



Enquête sur les paiements mobiles au point de vente : qu'en est-il de la vie privée des consommateurs?

RAPPORT DE RECHERCHE

Rapport réalisé par Option consommateurs
et présenté au Bureau de la consommation d'Industrie Canada (désormais appelé
Innovation, Sciences et Développement économique Canada)
Juin 2016

Option consommateurs a reçu un financement en vertu du programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Industrie Canada (désormais appelé Innovation, Sciences et Développement économique Canada). Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Innovation Sciences et Développement économique ou du gouvernement du Canada. La reproduction de ce rapport, tout ou parties, est autorisée, à condition que la source soit mentionnée. Sa reproduction ou toute allusion à son contenu à des fins publicitaires ou lucratives sont toutefois strictement interdites.

Rédigé par : Annik Bélanger-Krams

Dépôt légal Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN 978-2-89716-028-9

Option consommateurs
50, rue Ste-Catherine Ouest, Bureau 440
Montréal (Québec)
H2X 3V4
Téléphone : 514 598-7288
Télécopieur : 514 598-8511

Adresse électronique : info@option-consommateurs.org
Site Internet : www.option-consommateurs.org

Table des matières

Option consommateurs	Erreur ! Signet non défini.
Remerciements	7
Résumé.....	8
Introduction	9
Méthodologie.....	10
Section 1. Le paysage des paiements mobiles dans le contexte canadien	12
1.1. Définition de paiements mobiles.....	12
1.2. Type de paiements mobiles	12
1.3. Les acteurs dans l'écosystème de paiements mobiles	14
1.4. Coup d'œil sur les applications de paiements mobiles offertes aux Canadiens	16
1.4.1. Les APMPV offertes par les commerçants.....	17
1.4.2. Les applications APMPV offertes par les institutions financières	18
1.4.3. Les portefeuilles électroniques non émis par des institutions financières	19
1.4.4. Les applications de paiements offertes par les commerçants de vente de détails.....	19
1.5. Survol de l'encadrement législatif des paiements mobiles au Canada	20
Section 2. Les APMPV : bref survol de la problématique de vie privée.....	23
2.1. Point soulevé par les experts	23
2.2. Les enjeux de vie privée spécifique aux téléphones intelligents.....	25
2.3. ... et aux paiements électroniques.....	26
2.4. Le défi des APMPV	28
Section 3. Cadre juridique.....	29
3.1. Le droit à la vie privée	29
3.2. Le contexte économique et protections des données	29
3.3. Champ d'application général	29
3.3.1. Les principes relatifs à l'équité dans le traitement de renseignements	31
3.3.1.1. Premier principe : la responsabilité.....	32
3.3.1.2. Deuxième principe : la détermination des fins de la collecte des renseignements	32
3.3.1.3. Troisième principe : le consentement	33

3.3.1.4. Quatrième principe : la limitation de la collecte	34
3.3.1.5. Cinquième principe : la limitation de l'utilisation, de la communication et de la conservation.....	35
3.3.1.6. Sixième principe : l'exactitude.....	35
3.3.1.7. Septième principe : les mesures de sécurité	35
3.3.1.8. Huitième principe : la transparence	36
3.3.1.9. Neuvième principe : l'accès aux renseignements personnels.....	36
3.3.1.10. Dixième principe : la possibilité de porter plainte.....	36
3.3.2. La limitation de la finalité	36
3.4. Les renseignements personnels.....	37
3.5. La confiance	39
3.6. La publicité comportementale en ligne	40
3.7. La protection intégrée de la vie privée (Privacy by design).....	42
3.8. Les renseignements des consommateurs stockés aux États-Unis	44
3.9. Portrait du droit étranger	44
3.9.1. Les États-Unis.....	45
3.9.2. L'Union européenne	47
Section 4. Analyse des politiques de confidentialité des applications de paiements mobiles.....	50
4.1. Notre échantillonnage	51
Tableau 1 – Applications offertes aux utilisateurs d'Android (28 applications ont été analysées).....	52
Tableau 2 – Applications offertes aux utilisateurs d'iPhone (19 applications ont été analysées).....	52
4.2. Notre analyse	53
4.2.1. Première lacune : les politiques de confidentialité ne sont pas toujours facilement accessibles	53
4.2.2.. Deuxième lacune : les politiques de confidentialité ne sont pas toujours adaptées à la réalité des mobiles.	55
4.2.3. Troisième lacune : les politiques de confidentialité manquent parfois de clarté	57
4.2.4. Quatrième lacune : les politiques de confidentialité définissent souvent un renseignement personnel uniquement comme un renseignement nominatif	58
4.2.5. Cinquième lacune : les politiques de confidentialité recueillent souvent trop d'informations.....	59

