Deloitte.

Rapport sur la collecte et l'utilisation des renseignements personnels des Canadiens par les fournisseurs de services sans fil et les entités tierces

6 janvier 2017
ISBN : BC92-92/2017F-PDF
978-0-660-07480-1

Table des matières

1. Sommaire

1.1. But et objectifs

Le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) s'est engagé à s'assurer que le Code sur les services sans fil (le Code) est efficace, et a entrepris en 2016 un examen du Code qu'il poursuivra en 2017 afin de mesurer l'efficacité des objectifs de ce dernier, notamment pour veiller à ce que les consommateurs aient une meilleure compréhension de leurs services et qu'ils soient en mesure de prendre des décisions éclairées en matière de services sans fil.

Ce rapport a pour objectif général d'offrir un aperçu de la collecte et de l'utilisation des renseignements personnels (RP) des Canadiens par des fournisseurs de services sans fil (FSSF) et des entités tierces. Le rapport vise à :

- contribuer à améliorer la compréhension générale qu'a le CRTC des enjeux actuels et émergents relatifs à la protection des renseignements personnels au sein du marché des services sans fil afin de l'aider à atteindre les objectifs de la *Loi sur les télécommunications*;
- appuyer le CRTC dans le cadre de son examen de 2016-2017 du Code, code obligatoire imposé en tant que condition de fournir ces services aux FSSF en vertu de l'article 24 de la *Loi sur les télécommunications*, en présentant ses observations sur la façon dont le Code atteint ses objectifs sur le plan de ses dispositions relatives à la protection des renseignements personnels.

1.2 Résumés des conclusions

Ce rapport est basé sur une recherche primaire constituée d'entrevues menées auprès de quinze chefs de la protection des renseignements personnels de FSSF canadiens, et sur une recherche secondaire d'articles. Le résumé des grandes conclusions de la recherche suit.

La collecte et l'utilisation de RP des consommateurs par des FSSF tiennent compte tant des besoins opérationnels des FSSF que de la protection des renseignements personnels des consommateurs.

Alors que le Code a créé une uniformité au sein de l'industrie aux yeux des consommateurs, tous les chefs de la protection des renseignements personnels de FSSF considèrent que c'est la *Loi sur la protection des renseignements personnels et les documents électroniques* (« LPRPDE ») qui est le pilier principal de la règlementation et des normes de la protection des renseignements personnels et

qui doit régir cette dernière dans l'industrie des services sans fil. Les FSSF recueillent des RP conformément aux obligations qui leur incombent conformément à la LPRPDE, et les objectifs de cette collecte sont décrits de manière appropriée dans leurs politiques sur la protection des renseignements personnels. Les FSSF rapportent qu'ils font usage des RP des consommateurs dans le cadre de leurs activités opérationnelles.

Les FSSF ne vendent pas de renseignements personnels de consommateurs à de tierces parties

Les FSSF rapportent qu'ils ne vendent pas de RP de consommateurs à de tierces parties, et ce, en aucune circonstance. Toutefois, les FSSF partagent effectivement des RP de consommateurs avec différentes tierces parties lorsque ces dernières leur offrent un service qui vise à soutenir leurs activités opérationnelles (p. ex. impression et envoi de facture aux consommateurs).

Les FSSF ont mis sur pied des rôles et des responsabilités concernant la protection des renseignements personnels

Les FSSF de toutes tailles ont mis en place un modèle de responsabilité en matière de protection des renseignements personnels afin d'intégrer la protection des renseignements personnels des consommateurs à leur organisation. Ce modèle est généralement fonction de la taille de l'organisation (c.-à-d. grand FSSF, marque dérivée ou petit FSSF), ce qui correspond aux diverses structures présentes dans d'autres secteurs d'activités.

La majorité des FSSF ont mis en place une procédure officielle et documentée en matière d'atteinte à la vie privée

La majorité des FSSF ont une politique ou une procédure officielle et documentée en matière d'atteinte à la vie privée; l'ampleur et le caractère officiel de la politique sont, de manière générale, proportionnels à la taille du FSSF.

Les restrictions contractuelles constituent l'outil principal dont les FSSF se servent pour restreindre l'utilisation et la collecte par les tierces parties des RP des consommateurs

Les données probantes suggèrent que les restrictions contractuelles représentent l'outil principal dont se servent les FSSF pour restreindre la collecte et l'utilisation de RP des consommateurs par de tierces parties, mais que d'autres méthodes dont la nature varie parmi les différents FSSF (p. ex. des vérifications) sont aussi utilisées.

De nos jours, l'usage de RP de consommateurs à des fins complémentaires constitue une rareté dans l'industrie des services sans fil

Les FSSF n'utilisent pas régulièrement les RP des consommateurs à de nouvelles fins qui sortent du cadre de ce qui était prévu à l'origine, mais s'ils l'ont fait ou

lorsqu'ils l'ont fait, ils ont reçu le degré de consentement requis. Les chefs de la protection des renseignements personnels des FSSF sont conscients des préférences des consommateurs en ce qui concerne les différentes fonctions et tâches permettant de s'assurer que le consentement a été correctement obtenu lorsqu'une nouvelle utilisation ou une divulgation de RP est envisagée.

La plupart des FSSF envisagent d'offrir aux consommateurs des services qui intègrent des technologies émergentes

Les résultats des entrevues au sujet des technologies émergentes mettent en lumière la rapidité à laquelle le marché canadien des services sans fil et l'offre aux consommateurs évoluent. Au moment où les entrevues ont eu lieu, la plupart des FSSF canadiens envisageaient d'offrir des services qui intégraient les technologies émergentes (p. ex. l'Internet des objets ou la réalité augmentée) aux consommateurs de services sans fil, mais l'ampleur de l'adoption prévue et l'échéancier de la mise en œuvre de ces technologies n'avaient toutefois pas été envisagés, et ainsi, les exigences en matière de protection des RP liées à ces technologies n'avaient pas non plus été entièrement considérées.

Cependant, et bien que ce soit à différents degrés et parfois seulement de façon accessoire, les FSSF ont déjà commencé à s'aventurer dans l'univers des technologies émergentes. En effet, des solutions d'Internet des objets sont déjà offertes par certains FSSF, mais il faut toutefois mentionner que la grande majorité de ces services sont destinés à de grandes entreprises et non pas à des particuliers. Quelques FSSF offrent aussi des technologies portables, comme les montres intelligentes, en tant qu'accessoires aux appareils mobiles de leurs clients. Les grands FSSF offrent pour leur part des casques de réalité virtuelle que les consommateurs peuvent utiliser avec leur téléphone intelligent. La plupart des FSSF vendent des téléphones intelligents à partir desquels les consommateurs peuvent télécharger des applications de réalité augmentée offertes par de tierces parties, comme l'application Pokémon Go. Bien que ce type d'application soit accessible par les réseaux des FSSF, ces derniers n'ont pas d'entente contractuelle directe avec les tierces parties qui offrent ces applications; ce sont plutôt les consommateurs qui acceptent l'entente de confidentialité des fournisseurs d'applications.

Avis et consentement, l'erreur humaine et l'Internet des objets : les plus grands défis en matière de protection des renseignements personnels dans le marché des services sans fil d'aujourd'hui

Les FSSF ont établi la liste des enjeux suivants qui représentent les plus grands défis relatifs à la protection des renseignements personnels des consommateurs dans le marché des services sans fil actuel : avis et consentement, erreur humaine, Internet des objets, complexités juridiques, transparence, menaces externes, intention malveillante et données massives. En raison de la complexité grandissante de l'offre de services, des technologies, du marché des services sans fil et du marché actuel en général, les chefs de la protection des renseignements personnels

sont aujourd'hui confrontés aux défis que posent la formulation d'avis compréhensibles pour les consommateurs et l'obtention d'un consentement éclairé de leur part. Les chefs de la protection des renseignements personnels ont aussi exprimé leurs préoccupations à l'égard d'erreurs qui pourraient être commises par des employés et qui pourraient être la cause d'incidents liés à la protection des renseignements personnels ou d'atteinte à la vie privée. Ils considèrent aussi que l'Internet des objets représente un défi distinct parce qu'ils ne peuvent pas contrôler ce que les consommateurs partagent en fait de RP parmi leurs différentes applications et leurs différents appareils, mais qu'il existe malgré tout un risque lié à la protection des RP de leurs clients.

Les défis liés à la protection des renseignements personnels dans le marché des services sans fil actuel ne sont pas sans rappeler ceux qui existent dans les autres industries

Les résultats des entrevues ont démontré que les plus grands défis liés à la protection des renseignements personnels dans le marché des services sans fil actuel sont de même nature que ceux qui existent au sein d'autres industries, notamment l'obtention du consentement éclairé de la part des consommateurs et la formulation d'avis compréhensible dans un environnement de plus en plus complexe, ainsi que la protection des renseignements personnels des consommateurs dans un contexte de technologies émergentes.

Les consommateurs ne comprennent pas toujours bien ce que la divulgation de renseignements personnels par les FSSF signifie

Bien que les politiques relatives à la protection des renseignements personnels des FSSF qui participaient à la recherche faisaient état des divulgations autorisées des RP de consommateurs, la nature de certaines de ces divulgations semble déborder de l'idée que peut se faire un consommateur sur ce que représente une divulgation de RP. Par exemple, il se peut qu'un client de service sans fil n'envisage pas qu'il soit possible que ses renseignements personnels soient communiqués pour le développement de produits, le marketing, la recherche et les services à un agent d'une tierce partie, et des termes tels que « marketing » et « recherche » sont peut-être trop vagues pour que les consommateurs comprennent bien leur signification dans ce contexte.

Les consommateurs bénéficieraient d'une éducation plus poussée en ce qui concerne la protection des renseignements personnels

Les FSSF ont mentionné que les consommateurs bénéficieraient grandement d'une éducation plus poussée au sujet de la protection des renseignements personnels et des technologies d'échange d'information (p. ex. les médias sociaux) parce qu'ils pourraient mieux comprendre comment protéger leurs renseignements personnels, et qu'ainsi les compagnies pourraient en retour mieux répondre à leurs demandes.

Les FSSF ont mentionné qu'ils agissaient en conformité avec la plupart des règles en matière de protection des renseignements personnels du Code des services sans fil

Selon les résultats des entrevues, la plupart des FSSF considèrent qu'ils respectent généralement la plupart des règles en matière de protection des renseignements personnels du Code des services sans fil. Par exemple, chaque FSSF qui a participé aux entrevues a rendu accessible une politique sur la protection des renseignements personnels sur son site Web, et a aussi indiqué qu'il informe ses clients de modifications apportées à cette politique trente jours avant l'entrée en vigueur de ces modifications.

Toutefois, il est intéressant de souligner que le Code exige aussi que les clients des différents FSSF reçoivent une copie papier de la politique sur la protection des renseignements personnels du fournisseur à la signature d'un contrat, à moins que les clients n'acceptent expressément et en toute connaissance de cause de recevoir une copie électronique. De plus, le Code exige qu'une copie accessible de cette politique soit rendue disponible aux consommateurs, sur demande et sans frais, dans un format de rechange à l'intention des personnes handicapées[1]. Selon ce qui ressort des entrevues, seuls un grand FSSF et sa marque dérivée fournit à ses clients une copie papier de sa politique sur la protection des renseignements personnels à la signature d'une entente d'offre de services, et la plupart des FSSF, mais pas tous, offrent aussi cette politique dans un format de rechange pour les personnes handicapées.

