Lignes directrices en matière de consentement en ligne

Commissariat à la protection de la vie privée du Canada

Office of the Information & Privacy Commissioner for British Columbia
Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner of Alberta

> *« Les témoignages présentés au Comité font ressortir les difficultés auxquelles se heurtent les Canadiens au moment de donner leur consentement dans les contrats et ententes avec les médias sociaux. Pour bien appliquer les lois canadiennes en matière de protection de la vie privée et protéger les intérêts des citoyens à cet égard, il est impératif que le consentement donné soit valable et adapté aux circonstances, conformément aux principes énoncés dans la LPRPDE. Le Comité prend acte que, pour ce faire, le langage utilisé pour s'adresser aux individus doit être clair et accessible. »*

Protection de la vie privée et médias sociaux à l'ère des mégadonnées : Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique
Avril 2013

1. Introduction

Le consentement valable constitue un élément essentiel de la loi canadienne sur la protection des renseignements personnels qui s'applique au secteur privé. En effet, en vertu des lois sur la protection des renseignements personnels, les organisations sont tenues d'obtenir un consentement valable avant de recueillir, d'utiliser et de communiquer des renseignements personnels. Le consentement est considéré comme valable quand les personnes comprennent ce que les organisations font de leurs renseignements.

Selon une étude réalisée en 2012 par le Commissariat à la protection de la vie privée du Canada et portant sur des sites Web canadiens très fréquentés, les pratiques des organisations en matière de protection de la vie privée, notamment en ce qui a trait à la communication de renseignements personnels à des tiers, ne sont pas toujours expliquées de manière efficace aux consommateurs en ligne. Par ailleurs, le tout premier ratissage d'Internet sous l'égide du Global Privacy Enforcement Network, auquel le Commissariat et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique ont participé, a mis en évidence des lacunes dans la façon dont certaines organisations renseignent les consommateurs sur leurs pratiques en matière de protection de la vie privée. Cela donne à penser que de nombreuses entreprises semblent avoir du mal avec le consentement en ligne.
C'est pourquoi le Commissariat, de concert avec les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, publie les présentes lignes

directrices afin d'analyser la question des exigences en matière de consentement en vertu de la loi sur la protection des renseignements personnels qui s'applique au secteur privé et de faire connaître ses attentes en ce qui a trait aux mesures que doivent prendre les organisations pour s'assurer d'obtenir un consentement valable dans l'environnement en ligne. À toutes fins utiles, les organisations doivent avoir une politique de confidentialité claire, descriptive et accessible et, si les circonstances le justifient, fournir des explications dynamiques sur la protection des renseignements personnels tout au long de l'expérience de l'utilisateur.

Le présent document illustre les principes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui est une loi fédérale, et des lois sur la protection des renseignements personnels de l'Alberta et de la Colombie-Britannique (LPRP-AB et LPRP-CB). Bien que les trois lois soient à peu près similaires et reposent sur les mêmes principes sous-jacents, il existe quelques différences entre elles. Les organisations doivent comprendre les obligations qui leur incombent en vertu de la loi à laquelle elles sont assujetties[1].

Qu'entend-on par renseignements personnels?

En vertu de la loi canadienne sur la protection des renseignements personnels qui s'applique au secteur privé, l'expression « renseignement personnel » s'entend de tout renseignement concernant un individu identifiable. La Cour fédérale a statué que « les renseignements seront des renseignements concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources ».

Une série de données propres à l'environnement en ligne peuvent être considérées comme des renseignements personnels dans des cas particuliers[2], par exemple :

- l'information sur l'emplacement, y compris les données GPS;
- les identifiants d'appareils, comme l'adresse IP et MAC; et,
- les données sur le parcours[3], l'historique de navigation, les signets;
- les données des réseaux sociaux créées par l'utilisateur, comme les commentaires, les évaluations, les « J'aime » et « Je n'aime pas », le flux Twitter, les interactions avec les services à la clientèle.

Le fait de combiner des bribes d'information disparates provenant de plusieurs sources peut aussi mener à l'établissement de profils détaillés permettant d'identifier les individus. Les organisations qui utilisent des techniques d'analyse avancée devraient être particulièrement attentives à la définition de renseignement personnel, puisque les risques de réidentification de données

[1] Pour des questions précises sur la façon dont les présentes lignes directrices s'appliquent à votre organisation, veuillez communiquer avec le commissariat de votre province.
[2] Veuillez adresser toute question sur la définition des renseignements personnels au commissariat de votre province.
[3] Les données sur le parcours conservent la trace de l'activité de l'utilisateur sur Internet, y compris de chaque page de chaque site Web que l'utilisateur visite, du temps qu'il passe sur une page ou un site et de l'ordre dans lequel il visite les pages. (traduction libre d'une définition tirée de webopedia.com)

anonymes ont fortement augmenté par suite des progrès technologiques permettant de recueillir et de regrouper de grandes quantités de données.