4.2.6. Sixième lacune : il y a parfois des problèmes sur le plan du consentement et de son retrait.....	62
Section 5. Groupe de discussion avec les consommateurs	64
5.1. Utilisation des applications de paiements mobiles au point de vente par les consommateurs	65
5.2 . Quelques inquiétudes.....	65
5.3. Des connaissances de base	66
5.4. Lecture des termes et conditions de l’entente ou de la clause de confidentialité	66
5.5. Les informations que les consommateurs sont prêts à divulguer.....	67
5.6. Réaction des consommateurs à la suite de la lecture des politiques de confidentialité	68
5.7. Comment ces clauses peuvent être améliorées	68
Conclusion et recommandations	70

Option consommateurs

MISSION

Option consommateurs est une association à but non lucratif qui a pour mission de promouvoir et de défendre les droits et les intérêts des consommateurs et de veiller à ce qu'ils soient respectés.

HISTORIQUE

Issue du mouvement des associations coopératives d'économie familiale (ACEF), et plus particulièrement de l'ACEF de Montréal, Option consommateurs existe depuis 1983. En 1999, elle a regroupé ses activités avec l'Association des consommateurs du Québec (ACQ) qui existait depuis plus de 50 ans et accomplissait la même mission qu'elle.

PRINCIPALES ACTIVITÉS

Option consommateurs aide les consommateurs qui vivent des difficultés, les reçoit en consultation budgétaire et donne des séances d'information sur le budget, l'endettement, le droit de la consommation et la protection de la vie privée.

Chaque année, nous réalisons des recherches sur des enjeux de consommation d'importance. Nous intervenons également auprès des décideurs et des médias pour dénoncer des situations inacceptables. Lorsque nécessaire, nous entreprenons des recours collectifs (désormais appelés actions collectives) contre des commerçants.

MEMBERSHIP

Pour faire changer les choses, les actions d'Option consommateurs sont multiples : recherches, actions collectives et pressions auprès des instances gouvernementales et des entreprises. Vous pouvez nous aider à en faire plus pour vous en devenant membre d'Option consommateurs au www.option-consommateurs.org

Remerciements

Cette recherche a été réalisée et rédigée par Me Annik Bélanger-Krams. Cette dernière a été supervisée par Mme Maryse Guénette, responsable du service de recherche et de représentation d'Option consommateurs, qui a aussi participé à la rédaction.

L'auteure remercie M. Bruno Marien pour son soutien méthodologique durant la réalisation de ce rapport. M. Marien est sociologue ainsi que chargé de cours au département de science politique et de droit de l'Université du Québec à Montréal (UQAM). Il enseigne la méthodologie de la recherche et les statistiques au sein de ce département depuis plus de quinze ans. Elle remercie également M. Jean-Pierre Beaud, professeur à la faculté de science politique et de droit à l'UQAM, qui a effectué l'évaluation du rapport.

L'auteure tient également à remercier tous les employés d'Option consommateurs qui, de près et de loin, ont collaboré à cette recherche. Elle remercie plus particulièrement Carole-Anne Émond et Emmanuelle Dione, étudiantes en droit de l'Université de Montréal ainsi que Pierre-Olivier Valiquette, étudiant en droit de l'Université McGill.