Répercussions stratégiques

Les résultats des entrevues démontrent que les chefs de la protection des renseignements personnels considèrent que les enjeux liés à la protection des renseignements personnels au sein de leur industrie sont similaires à ceux rencontrés dans d'autres industries. À cet égard, il serait important que le CRTC collabore avec le Commissariat à la protection de la vie privée du Canada (CPVP) afin de veiller à ce que la réglementation propre à l'industrie des services sans fil s'harmonise avec celle des autres industries.

Les résultats des entrevues ont aussi démontré que bien que le Code a fait en sorte que les consommateurs comprennent mieux leurs droits de la protection des renseignements personnels et les options de services sans fil, c'est la LPRPDE qui doit régir la protection des renseignements personnels dans l'industrie des services sans fil selon tous les chefs de la protection des renseignements personnels des FSSF. C'est pourquoi toute modification apportée au Code en matière de protection des renseignements personnels devrait tenir compte des solides protections de renseignements personnels stipulées dans la LPRPDE et devrait être faite en collaboration avec le CPVP.

[1] Voir le paragraphe 310 http://crtc.gc.ca/fra/archive/2013/2013-271.pdf

Les résultats des entrevues démontrent que les FSSF considèrent qu'ils respectent les règles en matière de protection des renseignements personnels du Code, toutefois, le CRTC pourrait vouloir explorer cet aspect lors de sa révision du Code, et particulièrement en ce qui a trait aux copies papier et aux copies accessibles aux personnes handicapées.

2. Introduction

2.1 Contexte

En 2013, le Conseil a mis en place le Code sur les services sans fil (le Code), un code de conduite obligatoire pour les fournisseurs de services de téléphonie et de données sans fil mobiles de détail (FSSF). Le Code a été créé afin de permettre aux consommateurs de mieux connaître leurs droits et obligations aux termes des contrats qu'ils souscrivent avec des FSSF. Les principaux objectifs du Code sont d'assurer que le marché du sans-fil fonctionne d'une manière favorable aux consommateurs et de donner à ces derniers toute l'information dont ils ont besoin pour mieux comprendre leurs options de services sans fil. En 2016 et 2017, le Conseil effectue un examen du Code, dans le cadre de son Plan triennal 2016-2019, afin de « s'assurer qu'il répond aux objectifs fixés ». En plus de cet examen triennal, le Conseil a aussi réalisé des sondages d'opinion publique annuels sur les forfaits de services sans fil pour consommateurs depuis l'entrée en vigueur du Code.

Les dispositions du Code en matière de protection des renseignements personnels imposent aux FSSF de mener les activités suivantes :

- S'assurer que leurs contrats de services sans fil et les documents connexes (p. ex. la politique sur la protection des renseignements personnels) sont rédigés dans un langage clair que les clients peuvent facilement lire et comprendre;
- Remettre sans frais au client, avant qu'il quitte le point de vente, une copie permanente du contrat et de la politique sur la protection des renseignements personnels, ou lui envoyer une copie permanente de ces documents dans les 15 jours suivant son acceptation de l'entente, si elle est conclue par téléphone ou en ligne;
- Fournir au client une copie papier de la politique sur la protection des renseignements personnels, sauf si le client décide expressément qu'une copie électronique est acceptable;
- Inclure une description facile à lire de la politique sur la protection des renseignements personnels dans le contrat;
- Au moins 30 jours civils avant d'apporter des modifications à la politique sur la protection des renseignements personnels, donner aux clients un avis expliquant clairement ces modifications et indiquant leur date d'entrée en vigueur.

2.2 Portée

Le présent rapport propose une analyse approfondie des éléments suivants :

- Le type, la quantité et le caractère plus ou moins confidentiel des renseignements personnels que recueillent les FSSF;
- L'utilisation par les FSSF des données sur leurs clients, notamment en les communiquant, en les monnayant ou en les vendant à de tierces parties
- Mesures intégrées de protection de la vie privée;
- Traitement des atteintes à la vie privée par les FSSF;
- Comment les FSSF permettent aux clients de décider la façon dont sont traités leurs renseignements personnels;
- Restrictions mises en place par les FSSF en matière de collecte et d'utilisation des renseignements personnels par de tierces parties;
- Les plus grands défis liés à la protection de la vie privée des clients de services sans fil dans le marché actuel.

L'analyse et les constatations détaillées (voir la **Section 3**) englobent les recherches primaires et secondaires suivantes :

- Résultats d'entrevues menées auprès de neuf (9) responsables de la protection des renseignements personnels représentant quinze (15) FSSF;
- Information issue de recherches secondaires accessibles au public sur la collecte de données et la protection de leur confidentialité dans l'industrie des services sans fil;
- Références aux politiques sur la protection des renseignements personnels (documents publics) des quinze (15) FSSF participants;
- Résultats d'une entrevue réalisée auprès d'un spécialiste du Commissariat à la protection de la vie privée du Canada (CPVP).

2.3 Méthodologie

Ce rapport s'appuie sur les résultats de neuf (9) entrevues menées auprès de responsables de la protection des renseignements personnels représentant quinze (15) FSSF. Les fournisseurs participants appartiennent à l'une des catégories suivantes :

- **Principaux fournisseurs de services sans fil canadiens :** Les principaux FSSF sont les trois (3) grands fournisseurs canadiens du marché actuel du sans-fil qui ont le plus grand nombre de clients et d'employés.
- **Fournisseurs de services sans fil de marques dérivées :** Les FSSF de marques dérivées sont des prolongements des principaux FSSF en place; ils commercialisent des offres de services distinctes sous d'autres marques. Ces

FSSF ont généralement moins de clients et d'employés que les principaux FSSF.

- **Petits fournisseurs de services sans fil :** Il s'agit de FSSF indépendants des principaux FSSF, de taille plus modeste, qui emploient moins de personnel et comptent moins de clients que les principaux FSSF canadiens.

Les noms des FSSF participants figurent **à l'annexe A – Fournisseurs de services sans fil participants**. Pour des raisons de confidentialité, veuillez noter que l'identité des responsables de la protection des renseignements personnels n'est pas révélée dans ce rapport et que les commentaires cités ne sont attribués à aucun FSSF en particulier.

Les entrevues menées auprès des responsables de la protection des renseignements personnels couvraient au moins les questions suivantes (voir **l'annexe B – Exemple de questionnaire d'entrevue**) :

- Le type, la quantité et le caractère plus ou moins confidentiel des renseignements personnels que recueillent et utilisent les FSSF;
- L'éventuelle communication ou vente à des tiers de renseignements que le FSSF recueille sur ses clients et les mesures qu'il prend pour assurer leur confidentialité, le cas échéant;
- Les types de restriction que le FSSF impose à des tiers pour protéger les renseignements personnels de ses clients;
- Ce que fait leur propre FSSF (leur employeur) pour protéger les renseignements personnels de ses clients;
- Les moyens pris par le FSSF pour permettre aux clients de décider la façon dont sont traités leurs renseignements personnels (notamment l'obtention de leur consentement à ce que le FSSF utilise ces renseignements à d'autres fins que celles prévues initialement);
- La façon dont le FSSF informe ses clients d'un changement apporté à sa politique de protection des renseignements personnels;
- À quel moment et comment le FSSF avise ses clients en cas d'atteinte à la vie privée, et ce qu'il fait pour atténuer les répercussions de ces atteintes;
- Ce que le responsable de la protection des renseignements personnels considère comme les grands défis de l'heure en matière de protection de la vie privée des clients du sans-fil.

Le rapport examine aussi les points de vue d'un spécialiste de la protection de la vie privée du CPVP sur des questions relevant des mandats du Commissariat. Les résultats d'entrevues sont présentés à la **Section 3 – Analyse et constatations détaillées**. Cette section contient aussi de l'information issue de ses recherches primaires ainsi que sur des données accessibles au public sur la collecte de renseignements et la protection de leur confidentialité dans l'industrie des services sans fil.

Le rapport se concentre sur les **services mobiles** définis dans le contrat de services du FSSF ou auxquels un client peut s'abonner (p. ex. services téléphoniques, de messagerie texte ou de données sans fil mobiles). Bien que le téléphone intelligent soit l'appareil le plus souvent utilisé par ces abonnés, le rapport étudie aussi des enjeux de protection des renseignements personnels émergents liés à l'emploi d'autres appareils dans le cadre d'un contrat de services téléphoniques ou de données avec un FSSF, comme les tablettes, les montres intelligentes et les voitures branchées. Diverses technologies interviennent dans ces **enjeux de protection des renseignements personnels émergents**, telles que définies ci-dessous :.

Métadonnées : Une métadonnée est une donnée générée lors de l'emploi d'une technologie, donnée qui fournit des renseignements sur d'autres données. Dans le contexte des communications, les métadonnées donnent des précisions concernant la création, la transmission et la diffusion d'un message (p. ex. lieu de provenance d'un appel téléphonique). [2]

Internet des objets : Le terme Internet des objets (IdO) désigne le réseau grandissant des objets (p. ex., montres, véhicules) dotés d'une adresse IP qui leur permet de communiquer avec Internet, ainsi que les communications qu'établissent ces objets entre eux et d'autres appareils et systèmes sans fil. À titre d'exemple, un FSSF peut proposer des services connectés embarqués aux constructeurs d'automobiles et un appareil de télématique aux consommateurs. Certains ont fait remarquer que l'IdO fera profiter les consommateurs de nombreux avantages, en particulier dans le domaine des soins de santé puisque les patients pourront eux-mêmes surveiller leurs signes vitaux, ce qui réduira les besoins en séjours hospitaliers. [3]

Mégadonnées : Le terme mégadonnées désigne de très volumineux ensembles de données qui, lorsque soumises à une analyse computationnelle, peuvent révéler des profils, des tendances et des associations caractérisant notamment les comportements humains et les interactions sociales.

Réalité augmentée : Les technologies dites « de réalité augmentée » partagent plusieurs de ces caractéristiques distinctives : elles ont des propriétés de senseur donnant de l'information sur le monde réel, traitent l'information en temps réel et la communiquent à l'utilisateur, donnent des renseignements contextuels, peuvent

---

[2] Commissariat à la protection de la vie privée du Canada, Métadonnées et vie privée : Un aperçu technique et juridique, octobre 2014.
https://www.priv.gc.ca/media/1793/md_201410_f.pdf

[3] Rapport de la Federal Trade Commission (É.-U.). Internet of Things: Privacy & Security in a Connected World. Janvier 2015.
https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

reconnaître et suivre des objets du monde réel et sont mobiles ou même prêt-à-porter. [4]

Stockage infonuagique : Le terme « stockage infonuagique » désigne les services distants de maintenance, gestion et sauvegarde de l'information auxquels les utilisateurs peuvent accéder sur un réseau, soit en général par Internet. Dans un rapport récemment publié par l'Université de Toronto, on explique que diverses conceptions, certaines erronées, se sont progressivement greffées sur la notion originale de « nuage ». Ces fausses définitions peuvent laisser croire à la population que le nuage existe en dehors du monde physique et indépendamment des territoires et juridictions où sont exploités les équipements de télécommunications (p. ex. les serveurs) qui alimentent le nuage.[5]

Point d'échange Internet : On appelle « point d'échange Internet » les infrastructures matérielles auxquelles les grands fournisseurs de réseaux peuvent relier leurs réseaux afin d'échanger du trafic Internet. Les fournisseurs de services sans fil peuvent par exemple utiliser des points d'échange Internet pour savoir où et quand leurs clients utilisent leurs services en itinérance et pouvoir facturer ces services en conséquence.