Obstacles à la transparence et à l'obtention d'un consentement valable en ligne

Pour obtenir un consentement valable, il faut absolument faire preuve de transparence. Quand une organisation explique clairement ses pratiques de gestion de l'information et que ces explications sont facilement accessibles, les individus sont mieux en mesure de prendre des décisions éclairées concernant la communication de leurs renseignements personnels. Il est donc essentiel que les utilisateurs comprennent ce que les organisations font de leurs renseignements personnels au moment de décider à qui les communiquer et dans quelles circonstances.

Cette question est encore plus importante dans les environnements en ligne et mobile, où des pratiques complexes de gestion de l'information, de nouveaux modèles opérationnels et des innovations technologiques peuvent se révéler déroutants, voire étourdissants, pour l'utilisateur moyen. Les téléphones intelligents présentent un problème particulier du fait qu'ils recueillent une couche supplémentaire de renseignements personnels, notamment l'emplacement, ce qui rend encore plus difficile la protection des renseignements personnels. Par ailleurs, leurs capacités avancées et diversifiées de collecte et de traitement des données sont dissimulées derrière un petit écran où, faute de place, les explications sur la protection des renseignements personnels n'attirent guère l'attention de l'utilisateur.

Or, les progrès technologiques ont grandement amélioré la capacité des organisations à recueillir, traiter et communiquer instantanément d'énormes quantités de données. L'évolution du Web social et l'omniprésence de l'analyse des données font en sorte que la collecte et le traitement de données ne se font pas seulement à l'écran, mais également dans l'ombre, où bien des entreprises invisibles peuvent avoir accès aux renseignements personnels de tout un chacun. En ce qui concerne le comportement en ligne, la rapidité d'accès à un service ou à une activité constitue souvent la priorité. Les études nous indiquent que les gens veulent avoir accès à un service ou une application en ligne dès leur arrivée sur un site Web et qu'ils cliquent rapidement sur les menus et les options susceptibles de les y mener. Il n'est donc pas étonnant qu'ils ne puissent guère porter attention à la recherche d'information sur la protection des renseignements personnels. Cet environnement multicouches, axé sur les données et où tout va très vite requiert dès lors une approche réfléchie à l'égard des communications relatives à la vie privée.

La protection des renseignements personnels constitue un avantage concurrentiel

Il est évident que pour trouver des façons de rendre les politiques de confidentialité plus claires et accessibles, il faudra peut-être déployer des efforts supplémentaires et faire preuve de créativité, en particulier dans l'environnement mobile. Toutefois, nous sommes convaincus que les organisations ont la capacité de trouver des solutions inédites et novatrices pour accroître la transparence. Être avant-gardiste dans ce domaine n'est pas seulement important pour la protection des renseignements personnels, mais aussi pour les relations des organisations avec leurs utilisateurs.

Le caractère transparent des pratiques en matière de protection des renseignements personnels et l'accès plus facile des utilisateurs à ces renseignements renforceront la confiance des consommateurs, ce qui est bon pour les affaires. La protection des renseignements personnels

n'a jamais eu autant d'importance qu'aujourd'hui dans la décision des consommateurs d'acheter ou d'utiliser des produits et services, et les organisations qui se méritent et maintiennent la confiance de leurs clients à cet égard ont une longueur d'avance sur la concurrence. Si les gens n'ont pas peur de fournir leurs renseignements personnels en ligne, ils seront mieux en mesure de participer pleinement à l'économie numérique, ce qui stimulera l'innovation et entraînera des retombées économiques pour le Canada.

2. Protection des renseignements personnels 101 : le consentement est requis

Une organisation est tenue d'obtenir le consentement valable d'une personne avant de recueillir, d'utiliser et de communiquer ses renseignements personnels.

- Les personnes doivent être informées des pratiques de gestion de l'information d'une organisation pour être en mesure de donner un consentement jugé valable en vertu des lois sur la protection des renseignements personnels.
- Les fins pour lesquelles l'organisation recueille, utilise et communique des renseignements personnels doivent être précisées au moment de la collecte ou avant.
- Si l'organisation décide d'utiliser les renseignements personnels à une nouvelle fin après leur collecte, elle doit en informer les personnes concernées et obtenir leur consentement.
- L'obtention du consentement ne dégage pas l'organisation de ses autres obligations en vertu des lois sur la protection des renseignements personnels, comme la responsabilité générale, les mesures de sécurité et un motif raisonnable de recueillir, d'utiliser et de communiquer les renseignements personnels.