Elle remercie enfin tous les représentants d'organismes et les experts mentionnés ci-dessous qui lui ont accordé une entrevue, soit :

- Commissariat à la protection de la vie privée du Canada
- Professeur Harold Boeck, ESG, UQAM
- Dr Colin Bennett, University of Victoria
- Dr Anne Cavoukian, Directrice Générale, Privacy & Big Data Institute, Ryerson University
- Dr Cynthia Chassigneux, Commissaire à la Commission d'accès à l'information du Québec
- Professeur Marc Lacoursière, Université Laval
- Professeur Jacques Nantel, HEC Montréal
- M. Anthony Palermo, co-fondateur et président directeur général, Connect&Go
- M. Frédéric René, vice-président des opérations de Les boutiques LikiSoft Inc.
- M. Ira Rheingold, directeur général et avocat principal de la National Association of Consumer Advocates
- Professeur Teresa Scassa, Chaire en droit de l'informatique, Université d'Ottawa
- M. Jacques St-Amant, chargé de cours, UQAM
- Professeur Nicolas Vermeys, directeur Adjoint, Laboratoire de cyberjustice
- Mme Nataly Lévesque, étudiante au doctorat en administration, UQAM

Résumé

Les téléphones intelligents sont plus populaires que jamais. Les consommateurs peuvent y télécharger un grand nombre d'applications susceptibles de leur faciliter la vie. Par exemple, grâce aux applications de paiements mobiles au point de vente (APMPV), ils peuvent payer leurs achats sans ouvrir leur portefeuille, voire regrouper dans un portefeuille électronique toutes leurs cartes de paiements, leurs cartes cadeaux et leurs cartes fidélités.

Pour fonctionner, les APMPV requièrent un grand nombre d'informations personnelles. Ce qui comporte des enjeux importants en matière de vie privée. D'une part, ces applications posent des défis quant à la divulgation et à la communication d'informations importantes relativement à la collecte, la protection et la diffusion des renseignements personnels, tel qu'énoncé dans la politique de confidentialité. D'autre part, ils posent des défis en raison de leur utilisation sur un support mobile, ce qui permet de recueillir un vaste éventail de renseignements personnels.

Afin de déterminer comment les entreprises offrant des APMPV informent les consommateurs de ces enjeux, nous avons étudiés leurs politiques de confidentialité, puis nous avons utilisé toutes les APMPV pouvant être utilisées à Montréal durant une période donnée. Notre analyse révèle que plusieurs des politiques de confidentialité comportent des lacunes. Tantôt, elles sont difficiles d'accès ou manquent de clarté, tantôt, elles sont mal adaptées au contexte de la communication d'information sur support mobile.

Alors que plusieurs des politiques de confidentialité donnent une définition de renseignements personnels qui diffère de celle du CPVP, d'autres posent problème quant à la manière d'obtenir le consentement des consommateurs. Bien que, dans le contexte actuel, il soit normal que les applications recueillent les renseignements personnels nécessaires aux paiements mobiles. Certaines APMPV en recueillent un trop grand nombre.

Afin d'obtenir le pouls des consommateurs, nous avons tenu six groupes de discussions, trois à Montréal et trois à Toronto, avec des utilisateurs d'APMPV. La majorité des participants ont été surpris du grand nombre de renseignements collectés par ces applications et partagés avec des tiers, au point où certains se sont dits prêts à reconsidérer leur habitude d'utilisation. Ils trouvaient pertinent de rendre les politiques de confidentialité mieux adaptées au support mobile, qui est particulièrement convivial et dynamique.

De plus, la compréhension du système des paiements mobiles n'est pas à la portée de tous. Il peut être difficile pour les consommateurs de comprendre comment leurs renseignements personnels seront traités durant le processus de paiement. Par conséquent, il est essentiel que les politiques de confidentialités soient transparentes et faciles à comprendre. Or, certaines d'entre-elles ne le sont pas. Il faut que les entreprises améliorent leurs pratiques, notamment en se préoccupant de la vie privée dès la conception d'un appareil (conception de la vie privée intégrée). Ce n'est qu'ainsi qu'elles pourront bien protéger les consommateurs et s'assurer de leur confiance, une condition *sine qua non* au système des paiements mobiles.