[4] Tech Policy Lab, Université de Washington, Augmented Reality: A Technology and Policy Primer, septembre 2015.
http:// http://techpolicylab.org/augmented-reality-technology-policy-primer/
[5] Université de Toronto. Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World. 2015.
http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf.

3. Analyse et constatations détaillées

Cette section présente les constatations tirées d'entrevues menées auprès des responsables de la protection des renseignements personnels des FSSF et du spécialiste de la question du CPVP et ce qui ressort de l'examen de documents disponible publiquement sur la protection des renseignements personnels publiés par les FSSF et d'autres publications disponibles publiquement sur la collecte de renseignements et la protection de leur confidentialité dans l'industrie des services sans fil. Cette section contribuera à la compréhension qu'à le Conseil du type, de la quantité et du caractère plus ou moins confidentiel des renseignements personnels que recueillent et utilisent les FSSF, de leurs pratiques de communication ou de vente de renseignements à des tierce parties et des mesures que prennent les FSSF canadiens pour protéger les renseignements personnels de leurs clients. Cette section contibuera aussi à la compréhension générale qu'à le CRTC des enjeux de protection des renseignements personnels dans le marché des services sans fil en prévision de son prochain examen du.

3.1 Le type, la quantité et le caractère plus ou moins confidentiel des renseignements personnels que recueillent les FSSF

Dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) – la loi fédérale sur la protection des renseignements personnels à laquelle tous les FSSF sont assujettis – le terme « renseignement personnel » est défini comme « tout renseignement concernant un individu identifiable ».[6] Il peut s'agir de tout type de renseignement, par exemple : l'âge, le nom, un numéro d'identification personnelle, le revenu, l'origine ethnique ou le groupe sanguin; une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire; le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical, l'existence d'un différend entre un consommateur et un commerçant ou le projet d'une personne (p. ex. intention d'acquérir des biens et services). Les organisations assujetties à la LPRPDE, y compris les FSSF, ne

[6] Commissariat à la protection de la vie privée du Canada. Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La Loi sur la protection des renseignements personnels et les documents électroniques du Canada. Décembre 2015 p. 3 https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

peuvent recueillir que les renseignements personnels dont ils ont besoin pour des fins déterminées. La collecte doit se limiter aux renseignements raisonnablement requis dans les circonstances, en faisant la part des choses entre les besoins du client et son droit à la vie privée.

Comme l'ont précisé en entrevue les responsables de la protection des renseignements personnels, et selon les politiques des FSSF, disponibles en ligne, sur le respect de la vie privée, les FSSF recueillent tous les mêmes types de renseignements personnels (RP) pour les besoins de leurs activités d'affaires courantes. Les renseignements personnels suivants sont recueillis par les FSSF eux-mêmes : nom, numéro de téléphone, adresse de courriel, adresse de facturation, date de naissance (DDN), pièce d'identité délivrée par le gouvernement (ID), numéro d'assurance sociale (NAS) (aux fins de vérification de solvabilité seulement), historique de paiement, historique d'utilisation et données de localisation (pour la facturation seulement). La majorité des FSSF participants utilisent des fichiers témoins (« cookies ») sur leurs sites Web. Moins de la moitié retiennent l'enregistrement des appels (p. ex. à leurs centres de service à la clientèle), la langue de préférence du client ou des renseignements sur les autres utilisateurs autorisés du compte, sur les préférences du client ou sur les films qu'il a vus (s'il est aussi abonné à des services de télévision). Le **Tableau 2** détaille les types de renseignements personnels que les FSSF recueillent eux-mêmes sur leurs clients.

Tableau 1 : Types de renseignements personnels que les FSSF recueillent eux-mêmes sur leurs clients

	FSSF 1	FSSF 2	FSSF 3	FSSF 4	FSSF 5	FSSF 6	FSSF 7	FSSF 8	FSSF 9	FSSF 10	FSSF 11	FSSF 12	FSSF 13	FSSF 14	FSSF 15
Nom	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Numéro de téléphone	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Adresse de courriel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Adresse de facturation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DDN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	FSSF 1	FSSF 2	FSSF 3	FSSF 4	FSSF 5	FSSF 6	FSSF 7	FSSF 8	FSSF 9	FSSF 10	FSSF 11	FSSF 12	FSSF 13	FSSF 14	FSSF 15
NAS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enregistrement d'appels		✓	✓	✓	✓	✓						✓	✓		
Historique de paiement	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Historique d'utilisation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Données de localisation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Langue de préférence							✓	✓	✓			✓	✓		
Renseignements sur autres utilisateurs autorisés							✓	✓	✓			✓	✓		
Renseignements sur les préférences du client[7]							✓	✓	✓			✓	✓		
Historique des films[8]							✓	✓	✓						

Certains FSSF font appel à des tiers pour recueillir des renseignements personnels sur leurs clients. C'est par exemple le cas des principaux FSSF qui exploitent chacun leur réseau de détaillants pour faire des affaires « sur place » avec leurs clients (p. ex., kiosques aménagés dans des centres commerciaux). Ces réseaux de détaillants recueillent les mêmes types de renseignements personnels que ceux que collectent les FSSF lorsque les clients s'adressent directement à eux pour s'abonner (p. ex., nom, numéro de téléphone, adresse de courriel, DDN, ID, NAS). Les FSSF peuvent aussi obtenir indirectement des renseignements personnels sur un client lorsqu'ils font vérifier sa solvabilité par une agence d'évaluation du crédit (p. ex., Equifax). On a cependant constaté que la plupart des petits FSSF n'ont pas recours

[7] Recueillis lors de sondages ou lorsque le client parle avec des représentants du service à la clientèle.
[8] Informations compilées par le service de télévision qu'offre le FSSF.

à la collecte indirecte des RP sur leurs clients et qu'ils font plutôt eux-mêmes cette collecte.

Tableau 2 : Types de RP que les FSSF font recueillir par des tiers

	FSSF 1	FSSF 2	FSSF 3	FSSF 4	FSSF 5	FSSF 6	FSSF 7	FSSF 8	FSSF 9	FSSF 10	FSSF 11	FSSF 12	FSSF 13	FSSF 14	FSSF 15
Nom		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Numéro de téléphone		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Adresse de courriel		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
DDN		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
ID		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
NAS		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Résultats de vérification de la solvabilité		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Historique d'utilisation							✓	✓	✓			✓	✓		
Données de localisation							✓	✓	✓			✓	✓		
Langue de préférence							✓	✓	✓			✓	✓		
Renseignements sur autres utilisateurs autorisés							✓	✓	✓			✓	✓		
Renseignements sur les							✓	✓	✓						

	FSSF 1	FSSF 2	FSSF 3	FSSF 4	FSSF 5	FSSF 6	FSSF 7	FSSF 8	FSSF 9	FSSF 10	FSSF 11	FSSF 12	FSSF 13	FSSF 14	FSSF 15
préférences du client[9]															

Les entrevues ont révélé que six (6) des FSSF utilisent un système établi de classification de la confidentialité (p. ex. cote élevée, moyenne ou faible) pour les RP qu'ils recueillent sur leurs clients. Tous ces fournisseurs donnent leur cote de confidentialité la plus élevée aux données financières (p. ex., résultats de vérification de la solvabilité, renseignements sur la carte de crédit). Huit (8) autres FSSF utilisent actuellement une forme non officielle (p. ex. non documentée) de gradation de la confidentialité des RP, et un seul FSSF n'emploie aucune méthode pour déterminer la confidentialité de ces données. Plusieurs FSSF tiennent aussi compte d'autres exigences que celles prévues par la législation sur la protection des RP pour déterminer le caractère plus ou moins confidentiel de ces renseignements. À titre d'exemple, bien des FSSF qui collectent des renseignements personnels s'assurent en outre de respecter la norme de sécurité des données de l'industrie des cartes de paiement.

La plupart des FSSF participants collectent des métadonnées, lesquelles servent uniquement à des fins opérationnelles (p. ex., durée d'un appel téléphonique pour produire la facture), à l'exception de deux petits FSSF qui ne possèdent pas l'infrastructure requise pour en recueillir.

Les résultats des entrevues et l'examen des politiques sur la protection des renseignements personnels nous indiquent que les FSSF recueillent les RP conformément aux obligations imposées par la LPRPDE et qu'ils expliquent convenablement les raisons de cette pratique dans leurs politiques sur la protection des renseignements personnels.

3.2 Utilisation par les FSSF des données sur leurs clients, notamment en les communiquant, en les monnayant ou en les vendant à de tierces parties

[9] Recueillis lors de sondages ou lorsque le client parle au téléphone avec des représentants du service à la clientèle.

Le CPVP énonce des lignes directrices pour les organisations relativement aux façons appropriées d'utiliser, de communiquer et de conserver les renseignements personnels des clients à des fins d'exploitation. Cela comprend :

- N'utiliser ou ne communiquer des renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis, à moins que la personne concernée ne donne son consentement.
- Ne conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins établies.
- Conserver les renseignements personnels utilisés pour prendre une décision au sujet d'une personne pendant un temps raisonnable. De cette façon, celle-ci peut y avoir accès et demander réparation au besoin.
- Détruire, ou dépersonnaliser les renseignements dont vous n'avez plus besoin aux fins précisées ou prévues par la loi.[10]

Selon les entrevues réalisées et l'examen des politiques des FSSF sur la protection de la vie privée, les FSSF utilisent les renseignements personnels des clients pour appuyer leurs activités opérationnelles, y compris les activités décrites ci-dessous :

- Envois de communications aux clients par la poste
- Envois de factures aux clients par la poste
- Création de matériel de marketing (à l'interne)
- Validation de l'identité des clients
- Traitement des paiements des clients
- Service d'aide à la clientèle
- Compréhension des besoins et des préférences des clients
- Compréhension de l'admissibilité des clients aux produits et services
- Élaboration et amélioration des offres de produits et de services
- Gestion des activités commerciales, y compris les questions d'emploi
- Respect des exigences législatives et réglementaires

Tous les agents de la protection des renseignements personnels ont formellement déclaré que les FSSF ne vendent pas les renseignements personnels des clients à de tierces parties. Selon les politiques sur la protection de la vie privée des FSSF participants à l'enquête, les renseignements personnels des clients sont

[10] Commissariat à la protection de la vie privée du Canada Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La Loi sur la protection des renseignements personnels et les documents électroniques du Canada. Décembre 2015 P. 23. https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

communiqués à de tierces parties pour offrir un soutien opérationnel au FSSF (p. ex. facturation et envois postaux). Voir le **Tableau 3** ci-dessous pour consulter la liste des fins pour lesquelles les renseignements personnels des clients sont couramment communiqués à de tierces parties.