En vertu de la LPRP de l'Alberta et de la Colombie-Britannique, ainsi que de la LPRPDE, les organisations doivent obtenir le consentement pour recueillir, utiliser et communiquer les renseignements personnels.

Le consentement doit être valable

En vertu des lois sur la protection des renseignements personnels, la personne qui donne son consentement doit comprendre à quoi elle consent. Or, pour que le consentement soit considéré comme valide ou valable, les organisations doivent informer les personnes de leurs pratiques en matière de protection de la vie privée de manière détaillée et en des termes faciles à comprendre. Ce n'est qu'une fois informé des politiques et des pratiques de l'organisation et après qu'il les a comprises que l'intéressé peut fournir un consentement valable. Il devrait pouvoir comprendre les risques et les avantages de la communication de ses renseignements personnels à l'organisation et être en mesure de décider librement quoi faire.

Les organisations sont tenues de rendre facilement accessibles leurs politiques et pratiques de gestion des renseignements personnels. Ces politiques et pratiques doivent être claires, détaillées et faciles à trouver. Si les pratiques décrites sont complexes et font intervenir plusieurs parties, l'organisation devrait déployer un effort concerté pour s'assurer que l'utilisateur peut comprendre tous les éléments du processus, y compris les types de tierces parties concernées et les raisons de leur participation.

Les organisations devraient pouvoir prouver que le consentement obtenu repose sur de l'information exhaustive et compréhensible. Les lois sur la protection des renseignements personnels obligent expressément les organisations à informer les individus des fins auxquelles leurs renseignements personnels seront utilisés. Cette explication doit être facilement accessible et compréhensible pour l'utilisateur moyen. Le consentement n'est valide que pour les fins dont la personne a été informée.

Qu'est-ce que les organisations devraient aussi savoir sur le consentement?

Motif raisonnable

Il importe de se rappeler que les fins pour lesquelles une organisation recueille et utilise les renseignements personnels doivent être raisonnables et définies. Même si l'intéressé a donné son consentement, les lois sur la protection des renseignements personnels obligent les organisations à limiter la collecte, l'utilisation et la communication des renseignements personnels aux fins qu'une personne raisonnable jugerait appropriées dans les circonstances. Autrement dit, le consentement de l'intéressé ne donne pas à l'organisation l'entière liberté de recueillir et d'utiliser sans discernement les renseignements personnels comme bon lui semble.

Conditions du service

Souvent, une organisation aura besoin de certains renseignements personnels pour fournir le service ou le produit demandé. Si une personne refuse de donner ces renseignements, le service pourra lui être refusé. Toutefois, on ne peut forcer une personne à consentir à la communication de renseignements autres que ceux dont l'organisation a besoin pour atteindre un objectif particulier. Ce principe est particulièrement pertinent dans les environnements en ligne et mobile, où le consommateur tient avant tout à avoir rapidement accès à un service ou à une activité.

Retrait du consentement

En vertu des lois sur la protection des renseignements personnels qui s'appliquent au secteur privé, les individus ont le droit de retirer leur consentement, sous réserve des restrictions légales ou contractuelles. Le retrait du consentement devrait empêcher toute collecte ou utilisation ultérieure des renseignements personnels de l'individu. Dans certains cas, ce retrait peut également entraîner la suppression des données sur la personne concernée qui sont détenues par l'organisation. Par exemple, si un utilisateur supprime son compte sur le site d'un réseau social, l'organisation devrait effacer ses renseignements personnels du site, dans la mesure où cela est possible sur le plan technique. Dans certains cas bien précis toutefois, une organisation peut être obligée de conserver une partie des renseignements sur un individu qui a retiré son consentement. Par exemple, la liste des adresses de courriel des personnes qui ont demandé à ce qu'un service en ligne ne les contacte plus peut être conservée. Par ailleurs, d'autres lois peuvent exiger la conservation de ces renseignements. Par exemple, la législation et la réglementation applicables au secteur financier obligent les organisations à conserver des données comme les dossiers de crédit de leurs clients et les demandes de cartes de crédit pendant cinq ans à partir du jour de la fermeture du compte auquel elles se rapportent[4].

[4] *Ligne directrice 6G : Tenue de documents et vérification de l'identité des clients – Entités financières,* Centre d'analyse des opérations et déclarations financières du Canada, juillet 2010.

Le consentement n'est pas une solution miracle

Enfin, il est important de noter que le consentement ne libère pas l'organisation de ses autres obligations en vertu des lois sur la protection des renseignements personnels, par exemple la responsabilité générale, les limites de la collecte et les mesures de sécurité. En d'autres termes, si un individu consent à ce que ses renseignements personnels soient traités contrairement aux dispositions de la loi, l'organisation n'en sera pas moins considérée comme enfreignant ces dispositions. Par exemple, si des clients s'inscrivent à un service en ligne qui n'utilise pas le chiffrement des données, on peut considérer que l'organisation protège mal leurs renseignements personnels et cela, même si elle a obtenu leur consentement.