Introduction

Les téléphones intelligents sont de plus en plus populaires. Selon une étude récente, en un an, la proportion de Canadiens ayant un téléphone intelligent a augmenté de 13 %, passant de 55 % en 2014 à 68 % en 2015¹. En 2014, une étude révélait qu'au Québec, 52,5 % des adultes avaient un téléphone intelligent. Certains groupes utilisent les téléphones intelligents plus que d'autres, c'est le cas des adultes âgés de 25 à 34 ans (79.8 %) et les « foyers » ayant un enfant à la maison (78.2 %)². Parmi ceux qui ont un téléphone intelligent, 44 % ont un Android et 39 % ont un iPhone³.

Les consommateurs aiment les applications mobiles. Selon un sondage américain, lorsqu'ils les utilisent, ils le font durant 85 % du temps qu'ils passent sur leur téléphone intelligent⁴. Les consommateurs ont l'embarras du choix. Selon des chiffres de juillet 2015, les utilisateurs d'Android ont accès à 1,6 million d'applications alors que les utilisateurs d'iPhone ont accès à 1,4 million d'applications⁵.

Au cours des dernières années, les applications de paiements mobiles ont aussi fait leur apparition. Aujourd'hui, elles sont très populaires dans certains pays, notamment en Asie. En matière d'adoption des paiements mobiles, le Canada « est à la traîne » derrière certains pays, notamment les pays Scandinaves, le Japon, l'Australie et les États-Unis⁶. Les acteurs du secteur financier aimeraient que cette situation soit améliorée, d'autant plus que le Canada serait bien placé pour que les applications de paiements mobiles y soient adoptées avec succès. Selon le *Readiness Index*, qui évalue l'état de préparation à l'adoption des paiements mobiles, le Canada serait au deuxième rang parmi 34 pays. Ses points forts, on trouve le taux élevé de pénétration d'Internet, la qualité et le taux de pénétration des services financiers ainsi que le niveau de coopération entre les banques, les réseaux mobiles et le gouvernement dans la mise en place de l'écosystème de paiement⁷. De plus, les Canadiens sont ceux qui, dans le monde, passent le plus de temps en ligne; en moyenne 45 heures par mois. Les sites web plus fréquemment utilisés sont ceux liés aux finances personnelles, par exemple les sites web des banques. En 2013, 6,7 millions de consommateurs payaient leurs factures en ligne. Sans surprise, ce sont les jeunes, qui sont susceptibles d'adopter en premier les paiements mobiles. La rapidité, l'efficacité et la commodité sont importantes pour eux⁸.

¹ <http://catalyst.ca/2015-canadian-smartphone-market/>

² http://www.cefrio.qc.ca/media/uploader/Fascicule-Mobilit_Versionfinale.pdf

³ http://www.cefrio.qc.ca/media/uploader/Fascicule-Mobilit_Versionfinale.pdf

⁴ <http://techcrunch.com/2015/06/22/consumers-spend-85-of-time-on-smartphones-in-apps-but-only-5-apps-see-heavy-use/>

⁵ <http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

⁶ ADAMS Carlisle, « *Les paiements mobiles en tout temps en tout lieu : bref survol du paysage des paiements mobiles* », rapport présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 9

⁷ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 19

⁸ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 19

Les applications de paiements mobiles soulèvent des questions importantes en matière de vie privée. Elles permettent de recueillir plus d'information sur les consommateurs que ne le font les ordinateurs ou les autres types d'applications mobiles. Parmi les informations recueillies, mentionnons des informations sur les finances, les habitudes d'achat et l'emplacement en temps réel du consommateur (géolocalisation).