Tableau 3 : Fins pour lesquelles les renseignements personnels des clients sont couramment communiqués à de tierces parties.

	FSSF 1	FSSF 2	FSSF 3	FSSF 4	FSSF 5	FSSF 6	FSSF 7	FSSF 8	FSSF 9	FSSF 10	FSSF 11	FSSF 12	FSSF 13	FSSF 14	FSSF 15
Envois postaux	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Facturation	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓
Développement de produits		✓	✓	✓	✓						✓	✓	✓	✓	
Commercialisation		✓	✓	✓	✓						✓	✓	✓	✓	
Vérification de la solvabilité		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	
Communication exigée par la loi ou lors d'une situation d'urgence	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transmission de renseignements à un agent autorisé du client		✓	✓	✓	✓		✓	✓	✓			✓	✓	✓	
Recherche ou traitement de données		✓	✓	✓	✓		✓	✓	✓			✓	✓		
Services à un agent d'une tierce partie du FSSF (p. ex., ventes)		✓	✓	✓	✓		✓	✓	✓			✓	✓		✓
Facturation des interurbains	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Bien que les politiques des FSSF sur la protection de la vie privée prévoient la communication des types de renseignements personnels des clients mentionnés ci-dessus, il peut s'agir, dans certains cas, de communications autres que ce qu'un

client peut généralement considérer comme la communication de renseignements personnels. Par exemple, il se peut qu'un client de service sans fil n'envisage pas qu'il soit possible que ses renseignements personnels soient communiqués pour le développement de produits, le marketing, la recherche et les services à un agent d'une tierce partie. De plus, des termes tels que « marketing » et « recherche » sont assez vagues, et il se peut que les clients ne comprennent pas totalement à quoi correspondent ces communications sans d'abord demander plus de renseignements au FSSF, une pratique qui n'a pas fréquemment cours dans l'industrie des services sans fil. On peut donc conclure que les FSSF devraient penser à des moyens pour préciser aux clients les façons dont les renseignements personnels sont communiqués, autres que celles auxquelles ils peuvent raisonnablement s'attendre. [11]

3.3 Mesures intégrées de protection de la vie privée

La LPRPDE est fondée sur les dix (10) principes relatifs à la protection des renseignements personnels contenus dans le code type de l'Association canadienne de normalisation (« Code type de la CSA »), qui ont été énoncés dans la *Norme nationale sur la protection des renseignements personnels* en 1996. Le code type de la CSA est utilisé partout au Canada et dans le monde comme fondement des lois, des politiques et des procédures sur la protection des renseignements personnels. Voici les dix principes qui constituent le fondement du Code type de la CSA :

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte
5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte à l'égard du non-respect des principes

Selon le CPVP, les entreprises doivent savoir que, en plus des principes définis dans la LPRPDE, elles ont l'obligation suprême selon laquelle une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins

[11] Commissariat à la protection de la vie privée du Canada Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La *Loi sur la protection des renseignements personnels* et les documents électroniques du Canada. Décembre 2015 https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

qu'une personne raisonnable estimerait acceptables dans les circonstances.[12] Il s'agit d'un élément essentiel pour conserver la confiance des clients.

Lors des entrevues, les responsables de la protection des renseignements personnels ont parlé d'un certain nombre de mesures de protection des renseignements personnels adoptées pour protéger les renseignements personnels des clients, notamment :

La dépersonnalisation

Les FSSF utilisent des données groupées dépersonnalisées pour faire des choix éclairés quant aux services qu'ils offrent aux clients et/ou aux endroits où ils établissent leurs réseaux (p. ex. les tours).

L'anonymisation des renseignements personnels

Les FSSF anonymisent les données d'un client quand la personne cesse d'être cliente (p. ex. deux (2) ans après l'échéance ou la résiliation d'un contrat). Cela permet au FSSF de continuer d'utiliser les données anonymisées pour obtenir des perspectives d'affaires.

Cadres de responsabilisation en matière de protection des renseignements personnels

Un cadre de responsabilisation en matière de protection des renseignements personnels désigne un modèle de responsabilités et d'obligations relatives à la protection des renseignements personnels qui est intégré à l'organisation dans le cadre des différents rôles qu'on y retrouve (p. ex. agent de la protection des renseignements personnels, chef de la protection des renseignements personnels). Tous les FSSF ayant participé à l'enquête ont mis en place un cadre de responsabilisation en matière de protection des renseignements personnels, mais leurs structures varient. En règle générale, le chef de la protection des renseignements personnels, ou une personne occupant un poste équivalent, est le premier responsable de la protection et de la sécurité des renseignements personnels des clients. Dans certains cas, le chef de la protection des renseignements personnels est aidé par un chef adjoint de la protection des renseignements personnels, ou une personne occupant un poste équivalent. Les grands FSSF ont davantage tendance à adopter un modèle dispersé selon lequel chaque service possède son propre « champion des renseignements personnels » qui sert d'agent de liaison en matière de renseignements personnels au sein de son service, et fournit un précieux point de vue commercial aux responsables de la protection des renseignements personnels dans l'organisation. Les grands FSSF

[12] Commissariat à la protection de la vie privée du Canada Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La Loi sur la protection des renseignements personnels
et les documents électroniques du Canada. Décembre 2015
https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

confient également diverses facettes de leur structure de gouvernance en matière de renseignements personnels à un bureau du responsable de la protection des renseignements personnels, à une équipe chargée de la cybersécurité, à une équipe de prévention des pertes de données, à une équipe juridique ou à une équipe responsable de la sécurité dans l'entreprise. Les FSSF de marques dérivées ont tendance à tirer avantage des mesures de protection des renseignements personnels déjà en place chez les grands FSSF auxquels ils sont affiliées. Les petits FSSF ont des structures de responsabilité moins importantes en matière de protection des renseignements personnels, qui prévoient généralement un poste de directeur général responsable de la protection des renseignements personnels, dont relèvent un ou deux autres employés participant au traitement des plaintes des clients liées à la protection des renseignements personnels. Ces différentes structures de responsabilité sont cohérentes avec celles des autres secteurs d'activités, dans lesquels la maturité de la gouvernance en matière de protection des renseignements personnels est souvent proportionnelle à la taille et aux ressources de l'organisation.

Service à la clientèle axé sur la protection des renseignements personnels

Comme on le mentionne dans le Code, les contrats et les documents connexes des FSSF (p. ex. la politique sur la protection des renseignements personnels) doivent stipuler comment un client peut porter plainte au sujet des services sans fil.[13] Tous les FSSF ayant participé à l'enquête décrivent dans leur site Web et dans leur politique sur la protection des renseignements personnels comment un client peut porter plainte (p. ex. numéro de téléphone du centre d'appels, adresse courriel pour porter plainte). Pour le traitement des plaintes liées à la protection des renseignements personnels et au service, les FSSF ont recours à divers moyens afin d'offrir des services de règlement des plaintes similaires. Les sites Web de tous les FSSF ayant participé à l'enquête proposent une boîte aux lettres sur la protection des renseignements personnels, une adresse courriel à laquelle les clients peuvent envoyer leurs plaintes, et/ou un centre d'appels où des représentants du service à la clientèle sont en mesure de traiter les demandes de renseignements et les plaintes liées à la protection des renseignements personnels. Certains des grands FSSF ont aussi créé un groupe responsable des enquêtes pour traiter les problèmes plus graves liés à la protection des renseignements personnels.

Sécurité

La responsabilité de faire en sorte que les mesures de sécurité appropriées sont prises pour protéger les renseignements personnels des clients incombe généralement à des secteurs différents selon les FSSF. Pour de nombreux FSSF, le chef de la sécurité (ou une personne occupant un poste équivalent) est le premier responsable de la mise en place de mesures de sécurité appropriées, et il est généralement soutenu par une équipe pouvant inclure une équipe de prévention de

[13] Conseil de la radiodiffusion et des télécommunications canadiennes, Code sur les services sans fil, juin 2013 http://crtc.gc.ca/eng/archive/2013/2013-271.pdf.

la perte de données. D'autres responsables de la protection des renseignements personnels ont indiqué que la responsabilité à ce chapitre est partagée entre le chef de la protection des renseignements personnels et le chef de la sécurité, ainsi que leurs équipes de soutien respectives.

Globalement, il semble que les FSSF de toutes tailles disposent d'un modèle de responsabilisation en matière de protection des renseignements personnels au sein de leur organisation. Le type de modèle de responsabilisation en matière de protection des renseignements personnels est généralement fonction de la taille de l'organisation (c.-à-d. grand FSSF, marque dérivée ou petit FSSF), ce qui correspond aux diverses structures dans d'autres secteurs d'activités. Par exemple, le directeur général d'un FSSF relativement modeste peut être le premier responsable des renseignements personnels et être assisté d'un adjoint, tandis qu'un grand FSSF peut compter sur les services d'une équipe complète d'intervenants pour les questions de renseignements personnels (p. ex. un agent de la protection des renseignements personnels, une équipe responsable de la protection des renseignements personnels, des champions ou des chefs de la protection des renseignements personnels au sein des divers services).

3.4 Traitement des atteintes à la vie privée par les FSSF

De nouvelles modifications à la LPRPDE rendent obligatoires les dispositions sur la notification des atteintes à la sécurité des données et l'enregistrement des incidents de sécurité en vertu de la *Loi sur la protection des renseignements personnels numériques*[14] nouvellement adoptée. Une fois adoptées, les dispositions de la *Loi sur la protection des renseignements personnels numériques* relatives à la notification des atteintes modifieront la LPRPDE pour exiger des organisations qu'elles informent non seulement les personnes concernées, mais aussi le CPVP et les autres intervenants pertinents en cas d'atteinte. En vertu des dispositions relatives à la notification des atteintes, les organisations privées – incluant les FSSF – qui se rendent compte qu'elles ont subi une atteinte aux mesures de sécurité doivent procéder à l'analyse de la situation afin de déterminer si l'atteinte présente ou non un « risque réel de préjudice grave» à l'endroit d'un individu dont les renseignements personnels sont visés par l'atteinte. S'il existe un tel risque, les organisations doivent signaler l'atteinte au CPVP, ainsi qu'aux personnes touchées par l'atteinte, selon les modalités réglementaires prévues dans la *Loi sur la protection des renseignements personnels numériques*. La *Loi sur la protection des renseignements personnels numériques* exige de plus la consignation de toutes les atteintes, qu'il y ait ou non risque de préjudice grave.

[14] LE GOUVERNEMENT DU CANADA La *Loi sur la protection des renseignements personnels numériques* Juin 2015 http://laws-lois.justice.gc.ca/PDF/2015_32.pdf.

