignements.
- Protégez vos renseignements en utilisant des mots de passe difficiles à deviner, des logiciels de sécurité et un réglage approprié des paramètres de confidentialité.
- Naviguez en toute sécurité. Lorsque vous effectuez des transactions en ligne, assurez-vous que le site Web est sécurisé. Désactivez les fonctions Wi-Fi et Bluetooth quand vous n'en avez pas besoin.
- Protégez-vous contre le vol d'identité en limitant les renseignements que vous communiquez et les pièces d'identité que vous portez sur vous. Utilisez des mots de passe difficiles à deviner et déchiquetez les documents qui renferment des renseignements sensibles.
- Méfiez-vous des pourriels! N'y répondez jamais et ne cliquez pas sur les liens qui s'y trouvent.
- Faites attention aux renseignements que vous communiquez dans les médias sociaux. Respectez la vie privée des autres.



DIAPOSITIVE 26 : Pour en savoir plus

- Le présent exposé a été produit par le Commissariat à la protection de la vie privée du Canada, qui veille à l'application des lois fédérales sur la protection des renseignements personnels. Les Canadiens peuvent s'adresser au Commissariat afin d'obtenir de l'information sur la protection de la vie privée, de déposer une plainte ou de lui faire part de leurs préoccupations à cet égard.
- Le Commissariat fournit un appui au commissaire à la protection de la vie privée, qui est un agent indépendant du Parlement.
- Pour obtenir d'autres conseils afin de protéger votre vie privée, consultez le site Web www.priv.gc.ca.