Méthodologie

Notre recherche a été réalisée de juillet 2015 à mars 2016. Elle fait état de la situation qui prévalait durant cette période. Selon l'Organisation de Coopération et de Développement Économiques (OCDE), les paiements mobiles sont des paiements pour lesquels les données et l'ordre de paiement sont transmis *via* un téléphone mobile ou un autre équipement mobile. Les paiements mobiles peuvent être faits à distance ou en personne (au point de vente). Dans le cadre de cette recherche, nous restreignons notre échantillon à des applications de paiement mobiles offertes sur des téléphones intelligents. Nous avons sélectionné des applications de paiements mobiles qui permettent de faire des transactions au point de vente⁹ (à la caisse), et d'autres qui permettent de faire des transactions en magasin sans passer à la caisse.

Dans le cadre de cette recherche, nous cherchons à répondre aux questions suivantes : quels sont les renseignements recueillis par les applications de paiement mobiles utilisées par les consommateurs? Comment les consommateurs sont-ils informés de la collecte, de l'utilisation et de la communication de leurs renseignements personnels? Qu'en savent-ils et qu'en pensent-ils?

Pour y parvenir, nous avons effectué les étapes suivantes :

1. Recherche documentaire sur les applications de paiements mobiles au point de vente et sur la vie privée.
2. Entrevues avec des experts en droit, notamment en droit de la consommation, de la vie privée et du commerce électronique¹⁰ ainsi qu'avec deux entrepreneurs en informatique¹¹.
3. Nous avons également effectué une analyse du cadre juridique au Canada, aux États-Unis et en Union européenne.
4. Nous avons identifié les applications de paiements mobiles au point de vente (APMPV)¹² offertes aux consommateurs canadiens¹³.

⁹ Dans la doctrine, il y a une certaine ambiguïté. En effet, les auteurs définissent différemment ce type de paiement. Pour certains, les paiements au point de vente se font nécessairement à la caisse; pour d'autres, ils peuvent aussi se faire en magasin sans que le client ne passe à la caisse.

¹⁰ La liste des experts se trouve à la section des remerciements

¹¹ L'un d'eux crée des sites web pour des entreprises alors que l'autre est spécialisé en RFID.

¹² Pour les besoins de ce rapport, nous avons choisi de désigner le terme « application de paiements mobiles au point de vente » par l'acronyme APMPV.

¹³ Cette opération a été effectuée de Montréal.

5. Puis, nous en avons sélectionné un échantillon représentatif d'APMPV. Celui-ci a été créé en fonction des applications offertes aux consommateurs canadiens au moment de la rédaction de ce rapport¹⁴. Nous avons sélectionné des APMPV offertes par les commerçants (par exemple Starbucks), des APMPV offertes par des institutions financières¹⁵ et des applications de portefeuilles électroniques (par exemple Ugo). Nous avons aussi sélectionné des applications de paiements mobiles (APM) offertes par des commerçants, qui permettent aux consommateurs de « scanner » et de commander des articles en magasins, de les payer puis de se les faire livrer à la maison, tout cela sans passer directement à la caisse (par exemple application ToysRus ou Zara).

Dans le cadre de notre recherche, nous avons téléchargé les APMPV faisant partie de notre échantillonnage. Nous avons créés des comptes, puis nous avons utilisé ces applications. Notre but était de savoir à quel moment les politiques de confidentialité étaient affichées et si ces applications pouvaient être utilisées en magasins.

Nous avons analysé les politiques de confidentialité de ces applications afin de déterminer comment les consommateurs sont informés de la collecte, de l'utilisation et de la communication de leurs renseignements personnels.

Nous avons tenu des groupes de discussions, trois à Montréal et trois à Toronto, avec des consommateurs utilisant des applications de paiements mobiles au point de vente, afin de déterminer leurs connaissances et leurs perceptions sur la collecte de leurs renseignements personnels dans le cadre de l'utilisation de ces applications.

¹⁴ Nous avons utilisé toutes les APMPV que nous avons été en mesure d'utiliser de Montréal avec les téléphones que nous avons (ceux que nous avons acheté et ceux de nos testeurs) et avec nos fournisseurs de réseau cellulaire. Nous avons fait nos tests de la première semaine de janvier à la première semaine de mars.