Conformément à l'objet des modifications à la LPRPDE, nous avons noté lors des entrevues que douze (12) des FSSF ont mis en place une politique ou une procédure officielle sur les atteintes à la vie privée pour faciliter la gestion de ces atteintes. Les responsables de la protection des renseignements personnels de douze (12) des FSSF ayant participé à l'étude respectent les lignes directrices relatives aux atteintes à la vie privée fournies par le CPVP[15]. Ces douze FSSF ont mis en place une politique ou une procédure officielle sur les atteintes à la vie privée et comptent sur les services d'une équipe de personnes responsables de déceler les atteintes et d'y réagir avec l'appui d'autres équipes au sein de l'organisation. Les grands FSSF possèdent également des documents de référence exhaustifs sur la façon d'intervenir en cas d'atteintes à la vie privée. Les trois autres FSSF sont de petite taille, n'ont jamais connu d'atteintes à la vie privée et n'ont pas actuellement de politique ou de procédure documentée sur les atteintes à la vie privée.

Lors des entrevues, les responsables de la protection des renseignements personnels de tous les FSSF ont indiqué que les notifications aux clients en cas d'atteinte à la vie privée s'effectuent au cas par cas. Ainsi, un incident mineur d'atteinte à la vie privée peut justifier qu'une notification soit envoyée par la poste avec la prochaine facture du client, tandis qu'une importante atteinte à la vie privée ayant des répercussions graves pour le client (p. ex. vol d'identité) peut justifier de joindre le client par téléphone ou par courriel peu après que l'étendue de l'atteinte a été confirmée. Tous les FSSF ayant participé à l'étude préconisent le principe « le client d'abord », ce qui signifie que si le client peut subir un préjudice en raison de l'atteinte, ils informeront le client. Toutefois, c'est le FSSF qui détermine le moment où il notifiera le client et la façon dont il le fera en fonction de l'ampleuret de la gravité de l'atteinte à la vie privée ou de l'incident.

Pour les FSSF ayant une politique documentée sur les atteintes à la vie privée, la notification des clients en cas d'atteinte à la vie privée mettant en cause une tierce partie serait traitée de la même façon qu'une atteinte ayant eu lieu chez le FSSF, sauf que les équipes responsables des affaires juridiques et des approvisionnements du FSSF interviendraient davantage. Par exemple, le cadre de la protection des renseignements personnels d'un grand FSSF a fait remarquer que, lorsqu'il a été informé d'une atteinte à la vie privée chez un fournisseur tiers de téléphones intelligents, le FSSF a communiqué avec ses clients pour les informer de cette atteinte en vertu du principe « le client d'abord ».

Les renseignements obtenus lors des entrevues ont démontré que les grands FSSF sont prêts à se conformer aux modifications apportées à la LPRPDE, tandis que les FFSSF de plus petite taille ont encore du travail à faire pour se conformer aux changements à venir.

---

[15] Commissariat à la protection de la vie privée du Canada Principales étapes à suivre par les organisations en cas d'atteinte à la vie privée Août 2007. https://www.priv.gc.ca/media/2090/gl_070801_02_e.pdf.

3.5 Comment les FSSF permettent aux clients de décider la façon dont sont traités leurs renseignements personnels

Comme le décrit le CPVP dans sa trousse d'outils[16] et comme le confirme une spécialiste de la vie privée au CPVP, la LPRPDE a pour objet d'établir l'équilibre entre les besoins commerciaux de l'organisation et le droit de la personne à la vie privée. Cet équilibre est en partie possible si l'on fait en sorte que les clients puissent décider la façon dont sont traités leurs renseignements personnels. Dans un effort pour offrir aux clients des FSSF les outils dont ils ont besoin pour décider la façon dont sont gérés leurs renseignements personnels, le Code décrit les éléments suivants que devraient adopter les FSSF :

- Une politique sur la protection des renseignements personnels facile à lire et à comprendre par les clients.
- Une pratique visant à fournir, sans frais, aux clients une version papier permanente du contrat et de la politique sur la protection des renseignements personnels immédiatement au point de vente (ou envoyer une version permanente de la politique sur la protection des renseignements personnels dans les 15 jours, pour une entente convenue au téléphone ou en ligne);
- Une brève explication de la politique sur la protection des renseignements personnels intégrée au contrat.
- Une pratique prévoyant l'envoi d'un avis aux clients un minimum de trente (30) jours civils avant d'apporter des changements à la politique sur la protection des renseignements personnels, expliquant clairement quels sont les changements et le moment où ils entreront en vigueur.[17]

[16] Commissariat à la protection de la vie privée du Canada Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La *Loi sur la protection des renseignements personnels*
et les documents électroniques du Canada. Décembre 2015
https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

[17] Conseil de la radiodiffusion et des télécommunications canadiennes, Code sur les services sans fil Juin 2013 http://crtc.gc.ca/eng/archive/2013/2013-271.pdf.

Les observations qui suivent ont été faites relativement à la façon dont les FSSF ayant participé à l'étude mettent facilement à la disposition des consommateurs leur politique sur la protection des renseignements personnels :

- Chacun des FSSF participants possède une politique sur la protection des renseignements personnels accessible au public sur son site Web, décrivant quels sont les renseignements qu'ils recueillent, la façon dont ils utilisent ces renseignements ainsi que la façon dont ils protègent les renseignements personnels de leurs clients.
- Selon ce qui ressort des entrevues, seuls un grand FSSF et sa marque dérivée fournissent à ses clients une copie papier de sa politique sur la protection des renseignements personnels à la signature d'une entente d'offre de services.
- Tous les responsables de la protection des renseignements personnels confirment que les clients peuvent demander un exemplaire de leur politique sur la protection des renseignements personnels, en version papier ou électronique, en tout temps, par téléphone ou par courriel (à une adresse courriel spécifique ou dans une boîte aux lettres sur la protection des renseignements personnels dans leur site Web) ou en s'informant dans un magasin.
- La majorité des FSSF rendent accessible leur politique sur la protection des renseignements personnels dans des formats différents, sur demande (p. ex. en braille, en gros caractères).
- La majorité des FSSF ayant participé à l'étude propose un résumé simplifié de la politique sur la protection des renseignements personnels dans leurs contrats de service.
- Selon les entrevues effectuées, il est rare que des clients demandent des versions papier de leur politique sur la protection des renseignements personnels aux FSSF de toutes tailles.

Les observations qui suivent ont été faites relativement à la façon dont les FSSF ayant participé à l'étude communiquent à leurs clients les changements apportés à leurs politiques sur la protection des renseignements personnels :

- Selon les entrevues effectuées auprès des responsables de la protection des renseignements personnels des FSSF, ils n'apportent pas régulièrement des changements aux politiques sur la protection des renseignements personnels.
- Lorsque des changements sont apportés, tous les FSSF expliquent que dans le cadre de leurs communications avec leurs clients, ils en informent ces derniers au moins 30 jours à l'avance sur le site Web de l'entreprise.
- Certains parmi les grands FSSF publient également des FAQ (foires aux questions) sur leur site Web pour expliquer la nouvelle politique.
- En plus d'utiliser leur site Web pour informer les clients des changements à la politique sur la protection des renseignements personnels, certains FSSF envoient également des encarts aux clients avec leur facture, des messages texte ou des courriels pour les informer du changement.

- Les FSSF qui comptent un nombre important de clients utilisant des forfaits à paiements mensuels ont davantage tendance à transmettre les notifications aux clients par message texte.

Dans la soumission du CPVP présentée à l'instance publique du CRTC en 2012, qui a donné lieu à la création du Code, le CPVP souligne qu'il est essentiel de fournir des politiques sur la protection des renseignements personnels qui sont favorables aux clients et qui donnent suffisamment d'information sur la façon dont les renseignements personnels sont utilisés, ainsi que des instructions sur la façon de déposer une plainte[18]. En règle générale, les renseignements obtenus lors des entrevues auprès des responsables de la protection des renseignements personnels sont cohérents avec les observations faites par le CPVP lors des audiences publiques relatives au Code.

Les clients peuvent aussi décider la façon dont sont traités leurs renseignements personnels en choisissant d'adhérer à diverses fonctionnalités additionnelles ou de s'en retirer. Par exemple, l'un des grands FSSF et sa marque dérivée utilisent un programme de marketing comportemental en ligne pour créer des publicités personnalisées destinées aux clients. Pour ce programme, ils ont obtenu le consentement exprès des clients et le grand FSSF a également collaboré avec le CPVP pour faire en sorte de protéger les renseignements personnels pendant tout le cycle de vie du programme. D'autres FSSF n'utilisent pas de fonctionnalités additionnelles et ceux qui envisagent de le faire reconnaissent qu'ils obtiendraient d'abord le consentement exprès de leurs clients. Aucun des FSSF ayant participé à l'étude, selon les entrevues effectuées, n'utilise les renseignements personnels des clients à des fins secondaires sans obtenir leur consentement exprès.

Douze (12) des FSSF ayant participé à l'étude s'appuient sur le consentement exprès et tacite, tandis que trois (3) petits FSSF s'appuient uniquement sur le consentement tacite et n'utilisent pas les renseignements personnels des clients à d'autres fins que celles initialement prévues.[19] Par exemple, quand un client s'abonne à un forfait de téléphonie auprès d'un FSSF, il s'attend à ce que ses renseignements personnels (c.-à-d. son nom, son adresse postale) soient utilisés par le FSSF pour lui offrir le service. Les FSSF ont tendance à s'appuyer sur le consentement tacite quand l'activité fait partie du service qu'ils offrent et qu'elle fait

[18] Commissariat à la protection de la vie privée du Canada Instance dans le but d'établir un code obligatoire pour les fournisseurs de services sans fil mobiles : Soumission du Commissariat à la protection de la vie privée du Canada à l'intention du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). Décembre 2012 https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_crtc_121204/.

[19] Le consentement explicite est expressément donné, verbalement, par écrit ou au moyen d'une action précise en ligne (p. ex. en cliquant sur « J'accepte »), tandis qu'il y a consentement implicite lorsque l'intervention de la personne visée permet raisonnablement de conclure au consentement. Tiré de : Commissariat à la protection de la vie privée du Canada, *Trousse d'outils en matière de vie privée : Guide à l'intention des entreprises et des organisations*, Décembre 2015. https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

partie des attentes générales. Pour les vérifications de solvabilité, tous les FSSF ayant participé à l'étude obtiennent d'abord le consentement exprès. Les FSSF n'utilisent pas fréquemment les RP des consommateurs à de nouvelles fins qui sortent du cadre de ce qui était prévu à l'origine, mais s'ils le font, ils demandent tous le consentement des clients en fonction du degré de sensibilité des renseignements.

Ces résultats indiquent que les FSSF sont conscients des préférences des consommateurs en ce qui concerne les différentes caractéristiques à considérer et ce qui doit être fait pour garantir que le consentement a été correctement accordé lorsqu'une nouvelle utilisation ou une divulgation de RP est envisagée.