La législation sur la protection des renseignements personnels oblige aussi les organisations à limiter la collecte de renseignements personnels aux fins légitimes pour lesquelles elle est requise. Les organisations doivent pouvoir expliquer les raisons pour lesquelles elles recueillent chaque renseignement et comment elles l'utiliseront. C'est pourquoi, même si elles sont tentées de recueillir des renseignements personnels qui leur semblent pouvoir être utiles ultérieurement, elles devraient se retenir de le faire. En effet, les lois canadiennes sur la protection des renseignements personnels obligent les organisations à limiter leur collecte de renseignements personnels aux fins qui ont été précisées et à supprimer ceux dont elles n'ont plus besoin pour les fins pour lesquelles ils avaient été recueillis au départ.

Les aspects pratiques du consentement en ligne

Dans le monde hors ligne, le consentement prend souvent la forme d'une signature. En ligne, il est plus difficile d'exprimer son consentement d'une manière non ambiguë et universellement reconnaissable. En vertu de la législation sur la protection des renseignements personnels, toute déclaration ou comportement en ligne pouvant raisonnablement être interprété comme un consentement, soit explicitement ou implicitement, peut être acceptable compte tenu des circonstances. Il faut toutefois éviter qu'il y ait le moindre doute concernant le consentement.

Les organisations disposent de nombreuses options pour obtenir le consentement en ligne. Cliquer sur le bouton « J'accepte » ou cocher une case constituent des équivalents en ligne de la signature qui sont couramment utilisés. Le consentement peut également s'exprimer par une action, par exemple le téléchargement d'une application après avoir lu les renseignements personnels auxquels l'application aura accès et la façon dont les renseignements seront utilisés. On peut également déduire le consentement d'une non-intervention, par exemple, quand l'utilisateur n'a pas exercé son option de retrait. Les organisations sont libres de proposer l'approche qui fonctionne le mieux dans un environnement donné, en n'oubliant pas que le consentement doit être exprimé de manière appropriée selon la nature des renseignements, le contexte et les attentes raisonnables des utilisateurs.

Les organisations ont intérêt à mettre en place des procédures pour obtenir le consentement des individus et à conserver la preuve de l'obtention de ce consentement. Il peut arriver qu'une organisation doive donner la preuve qu'elle a bel et bien obtenu le consentement d'un individu, et la production de cette preuve intégrée à un processus documenté l'aidera dans cette démarche.

Les organisations ne peuvent obtenir un consentement valable en vertu des lois sur la protection des renseignements personnels si elles ne présentent pas clairement aux utilisateurs leurs

politiques et pratiques en matière de traitement de l'information. La politique de confidentialité constitue un outil courant à cette fin, comme nous l'expliquons ci-après.

3. Politiques de confidentialité et ce qu'elles devraient contenir

Les organisations doivent être entièrement transparentes à propos de leurs pratiques en matière de protection des renseignements personnels.

- Les politiques de confidentialité doivent décrire en détail les renseignements recueillis, les fins pour lesquelles les renseignements sont utilisés et à qui ils sont communiqués.
- Ces politiques doivent être précises, faciles d'accès et simples à lire.
- Les organisations doivent examiner régulièrement leurs politiques de confidentialité et les mettre à jour au besoin.

La diffusion d'une politique de confidentialité constitue la façon la plus simple pour une organisation d'informer les utilisateurs de ses pratiques en matière de protection des renseignements personnels. Or, il ressort du ratissage d'Internet effectué sous l'égide du GPEN qu'à l'échelle mondiale, 23 % des sites Web ne comportent aucun politique de confidentialité.

Les individus doivent recevoir suffisamment d'information pour comprendre ce qu'ils autorisent lorsqu'ils donnent leur consentement. Ils devraient savoir :

- quels renseignements sont recueillis, en particulier si les renseignements ne viennent pas directement d'eux;
- la raison pour laquelle les renseignements sont recueillis;
- à quelles fins les renseignements seront utilisés;
- qui aura accès aux renseignements;
- la façon dont les renseignements seront protégés;
- pendant combien de temps ils seront conservés;
- s'ils peuvent se soustraire à certaines pratiques, comme la publicité comportementale; et,
- dans le cas où les renseignements sont communiqués à des tierces parties :
    - de quels types de tierces parties il s'agit;
    - ce que les tierces parties feront avec les renseignements;
    - si les tierces parties se trouvent dans un autre pays et sont susceptibles d'être assujetties à d'autres lois.