3.6 Restrictions mises en place par les FSSF en matière de collecte et d'utilisation des renseignements personnels par des tierces parties

Dans le présent rapport, l'expression « tierces parties » désigne des fournisseurs externes de services publicitaires ou de marketing, des FSSF partenaires ou tout fournisseur offrant aux FSSF un service opérationnel (p. ex., l'impression de factures). Selon le CPVP,[20] les organisations devraient suivre les importants conseils suivants sur la transmission de renseignements personnels à de tierces parties :

- désigner une personne chargée de traiter tous les aspects du contrat liés à la protection de la vie privée;
- limiter l'utilisation des renseignements personnels aux fins nécessaires à l'exécution du contrat;
- ne communiquer les renseignements qu'en fonction des règles établies par votre organisation et des obligations législatives;
- diriger vers votre organisation les personnes qui souhaitent consulter les renseignements personnels les concernant;
- à l'achèvement du contrat, restituer les renseignements transmis ou les détruire;
- utiliser les mesures de sécurité qui s'imposent pour assurer la protection des renseignements personnels;
- au besoin, donner à votre organisation la possibilité de vérifier la mesure dans laquelle la tierce partie respecte les dispositions du contrat.

[20] Commissariat à la protection de la vie privée du Canada Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La Loi sur la protection des renseignements personnels
et les documents électroniques du Canada. Décembre 2015
https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

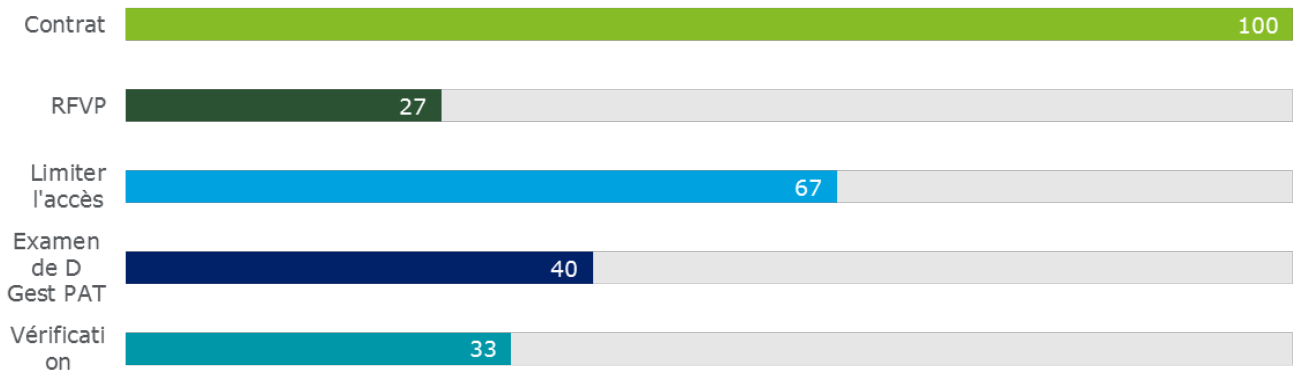
D’après les entrevues, tous les FSSF participants suivent une partie ou la totalité des conseils ci-dessus formulés par le Commissariat. Tous les FSSF se servent d’ententes contractuelles afin de restreindre la collecte et l’utilisation des renseignements personnels par de tierces parties. En outre, tous les responsables de la protection des renseignements personnels ont déclaré que leur FSSF préfère ne pas communiquer des renseignements personnels aux tierces parties si les fins commerciales pour lesquelles les services d’une tierce partie sont retenus peuvent être remplies adéquatement sans de tels renseignements. Une majorité des FSSF participants limite la collecte et l’utilisation des renseignements personnels des clients par les tierces parties en mettant en place divers contrôles d’accès (p. ex., accès en lecture seule). Plusieurs FSSF ont mis en place leurs propres mécanismes de restriction des tierces parties qui sont uniques à leur organisation. Par exemple, un conseiller ou une conseillère juridique d’un FSSF peut aviser l’équipe d’approvisionnement des renseignements auxquels une tierce partie pourrait avoir accès et ceux qui ne sont pas nécessaires aux fins commerciales de la tierce partie. L’accès aux renseignements sera alors limité en conséquence pour la tierce partie.

Les grands FSSF étaient plus susceptibles d’avoir un processus d’examen d’évaluation des facteurs relatifs à la vie privée (EFVP), de la vérification ou de la prévention de la perte de données aux fins de vérification des tierces parties. L’instauration de mécanismes de vérification des tierces parties contribue au renforcement des pratiques générales de gestion du risque d’une organisation et valide la force des contrôles en matière de protection des renseignements personnels des clients déjà en place.

Quatorze FSSF participants sur quinze ont un processus en place pour assurer la restitution ou la destruction des renseignements personnels des clients partagés précédemment avec une tierce partie aux fins commerciales pertinentes. Par exemple, à l’achèvement du projet d’un FSSF, une tierce partie doit restituer ou détruire (avec une preuve de destruction) les renseignements personnels recueillis des clients du FSSF. Que les renseignements soient restitués ou détruits reste à la discrétion du FSSF. Seul le plus petit des FSSF participants n’a pas cette pratique en place, en raison, ici encore, de son interaction limitée avec de tierces parties.

Les FSSF de marques dérivées ont tendance à recourir aux services de tierce partie obtenus par le FSSF parent, tandis que les petits FSSF, en raison de leur interaction limitée avec de tierces parties, ne disposent pas de pratiques officiellement documentées pour restreindre la collecte et l’utilisation de renseignements personnels de clients par une tierce partie. Le **graphique 1** ci-dessous présente ces outils limitant la divulgation de renseignements aux tierces parties.

Graphique 1 : Outils utilisés par les FSSF pour limiter la divulgation de renseignements aux tierces parties



*Les chiffres indiquent le pourcentage des FSSF participants

3.7 Fournisseurs de services sans fil et technologies émergentes

3.7.1 Fonctionnalités basées sur la localisation

Les services basés sur la localisation désignent les services offerts au moyen d'un téléphone mobile qui utilisent la géolocalisation de l'appareil. Tous les responsables interrogés ont expliqué que les FSSF utilisent le suivi géodépendant pour les cas d'urgence (p. ex., un appel au service 911). Certains des grands FSSF emploient également des données de géolocalisation à des fins de marketing ciblé, au moyen d'un préavis envoyé au client ainsi que d'un consentement exprès (p. ex., une disposition d'adhésion). En règle générale, les petits FSSF n'ont pas tendance à utiliser des fonctionnalités basées sur la localisation, à l'exception des cas d'urgence.

Le Centre pour la défense de l'intérêt public (CDIP), dans son rapport sur les technologies basées sur la localisation et la loi[21], avance qu'alors que les Canadiens utilisent de plus en plus les téléphones intelligents et d'autres appareils mobiles, il est possible que la LPRPDÉ ne protège pas suffisamment les Canadiens contre la collecte excessive des renseignements sur leur emplacement ou la mauvaise

[21] Le Centre pour la défense de l'intérêt public (CDIP). Déconnecté du réseau? Repérage des technologies basées sur la localisation et la Loi. Juin 2015. http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report_FR.pdf.

utilisation par les tierces parties. Le CDIP explique aussi que les fournisseurs de services de télécommunications canadiens peuvent actuellement disposer de l'accès le plus direct aux renseignements des utilisateurs d'appareils mobiles et qu'ils devraient, par conséquent, considérer la protection de la vie privée de leurs clients comme une priorité absolue. Alors que les responsables de la protection des renseignements personnels des FSSF ont déclaré que des données de géolocalisation sont recueillies auprès de clients, elles le sont aux fins indiquées seulement (comme décrit ci-haut) et elles ne sont pas directement utilisées par les FSSF autrement qu'à des fins opérationnelles ou sans un consentement positif.

3.7.2 L'Internet des objets (IdO) et la réalité augmentée

Aucun des responsables participants n'a indiqué que leur FSSF respectif offre actuellement des solutions IdO ou la réalité augmentée à leurs clients individuels. Cependant, les FSSF de toutes tailles ont exprimé un intérêt pour les technologies à l'avenir ou, du moins, ils désirent mieux comprendre les applications de réalité augmentée au sein de leur entreprise. Néanmoins, les FSSF ont commencé à s'aventurer dans le domaine des technologies émergentes, quoiqu'à divers degrés et parfois de manière marginale seulement. En effet, des solutions d'Internet des objets sont déjà offertes par certains FSSF, mais il faut toutefois mentionner que la grande majorité de ces services sont destinés à de grandes entreprises et non pas à des particuliers.

4.7.3 Stockage infonuagique, points d'échange Internet (IXP) et compétence

Au cours des entrevues avec les responsables de la protection des renseignements personnels, on a constaté que la majorité des FSSF se servait du stockage infonuagique, quelques-uns ayant déjà effectué des EFVP auprès de leur fournisseur tiers. Parmi les FSSF participants se servant du nuage, certains assurent qu'aucun renseignement personnel n'est transmis au nuage, alors que d'autres y stockent des renseignements personnels, tout en respectant des règles de compétence strictes[22] pour le faire. La majorité des FSSF se servant du nuage stockent uniquement des renseignements non sensibles dans le nuage et ils cherchent consciencieusement à répondre aux préoccupations des clients et à conserver leurs serveurs locaux. Les petits FSSF sont plus susceptibles de ne pas recourir aux services de stockage infonuagique en raison de leurs plus petits fonds de renseignements et de leurs ressources plus limitées, mais ils songent à utiliser ces services à l'avenir. Un des FSSF participants stocke un sous-ensemble de ses

[22] Ces règles se rapportent au pouvoir accordé par la loi à un tribunal pour se prononcer sur des questions de droit dans une région géographique donnée.

données de facturation de services sans fil dans le nuage. Les FSSF sont de plus en plus conscients des risques liés au stockage des données de facturation de services sans fil dans le nuage compte tenu des récentes préoccupations entourant les modèles de paiement des services sans fil. Ces préoccupations comprennent : l'éventuelle utilisation abusive des renseignements supplémentaires acquis sur les clients (p. ex., historique d'achat détaillé et marchands concernés); la possibilité accrue de « bourrage de facture de téléphone » (p. ex., des frais facturés sous des rubriques ambiguës ou trompeuses comme « frais de service » ou « autres frais »).[23]

Les conclusions tirées des entrevues correspondaient à celles d'un récent rapport de l'Université de Toronto qui recommandait que les organisations canadiennes évitent l'impartition de services de communications électroniques hors des frontières du pays.[24] Ce rapport indique que les points d'échange Internet publics canadiens peuvent contribuer à conserver le trafic de communications local. Si ces services sont externalisés, les organisations devraient soumettre le fournisseur de services tiers à une EFVP et à une évaluation des menaces et des risques (EMR), sans oublier de revoir les décisions passées en matière d'impartition.

Lorsqu'on les interroge au sujet des points d'échange Internet, les responsables de la protection des renseignements personnels de FSSF importants et de marques dérivées ont affirmé que leurs organisations sont en mesure d'utiliser de tels points canadiens et non canadiens aux fins de facturation seulement (p. ex., frais d'itinérance). Certains des petits FSSF sont uniquement en mesure d'utiliser des points d'échange Internet canadiens en raison de leur infrastructure. Tous les responsables ont indiqué que leurs FSSF ne répondent pas aux demandes internationales d'organismes d'application de la loi; une ordonnance judiciaire devra toujours être approuvée par un tribunal canadien avant qu'un FSSF canadien n'y réponde.