Les organisations doivent présenter l'information sur la protection des renseignements personnels en des termes faciles à comprendre et à lire pour le consommateur moyen[5]. À cette fin, elles peuvent fournir des explications claires en choisissant un niveau de langue adapté à un public varié et une taille de police facile à lire. La politique de confidentialité doit également être accessible de manière visible, par exemple grâce à un hyperlien sur la page de destination de

[5] Pour obtenir d'autres avis pratiques, les organisations de la Colombie-Britannique peuvent consulter le document d'orientation provincial intitulé *Practical Suggestions for your Organization's Website's Privacy Policy*.

l'organisation, de sorte que les utilisateurs puissent facilement la trouver. Les organisations doivent également s'assurer que la politique de confidentialité est facilement accessible à partir de tous les appareils que l'individu peut utiliser, notamment un téléphone intelligent, une tablette, un appareil de jeu et un ordinateur personnel.

Quand une organisation a l'intention d'apporter des modifications importantes à sa politique de confidentialité, elle devrait en aviser les utilisateurs à l'avance et envisager de leur demander de confirmer qu'ils y consentent avant l'entrée en vigueur de ces modifications. Une nouvelle entente de communication des renseignements personnels à une tierce partie ou l'utilisation de ces renseignements à une nouvelle fin constituent des exemples de modifications importantes.

Enfin, à titre de pratique exemplaire, les organisations doivent procéder régulièrement à une vérification de leurs pratiques de gestion de l'information pour s'assurer que les renseignements personnels sont traités de la manière décrite dans leur politique de confidentialité.

La transparence des pratiques de protection des renseignements personnels est un processus dynamique qui ne prend pas fin au moment de l'affichage de la politique de confidentialité mais qui se poursuit au fur et à mesure que les sites Web croissent et évoluent. Pour obtenir des renseignements généraux sur les pratiques de gestion de la protection des renseignements personnels, veuillez consulter notre document d'orientation intitulé *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*.

4. Les politiques de confidentialité ne sont pas toujours suffisantes

La communication des pratiques en matière de protection des renseignements personnels: il n'existe pas d'approche universelle

- La façon dont les pratiques sont communiquées devrait dépendre du contexte, du public et du niveau de complexité du traitement des renseignements personnels par l'organisation.
- Outre les politiques de confidentialité, d'autres types de communications relatives à la vie privée, comme les avis juste-à-temps, doivent fournir des explications sur la protection des renseignements personnels à des étapes clés de l'expérience de l'utilisateur.
- Les organisations doivent faire preuve de créativité quand elles décident du moment et de la façon de fournir aux utilisateurs de l'information sur la protection des renseignements personnels.

Ce que nous apprennent les études pourtant sur les politiques de confidentialité

Ce n'est pas d'aujourd'hui que les organisations ont recours aux politiques de confidentialité pour faire part de leurs pratiques de gestion de l'information au public. Toutefois, au fil des ans, ces politiques ont été la cible de nombreuses critiques en raison du jargon juridique et obscur de leur libellé et de l'effort requis pour les lire. En effet, selon une étude abondamment citée, les internautes auraient besoin de 244 heures par année pour lire les politiques de confidentialité des sites qu'ils ont visités.

L'étude du Commissariat sur les sites Web canadiens très fréquentés et leur communication de renseignements personnels à des tierces parties a par ailleurs révélé que les pratiques des organisations en matière de protection de la vie privée ne sont pas toujours communiquées de manière satisfaisante aux consommateurs. Il ressort du ratissage d'Internet effectué sous l'égide du GPEN que 33 % des politiques de confidentialité consultées étaient d'une utilité limitée pour le consommateur moyen à la recherche d'une explication claire concernant la façon dont les renseignements personnels sont utilisés.

Selon un sondage du Commissariat effectué en 2012, les Canadiens consultent rarement les politiques de confidentialité en ligne et quand ils le font, ils les trouvent souvent obscures. Seulement un répondant sur cinq a déclaré lire toujours (6 %) ou souvent (14 %) ces politiques, tandis que 29 % les lisent parfois, 26 % rarement et 24 % jamais. Soixante-deux pour cent des répondants estiment que les politiques de confidentialité sont assez vagues (36 %) ou très vagues (26 %).

En vertu des lois canadiennes sur la protection des renseignements personnels, les politiques et pratiques de gestion de l'information peuvent être communiquées de diverses façons. Par exemple, selon le principe de transparence énoncé dans la LPRPDA, la méthode choisie pour communiquer les pratiques en matière de protection de la vie privée « est fonction de la nature des activités de l'organisation et d'autres considérations ».