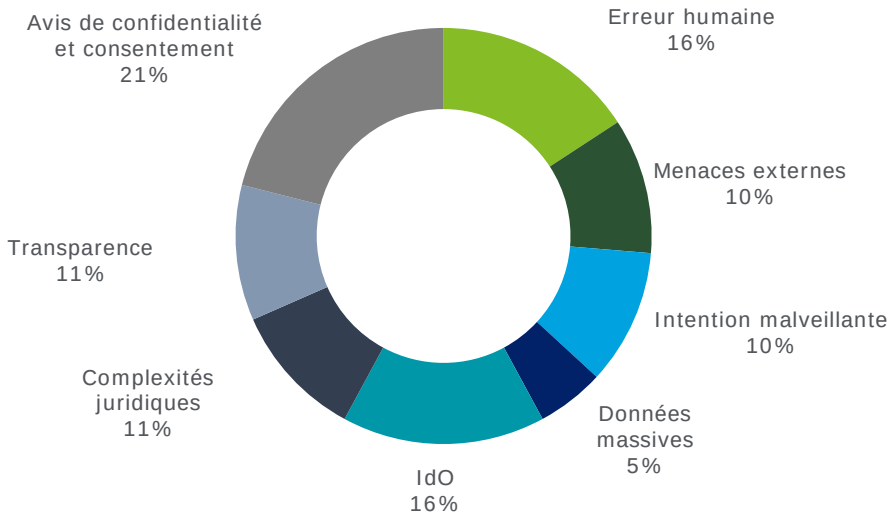
[23] Carlisle Adams, Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles. Juin 2013 https://www.priv.gc.ca/media/1774/mp_201306_f.pdf.

[24] Université de Toronto, Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World. 2015. http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf.

3.8 Les plus grands enjeux liés à la protection de la vie privée des clients de services sans fil dans le marché actuel

Les responsables de la protection des renseignements personnels des FSSF ont relevé les aspects suivants comme étant les plus grands enjeux liés à la protection de la vie privée des clients dans le marché actuel (voir le **graphique 2** ci-dessous).

Graphique 2 : Les plus grands enjeux liés à la protection de la vie privée des clients de services sans fil dans le marché actuel



Avis de confidentialité et consentement : Les responsables de la protection des renseignements personnels éprouvent des difficultés à fournir un préavis convenable aux clients et à obtenir un consentement adéquat de leur part. Les responsables participants y voient le résultat de la complexité croissante des services, des technologies, du marché des services sans fil et du marché actuel de manière plus générale.

Erreur humaine : Les responsables de la protection des renseignements personnels se disent préoccupés par les erreurs humaines, ou les fautes non intentionnelles commises par des employés qui pourraient être la cause d'incidents liés à la protection des renseignements personnels ou d'atteinte à la vie privée. Plusieurs d'entre eux perçoivent comme un défi la formation et la conscientisation des employés de manière continue et considèrent cela comme une cause possible de ces erreurs humaines.

Internet des objets (IdO) : Les responsables de la protection des renseignements personnels et le CPVP considèrent l'IdO comme un nouveau risque

pour la protection de la vie privée des clients de services sans fil. Les responsables appréhendent l'IdO comme un enjeu unique et comprennent qu'ils ne peuvent pas contrôler comment les personnes partagent leurs renseignements personnels d'une application ou d'un appareil à l'autre, mais qu'un risque pour la vie privée de leurs clients peut toujours être présent. Un récent rapport de recherche du CPVP portant sur l'Internet des objets soutient que les consommateurs du commerce de détail et à la maison pourraient en bénéficier puisqu'il offre une méthode pour analyser avec précision les comportements des consommateurs. Ces analyses permettent la mise en œuvre de pratiques de marketing de plus en plus personnalisées et cohérentes sur divers types d'appareils (p. ex., téléphones, tablettes)[25]. Inversement, parmi les risques pour la sécurité et la vie privée de l'IdO, il est possible, par exemple, que des données « désidentifiées » puissent être « réidentifiées ». [26]

Complexités juridiques : Les responsables de la protection des renseignements personnels ont souligné les défis causés par les lois multijuridictionnelles sur la protection des renseignements personnels. Pour se conformer aux différentes lois en la matière au Canada, les FSSF doivent y consacrer plus de temps et de ressources.

Transparence : Les responsables interrogés considèrent qu'accorder aux clients un degré raisonnable de transparence représente un défi. À titre d'exemple, certains FSSF reçoivent des demandes générales de renseignements concernant le compte d'un client nécessitant parfois des délais de plusieurs jours avant d'y accéder et de pouvoir répondre au client, ce qui oblige les FSSF à y consacrer du temps et des ressources. Ces FSSF souhaitent être transparents, mais de façon raisonnable. Le CPVP a également déterminé qu'il s'agit d'un nouvel enjeu important.

Menaces externes : Les responsables de la protection des renseignements personnels jugent les menaces externes (p. ex., des attaques par déni de service) comme l'un des plus importants obstacles à la protection de la vie privée des clients de services sans fil.

Intention malveillante : Les responsables estiment que l'intention malveillante ou les menaces internes (p. ex., un employé malveillant volant des renseignements relatifs aux cartes de crédit de clients) constituent l'un des principaux enjeux touchant la protection des renseignements personnels des clients.

Données massives : Les responsables se questionnent quant aux risques pour la vie privée que les analyses de données massives peuvent engendrer (p. ex., anonymisation de grandes quantités de données, exactitude des données).

---

[25] Commissariat à la protection de la vie privée du Canada L'Internet des objets : Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison. Février 2016. https://www.priv.gc.ca/media/1809/iot_201602_f.pdf

[26] Rapport de la Federal Trade Commission (É.-U.). Internet of Things: Privacy & Security in a Connected World.

Autres défis évoqués par le CPVP

Dans le cadre d'une entrevue menée auprès d'un spécialiste de la protection des renseignements personnels du CPVP, d'autres défis liés à la protection des renseignements personnels auxquels sont confrontés les FSSF ont été évoqués, notamment :

- les difficultés des petits FSSF qui ne disposent pas des mêmes ressources en protection de la vie privée que les grands FSSF;
- certains FSSF peuvent éprouver des problèmes d'adaptation à la nouvelle modification à la LPRPDE concernant la déclaration obligatoire d'une atteinte aux mesures de sécurité;
- le furetage des employés (p. ex., un membre de la famille consultant les renseignements du compte de services sans fil d'un de ses proches sans son consentement).

5. Conclusion et résumé des constatations

Les résultats des entrevues ont démontré que le secteur des services sans fil n'est pas nécessairement différent des autres secteurs lorsqu'il est question de protéger les renseignements personnels. La plupart des responsables de la protection des renseignements personnels ne voyaient pas les enjeux décrits dans la section d'analyse détaillée ci-dessus comme étant uniques à l'industrie des services sans fil. Plutôt, ces enjeux étaient considérés comme étant endémiques dans tous les secteurs en raison des récentes et constantes évolutions technologiques (p. ex., données massives, IdO).

Bien que la plupart des FSSF envisagent d'offrir des technologies émergentes, comme la réalité augmentée, aux clients des services sans fil, ils ont affirmé que ces types de services ne sont pas actuellement proposés à leurs clients individuels et que, par conséquent, ils n'intègrent pas actuellement des dispositifs protégeant la vie privée afin de régir ces technologies.

Néanmoins, les FSSF ont commencé à s'aventurer dans le domaine des technologies émergentes, quoiqu'à divers degrés et parfois de manière marginale seulement. En effet, des solutions d'Internet des objets sont déjà offertes par certains FSSF, mais il faut toutefois mentionner que la grande majorité de ces services sont destinés à de grandes entreprises et non pas à des particuliers.

Alors que les politiques sur la protection des renseignements personnels des FSSF participants présentent un survol des communications de renseignements personnels qu'ils pourraient effectuer, certaines de celles-ci peuvent excéder ce qu'un client considère habituellement comme une communication de renseignements personnels. Par exemple, il se peut qu'un client de service sans fil n'envisage pas qu'il soit possible que ses renseignements personnels soient communiqués pour le développement de produits, le marketing, la recherche et les services à un agent d'une tierce partie. De plus, des termes tels que « marketing » et « recherche » sont assez vagues, et il se peut que les clients ne comprennent pas totalement à quoi correspondent ces communications sans d'abord demander plus de renseignements au FSSF, une pratique qui n'a pas fréquemment cours dans l'industrie des services sans fil. On peut donc conclure que les FSSF devraient penser à des moyens pour préciser aux clients les façons dont les renseignements

personnels sont communiqués, autres que celles auxquelles ils peuvent raisonnablement s'attendre. [27]

Les conclusions du rapport ont également démontré, à l'instar des autres industries, que les plus importantes organisations disposent de davantage de ressources pour documenter les pratiques et politiques et, par conséquent, d'un cadre plus robuste et mature pour protéger les renseignements personnels. Au sein du secteur des services sans fil, les marques dérivées ont tendance à tirer parti des modèles établis par les marques mères. Il reste les petits FSSF, dont quelques-uns disposent de pratiques établies, alors que d'autres ont des cadres immatures en ce qui concerne la protection des renseignements personnels.

Plusieurs responsables de la protection des renseignements personnels ont indiqué que, dans le contexte actuel, l'élaboration de lois propres à une industrie peut décourager les innovations au sein du marché des services sans fil et créer des déséquilibres concurrentiels dans le marché en général. Alors que le Code a créé plus de cohérence pour les clients au sein du secteur, tous les responsables des FSSF jugent la LPRPDE comme étant la principale réglementation et la norme régissant la protection des renseignements personnels dans le secteur des services sans fil. En retour, les responsables de la protection des renseignements personnels des FSSF ont acquis une connaissance approfondie de la LPRPDE et ont mis en œuvre les mesures appropriées au sein de leurs organisations respectives pour assurer la conformité. C'est pourquoi toute modification apportée au Code en matière de protection des renseignements personnels devrait tenir compte des solides protections de renseignements personnels stipulées dans la LPRPDE et devrait être faite en collaboration avec le CPVP.

Peu importe le secteur d'activités, maintenir la confiance de la clientèle repose en grande partie sur l'équilibre entre les besoins des clients et leurs droits à la vie privée. Cela peut se faire en donnant aux clients des moyens pour contrôler leurs renseignements personnels de façon concrète. Un autre moyen utilisé pour protéger les droits à la vie privée, qui a également été exprimé par les responsables de la protection des renseignements personnels des FSSF, passe par l'éducation, non seulement au niveau de l'entreprise, mais aussi au niveau scolaire. Un programme éducatif à l'échelle du Canada sur la protection de la vie privée et les technologies d'échange d'information (p. ex., médias sociaux) aiderait grandement les consommateurs à mieux comprendre comment protéger leurs renseignements, afin que les entreprises, en contrepartie, répondent aux demandes des consommateurs.

---

[27] Commissariat à la protection de la vie privée du Canada Guide à l'intention des entreprises et des organisations : trousse d'outils en matière de vie privée – La *Loi sur la protection des renseignements personnels*
et les documents électroniques du Canada. Décembre 2015
https://www.priv.gc.ca/media/2039/guide_org_f.pdf.