Nul doute que les politiques de confidentialité jouent un rôle important quand il s'agit de rendre des comptes, mais elles peuvent être trop longues, obscures et ne pas bien communiquer l'information. Au fil des expériences vécues en matière de surveillance de la législation sur la protection des renseignements personnels applicable au secteur privé, il est devenu de plus en plus clair pour les commissariats que, dans de nombreux cas, les politiques de confidentialité dans l'environnement en ligne ne suffisent pas pour respecter les exigences de la loi concernant le consentement. Ceci est particulièrement vrai pour les technologies mobiles.

Amélioration des politiques de confidentialité

Des efforts louables ont été déployés pour améliorer les politiques de confidentialité. Par exemple, les explications concernant les pratiques en matière de protection de la vie privée peuvent prendre différentes formes et être utilisées pour présenter de l'information à différents moments au cours de l'expérience en ligne. Le Commissariat a indiqué dans ses *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne* que les organisations devraient réfléchir à la façon d'informer efficacement les individus de leurs pratiques en ayant recours à diverses méthodes de communication en temps réel, comme les bannières en ligne, les technologies multicouches et des outils interactifs tels que des fenêtres contextuelles qui apparaissent au passage de la souris[6].

[6] L'action de déplacer la souris sur une zone désignée fait apparaître une fenêtre contextuelle qui contient du texte (tiré de webopedia.com).

Avis « juste-à-temps »

La vitesse à laquelle les opérations ont lieu constitue un facteur important dans l'obtention d'un consentement valable dans l'environnement en ligne. Les utilisateurs veulent avoir rapidement accès aux services et à l'information, et ils éprouvent souvent un sentiment d'urgence au moment de prendre des décisions sur la communication des renseignements les concernant. Il est donc important de mettre l'information pertinente sur la protection des renseignements personnels à l'avant-plan, là où elle est bien visible et facile à consulter et à comprendre de manière intuitive. Par exemple, si l'âge d'un utilisateur est requis pour l'inscription à un service en ligne, un avis juste-à-temps expliquant pourquoi ce renseignement est demandé devrait apparaître près de l'endroit où l'utilisateur doit saisir l'information.

Avis multicouches

Les avis multicouches[7] facilitent la compréhension des textes fastidieux et complexes en présentant d'emblée un résumé des principaux points. Après avoir lu ces points, l'utilisateur a la possibilité de cliquer pour avoir accès à un avis condensé présentant toute l'information de base de manière concise et facile à lire. L'utilisateur peut également consulter la version intégrale de la politique de confidentialité qui traite de l'ensemble des exigences légales.

Icônes

On envisage d'utiliser des icônes[8] pour simplifier la communication des principales pratiques en matière de gestion de l'information d'une organisation. L'idée consiste à concevoir des icônes qui communiqueraient aux utilisateurs ce qu'ils veulent savoir, par exemple : le site communique-t-il les renseignements personnels à des tierces personnes? Le site procède-t-il au ciblage comportemental? Pendant combien de temps le site conserve-t-il les renseignements personnels? Ces icônes normalisées apparaîtraient sur les sites Web et permettraient aux utilisateurs de décider rapidement d'interagir ou non avec un site donné.

Attentes des utilisateurs

Les organisations devraient tenir compte des attentes des utilisateurs au moment de décider des pratiques à mettre en évidence et du moment pour le faire. Par exemple, en cas d'utilisation ou de communication d'information à une tierce personne, ce à quoi l'utilisateur ne peut raisonnablement s'attendre, l'organisation se doit d'être encore plus transparente et claire dans ses explications. Les avis juste-à-temps ou les icônes constituent alors une bonne façon d'attirer l'attention sur les pratiques en matière de protection des renseignements personnels.

Comme on l'explique dans le *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*, de nombreuses entités accèdent également à l'information en arrière-plan – réseaux de publicité, courtiers en données et entreprises d'analyse des données. Il est essentiel

---

[7] The Center for Information Policy Leadership, Hunton & Williams LLP. *Ten steps to develop a multilayered privacy notice.*

[8] Par exemple, le Mozilla Privacy Icons Project.

d'attirer l'attention des utilisateurs sur ces entités et leurs pratiques au moment où ils doivent prendre la décision de communiquer ou non leurs renseignements personnels.

Dans les *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, le Commissariat expose les inconvénients d'un recours excessif aux politiques de confidentialité pour obtenir un consentement valable. Il invite plutôt les organisations à utiliser divers outils de communication, comme les bannières en ligne, la technologie multicouches et les outils interactifs, pour expliquer leurs pratiques.

Difficultés propres aux technologies mobiles

Ce qui vaut pour la communication des pratiques en matière de protection de la vie privée dans l'environnement en ligne fixe est encore plus vrai dans l'environnement des technologies mobiles. Dans cet environnement, les nouveaux modèles opérationnels évoluent constamment, le public est diversifié et l'information est traitée encore plus vite. De plus, le support ne se prête pas à de longues explications.

Quand le temps et l'attention de l'utilisateur sont ce qui prime, les organisations doivent mettre en évidence les questions relatives à la protection des renseignements personnels aux étapes décisionnelles de l'expérience de l'utilisateur, soit lorsque celui-ci est susceptible de porter attention à l'information qu'on lui transmet et qu'il a besoin de directives. Par exemple, quand on demande aux utilisateurs de fournir des renseignements, notamment à l'étape de l'inscription, il y a lieu de préciser l'utilité de chaque renseignement et la façon dont il sera utilisé. Pour être efficace, l'information sur la protection des renseignements personnels doit être optimisée malgré les limites imposées par la petite taille de l'écran.

Notre guide sur les applications mobiles pour la promotion de pratiques exemplaires auprès des développeurs d'applications mobiles reconnaît que la communication efficace de l'information sur les choix en matière de protection des renseignements personnels n'est pas un exercice aisé. Outre les politiques de confidentialité, les utilisateurs devraient recevoir des avis précis et ciblés quand ils doivent prendre une décision sur la communication de leurs renseignements personnels. À cet égard, un avis efficace doit également tenir compte de la connaissance qu'ont les utilisateurs des concepts décrits et du fait que leur attention est sollicitée sur divers fronts.

5. Les enfants et les jeunes

Les organisations doivent tenir compte des considérations propres aux enfants et aux jeunes en ce qui a trait à la gestion des renseignements personnels, et s'y adapter.

- Les renseignements concernant les enfants sont considérés comme étant sensibles et méritent une attention particulière en vertu des lois sur la protection des renseignements personnels.
- Les organisations devraient mettre en place des approches novatrices pour présenter de l'information sur la protection des renseignements personnels aux enfants et aux jeunes en tenant compte de leur développement cognitif et affectif et de leur expérience de vie..

La capacité des enfants et des jeunes de fournir un consentement valable en ce qui a trait à la communication de leurs renseignements personnels en ligne dépend grandement de leur développement cognitif et affectif. Compte tenu des difficultés éprouvées par les adultes pour comprendre ce qu'il advient de leurs renseignements personnels dans un environnement en ligne, il serait irréaliste de s'attendre à ce que les enfants comprennent parfaitement les complexités et les risques de la communication de leurs renseignements personnels en ligne. Dès lors, la législation sur la protection des renseignements personnels applicable au secteur privé autorise le consentement par l'intermédiaire d'une personne autorisée, comme un parent ou le tuteur légal.

De façon générale, les renseignements concernant des enfants sont considérés comme sensibles et méritent une plus grande protection en vertu de la loi. Par exemple, selon les *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne* du Commissariat, les organisations devraient éviter de suivre et de profiler sciemment les enfants sur les sites Web conçus à leur intention compte tenu de la grande difficulté d'obtenir un consentement valable auprès des très jeunes utilisateurs d'Internet.

Dans une enquête portant sur Nexopia, réseau social en ligne à l'intention des jeunes, le Commissariat s'est entre autres demandé si un consentement valable avait été obtenu pour la collecte des renseignements au moment de l'inscription. Dans ses conclusions, le Commissariat a émis des doutes quant à l'efficacité de s'en remettre passivement aux utilisateurs en supposant qu'ils liront et accepteront les modalités d'une longue politique de confidentialité afin d'obtenir leur consentement. Le Commissariat a indiqué :

> *Des études récentes sur l'utilisation d'Internet chez les jeunes, ainsi que les messages récurrents qu'entend le Commissariat de la part de jeunes utilisateurs par le truchement de son programme de sensibilisation, révèlent que, bien que certains jeunes lisent les politiques de confidentialité en ligne, il est plus facile d'obtenir le consentement des jeunes si on utilise des techniques interactives et novatrices conçues spécialement pour eux dans le but de les informer des répercussions de leurs décisions sur leur vie privée avant qu'ils ne cliquent, que si on recourt à des liens menant aux conditions d'utilisation et aux politiques de confidentialité.*

Nexopia a accepté de présenter sa politique de confidentialité d'une manière qui tient compte de l'âge de ses utilisateurs, par exemple en affichant la politique en sections thématiques sur lesquelles on peut cliquer.

Conclusion

En vertu des lois canadiennes sur la protection des renseignements personnels applicables au secteur privé, les organisations sont tenues d'obtenir le consentement avant la collecte, l'utilisation et la communication de renseignements personnels. Le consentement est considéré comme valide si l'intéressé a été suffisamment bien informé des pratiques de traitement de l'information de l'organisation pour pouvoir raisonnablement comprendre ce qu'il autorise en donnant son consentement.