Annexe A – FSSF participants

- Bell Mobilité
- Rogers
- TELUS
- Virgin Mobile
- Fido
- Chatr
- Koodo
- Public Mobile Inc.
- Brooke Telecom
- Cityphone
- Eastlink
- Execulink
- Hay Communications
- SaskTel
- WIND Mobile (Shaw)

Annexe B – Exemple de questionnaire d'entrevue

Les services de Deloitte S.E.N.C.R.L. ont été retenus pour rédiger un rapport au nom du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) sur la collecte et l'utilisation des renseignements personnels de Canadiens par des fournisseurs de services sans fil (FSSF) et des entités tierces. Ce rapport vise à aider le CRTC à effectuer le prochain examen de son Code et à lui permettre de mieux comprendre les enjeux de la protection des renseignements personnels dans le secteur des services sans fil mobiles de détail, lequel évolue rapidement. Pour la préparation du rapport, le CRTC nous a demandé de mener des entrevues auprès des agents de la protection de la vie privée de douze (12) FSSF canadiens. Veuillez noter que l'identité des agents de la protection de la vie privée demeurera confidentielle et qu'aucune des réponses ne sera associée au nom de votre entreprise. Cependant, le rapport inclura une liste des fournisseurs de services sans fil qui auront participé aux entrevues.

Le questionnaire suivant sera à la base de la discussion durant l'entrevue planifiée. Veuillez lire le présent questionnaire avant notre rencontre et préparez-vous à répondre aux questions. Veuillez noter que certaines réponses pourront comprendre des renseignements similaires à ceux fournis dans des réponses précédentes.

Si vous remplissez le rôle d'agent de la protection de la vie privée pour plus d'un FSSF, préparez-vous à répondre à toutes les questions séparément pour chaque fournisseur.

Question	Réponse
Section 1 : Responsabilité	
1. Quelle personne a-t-on désignée au sein de l'organisation pour traiter tous les aspects liés à la protection des renseignements personnels dans les contrats conclus avec les clients?	

Question	Réponse
2. À qui les plaintes liées aux questions de confidentialité doivent-elles être transmises?	
3. À qui a-t-on confié la responsabilité de prendre les mesures de sécurité qui s'imposent pour assurer la protection des renseignements personnels?	
Section 2 : Politique de protection des renseignements personnels	
4. De quelle façon les clients peuvent-ils accéder à votre politique de protection des renseignements personnels (autre qu'en ligne)? Dans quels formats la politique est-elle offerte? Comment les clients doivent-ils procéder pour obtenir une copie papier ou une copie sur un autre support de la politique de protection des renseignements personnels?	
5. Quelle méthode utilisez-vous pour informer les clients des modifications apportées à votre politique de protection des renseignements personnels? Quel est le délai entre la communication de ces mises à jour et leur entrée en vigueur?	
Section 3 : Collecte, utilisation, divulgation et destruction de renseignements personnels	
6. Quels types de renseignements personnels votre organisation recueille-t-elle directement auprès de ses clients?	

Question	Réponse
Ces types peuvent inclure notamment des historiques de paiement, des données sur l'emplacement et de l'information de suivi.	
7. Quels types de renseignements personnels votre organisation recueille-t-elle auprès de ses clients par l'entremise d'un tiers? Ces types comprennent notamment des renseignements personnels provenant de fournisseurs de système d'exploitation de téléphone intelligent, de fournisseurs tiers d'applications ou d'annonceurs, ainsi que des métadonnées.	
8. Votre organisation classe-t-elle les renseignements personnels qu'elle collecte selon leur niveau de sensibilité? Si oui, comment?	
9. Comment votre organisation obtient-elle le consentement des personnes concernées ? Particulièrement, comment votre organisation obtient-elle le consentement de ses clients lorsque des renseignements personnels seront utilisés à d'autres fins que celles prévues initialement? (Veuillez fournir des exemples.)	
10. Avez-vous un processus en place pour déterminer si le traitement des renseignements personnels demeure conforme aux fins énoncées dans la politique de protection des renseignements (et pour lesquelles le consentement avait été obtenu initialement)? Si oui, veuillez décrire le processus. Qui est responsable de la gestion de ce processus?	

Question	Réponse
11. Offre-t-on aux clients le choix d'accepter ou de refuser des fonctions supplémentaires (p. ex., personnalisation du profil, publicité et fonctions géodépendantes)? Veuillez décrire la manière dont ces choix sont offerts.	
12. Comment limitez-vous la communication de renseignements à des tiers à ce que votre autorisation autorise à divulguer ou à ce que la loi exige de communiquer? Qui supervise cet aspect (qui en est responsable)? Comment communiquez-vous les renseignements aux clients?	
13. Quelle procédure suivez-vous pour retourner ou détruire les renseignements transmis lorsqu'un contrat est terminé? Qu'en est-il à la fin d'une initiative particulière (comme un programme de marketing comportemental en ligne qui est terminé)?	
Section 4 : Tiers	
14. Votre organisation transmet-elle ou vend-elle à des tiers les renseignements personnels des clients qu'elle recueille? Veuillez fournir quelques exemples généraux (p. ex., à des spécialistes du marketing, à des fournisseurs d'applications).	
15. Si des renseignements personnels de clients sont transmis ou vendus à des tiers, comment votre organisation en assure-t-elle la protection? Par exemple, les clients doivent-ils donner leur consentement? Sont-ils avisés?	
16. Quelles sortes de fonctions spéciales votre entreprise utilise-t-elle (p. ex., personnalisation du profil, publicité et fonctions géodépendantes),	

Question	Réponse
et à quels types de tiers faites-vous appel pour ces fonctions? Ces tiers ont-ils accès aux renseignements personnels des clients?	
17. Que faites-vous pour vous assurer que les tiers qui ont accès aux renseignements personnels des clients utilisent des mécanismes de protection des renseignements personnels équivalents aux vôtres? Imposez-vous des restrictions à l'accès qui est accordé aux tiers afin de protéger les renseignements personnels de clients?	
18. Votre organisation vérifie-t-elle dans quelle mesure les tiers respectent les dispositions du contrat? Dans l'affirmative, veuillez expliquer la procédure de vérification et la fréquence de celle-ci.	
19. De quelle façon informez-vous les clients des nouvelles utilisations de leurs données, dont certaines par des tiers? Leur demandez-vous d'abord s'ils y consentent ou les refusent? Si la procédure change selon l'initiative, sur quels critères pertinents fondez-vous votre décision?	
Section 5 – Enjeux émergents	
20. **Suivi :** Utilisez-vous des fonctions géodépendantes ou des fonctions de suivi? Dans l'affirmative, quelles sortes de fonctions employez-vous et comment obtenez-vous le consentement des clients à l'égard de l'utilisation de ces fonctions?	
21. **Nuage :** Utilisez-vous un service de stockage en nuage pour vos données? Ces données	

Question	Réponse
comprennent-elles des renseignements personnels? Quels types de renseignements personnels? Quel fournisseur de services? Avez-vous exprimé des préférences quant au stockage de vos données, comme un stockage par emplacement? Dans l'affirmative, comment le fournisseur de services infonuagiques a-t-il répondu?	
22. **Compétence :** Quelles sortes de points d'échange Internet (points IXP) utilisez-vous (p. ex., locaux/canadiens)? Des données identifiables passent-elles parfois par un autre territoire de compétence? Sont-elles chiffrées? Comment répondez-vous aux demandes de renseignements provenant d'organismes d'application de la loi d'autres territoires de compétence? Comment expliquez-vous ce processus aux clients?	
23. **Internet des objets/Réalité augmentée :** Quelles sortes de technologies de type Internet des objets/réalité augmentée prenez-vous en charge dans le cadre de vos services de réseau sans fil? En quoi ces contrats diffèrent-ils des contrats de téléphonie mobile? Où dirigez-vous les clients qui ont des questions sur la protection des renseignements personnels? Les dirigez-vous vers l'équipe ou la politique de protection des renseignements personnels du fabricant ou à votre propre équipe et politique en la matière?	
24. **Métadonnées :** Comment procédez-vous pour collecter, utiliser, stocker et détruire les métadonnées? Comment classez-vous les métadonnées? Sont-elles protégées comme des renseignements personnels ou de l'information de nature délicate? Transmettez-vous ou vendez-	

Question	Réponse
vous des métadonnées à des tiers? Comment faites-vous pour réduire les risques de ré-identification?	
Section 6 : Atteintes à la vie privée	
25. Comment votre organisation avertit-elle les clients lorsqu'il y a atteinte à la vie privée? À quel moment le fait-elle?	
26. Votre organisation avertit-elle les clients lorsqu'il y a atteinte à la vie privée par un tiers?	
27. En cas d'atteinte à la vie privée, quelles mesures votre entreprise prend-elle pour en atténuer l'incidence?	
Section 7 : Conclusion	
28. À votre avis, quels sont les plus grands défis en matière de protection des renseignements personnels des clients des services sans fil dans le contexte du marché actuel?	

Annexe C – Bibliographie

1. Adams, C., Université d'Ottawa, Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles, juin 2013. https://www.priv.gc.ca/media/1774/mp_201306_f.pdf

2. Bohaker, H. et coll., Université de Toronto, *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World*, 2015. http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf

3. British Columbia Freedom of Information and Privacy Association, Le véhicule connecté : Qui est aux commandes? https://fipa.bc.ca/connected-car/

4. Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World*, janvier 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

5. Commissariat à la protection de la vie privée du Canada, *Instance dans le but d'établir un code obligatoire pour les fournisseurs de services sans fil mobiles : Soumission du Commissariat à la protection de la vie privée du Canada à l'intention du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)*, 4 décembre 2012. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_crtc_121204/

6. Commissariat à la protection de la vie privée du Canada, *Métadonnées et vie privée : Un aperçu technique et juridique*, octobre 2014. https://www.priv.gc.ca/media/1793/md_201410_f.pdf

7. Commissariat à la protection de la vie privée du Canada, *Trousse d'outils en matière de vie privée : Guide à l'intention des entreprises et des organisations,* décembre 2015. https://www.priv.gc.ca/media/2039/guide_org_f.pdf

8. Commissariat à la protection de la vie privée du Canada, *L'Internet des objets : Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison*, février 2016. https://www.priv.gc.ca/media/1809/iot_201602_f.pdf

9. Tech Policy Lab, University of Washington, *Augmented Reality: A Technology and Policy Primer*, septembre 2015.
10. http://techpolicylab.org/wp-content/uploads/2015/10/Augmented_Reality_Primer.pdf

11. White, G., Le Centre pour la défense de l'intérêt public, *Déconnecté du réseau? Repérage des technologies basées sur la localisation et la Loi*, juin 2015.
12. http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report_FR.pdf

www.deloitte.ca

Deloitte, l'un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de la certification, de la fiscalité, de la consultation et des conseils financiers. Deloitte S.E.N.C.R.L., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, veuillez consulter le lien https://www2.deloitte.com/ca/fr/pages/about-deloitte/articles/about-deloitte.html.