Les organisations devraient avoir des politiques de confidentialité claires, détaillées et accessibles en ligne. Elles devraient également s'efforcer de communiquer l'information sur la protection des

renseignements personnels à des étapes clés de l'expérience de l'utilisateur pour aider ce dernier à comprendre la façon dont les renseignements personnels le concernant seront utilisés en ligne.

Les organisations devraient adapter leurs pratiques aux changements survenus quant aux expériences des utilisateurs dans l'environnement en ligne de façon à obtenir un consentement valable. On les encourage à communiquer avec les utilisateurs de manière plus créative, dynamique et interactive.

Une plus grande transparence des pratiques en matière de protection de la vie privée aidera à donner aux utilisateurs l'assurance que leurs renseignements personnels sont traités avec respect et augmentera leur confiance dans les activités en ligne. La confiance est essentielle pour que l'économie numérique canadienne puisse prospérer et que les Canadiens tirent parti des avantages économiques offerts par Internet.

DOCUMENTS DE RÉFÉRENCE ET RESSOURCES

- Task force on consumer consent, London School of Economics. *From Legitimacy to informed consent: mapping best practices and identifying risks*, mai 2009.
- The Department of Commerce Internet Policy Task Force. *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, décembre 2010.
- La Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*, rapport préliminaire du personnel de la FTC, décembre 2010.
- La Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, rapport du personnel de la FTC, mars 2012.
- Calo, Ryan M. *Against Notice Scepticism*, juillet 2011.
- Lawson, Philippa et Mary O'Donoghue. « Approaches to consent in Canadian data protection law », dans *Lessons from the Identity Trail,* chapitre 2.
- Perrin, Stephanie, Heather H. Black , David H. Flaherty et T. Murray Rankin. *The Personal Information Protection and Electronic Documents Act: An Annotated Guide,* 2001.
- Cranor, Lorrie Faith. *Privacy Tool User Studies*, novembre 2012. Présentation au National Telecommunications and information Administration internet Policy Task Force.
- Kerr, I. et coll. *Soft Surveillance. Hard Consent*.
- Article 29 Working Party. *Opinion 15/2011 on the definition of consent*, le 13 juillet 2011.
- Commissariat à la protection de la vie privée. Outil d'auto-évaluation – LPRPDE.
- OCDE. « Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandations de l'OCDE », dans *OECD Digital Economy Papers*, n° 120, OECD Publishing, 2006.

Facteurs importants à prendre en compte pour l'obtention d'un consentement valable en ligne

Une organisation est tenue d'obtenir le consentement valable d'une personne avant de recueillir, d'utiliser et de communiquer des renseignements personnels.

- Les personnes doivent être informées des pratiques de gestion de l'information d'une organisation pour être en mesure de donner un consentement jugé valable en vertu des lois sur la protection des renseignements personnels.
- Les fins pour lesquelles l'organisation recueille, utilise et communique des renseignements personnels doivent être précisées au moment de la collecte ou avant.
- Si l'organisation décide d'utiliser les renseignements personnels à une nouvelle fin après leur collecte, elle doit en informer les personnes concernées et obtenir leur consentement.
- L'obtention du consentement ne dégage pas l'organisation de ses autres obligations en vertu des lois sur la protection des renseignements personnels, comme la responsabilité générale, les mesures de sécurité et un motif raisonnable de recueillir, d'utiliser et de communiquer les renseignements personnels.

Les organisations doivent être entièrement transparentes à propos de leurs pratiques en matière de protection des renseignements personnels.

- Les politiques de confidentialité doivent décrire en détail les renseignements recueillis, les fins pour lesquelles les renseignements sont utilisés et à qui ils sont communiqués.
- Ces politiques doivent être précises, faciles d'accès et simples à lire.

Communication des pratiques en matière de protection des renseignements personnels: il n'existe aucune approche universelle

- La façon dont les pratiques sont communiquées devrait correspondre à l'environnement, au public et au niveau de complexité du traitement des renseignements personnels par l'organisation.
- Outre les politiques de confidentialité, d'autres types de communication relative à la vie privée, comme les avis juste-à-temps, les icônes et les avis multicouches, doivent fournir des explications sur la protection des renseignements personnels à des étapes clés de l'expérience de l'utilisateur.
- Les organisations doivent faire preuve de créativité au moment de décider quand et comment fournir aux utilisateurs de l'information sur la protection des renseignements personnels.

Les organisations doivent tenir compte des considérations propres aux enfants et aux jeunes en ce qui a trait à la gestion des renseignements personnels, et s'y adapter.

Les renseignements concernant les enfants sont considérés comme étant sensibles et méritent une attention particulière en vertu des lois sur la protection des renseignements personnels.

Les organisations devraient mettre en place des approches novatrices pour présenter de l'information sur la protection des renseignements personnels aux enfants et aux jeunes en tenant compte de leur développement cognitif et affectif et de leur expérience de vie.