¹⁵ Nous avons sélectionné des applications d'institutions financières bancaires (TD, Scotia, RBC et CIBC) et une institution financière non bancaire (Desjardins)

Section 1. Le paysage des paiements mobiles dans le contexte canadien

L'écosystème des paiements mobiles au Canada est complexe. On y trouve de nombreux acteurs, plusieurs types de modes de paiements et différents modèles d'applications. Ces différentes composantes sont imbriquées les unes aux autres. Pour s'y retrouver, il est important de bien les d'identifier et de saisir tant le rôle que l'importance de chacune d'elles. Chacune à leur façon, elles jouent un rôle sur la protection des renseignements personnels des consommateurs (un renseignement personnel est défini comme un renseignement qui concerne un individu identifiable¹⁶).

1.1. Définition de paiements mobiles

L'Organisation de Coopération et de Développement Économique (OCDE) définit les paiements mobiles comme des paiements pour lesquels les données et l'ordre de paiement sont transmis *via* un téléphone mobile ou un autre équipement mobile. Les paiements mobiles peuvent être faits à distance ou en personne (au point de vente)¹⁷. Entrent dans cette catégorie les paiements fait sur Internet au moyen d'un téléphone intelligent, de même que ceux fait par des « opérateurs de réseaux mobiles »¹⁸. L'OCDE considère les paiements mobiles comme étant une « sous-branche » du commerce électronique.¹⁹

1.2. Type de paiements mobiles

Il existe quatre types de paiements mobiles²⁰. D'abord, il y a le paiement mobile de personne à personne (*peer-to-peer*). Par exemple, je transfère 10 \$ à un ami pour lui remettre ce que je lui dois²¹. Ce type de paiement mobile ne sera pas étudié dans le cadre de cette recherche²².

Il y a aussi le paiement mobile appelé Acceptation mobile. « Il s'agit d'un paiement mobile hybride qui se situe entre le paiement de personne à personne et le PMPV. Deux personnes, un consommateur et un commerçant participent à cette opération ». Le consommateur paie avec sa carte de crédit ou de débit à un commerçant qui utilise un téléphone intelligent et un logiciel

¹⁶ Art 2 Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

¹⁷ [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP\(2010\)22/FINAL&docLanguage=Fr](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2010)22/FINAL&docLanguage=Fr)

¹⁸ Ce terme désigne les Telus et Bell de ce monde.

¹⁹ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 12

²⁰ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10 et DOLCOURT. J., « *Making Sense of Mobile Payments* », CENT, 2010

²¹ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10 et DOLCOURT. J., « *Making Sense of Mobile Payments* », CENT, 2010

pour traiter le paiement²³. Un exemple serait l'application Square. Ce type de paiement mobile ne sera pas non plus abordé dans cette recherche.

En troisième vient le paiement par commerce mobile (ou commerce en ligne). Ce mode de paiement permet d'utiliser le navigateur pour faire un paiement. Ce dernier peut être fait à partir d'un mobile ou d'un ordinateur²⁴. Nous ne l'étudierons pas non plus ici.

Le quatrième type de paiements mobiles est le paiement mobile au point de vente (PMPV). C'est lui que nous étudions dans cette recherche. Entrent notamment dans cette catégorie les paiements faits entre un consommateur et un commerçant, souvent à la caisse. Le consommateur utilise son téléphone intelligent pour payer un bien ou un service²⁵. Afin de faire un PMPV²⁶, il est possible d'utiliser la Communication en champ proche (NFC) ou une autre technologie, par exemple les codes à barres.

Le portefeuille électronique permet lui aussi de faire des PMPV. Il vient souvent sous la forme d'une application; c'est le cas du portefeuille Ugo, mais pas d'ApplePay. Agissant comme un organisateur numérique, il contient habituellement les informations du payeur, ses cartes de paiement, ses cartes prépayées, ses cartes de fidélité ainsi que ses coupons. Le portefeuille électronique contient également le matériel informatique (hardware) et le logiciel (software) permettant l'enregistrement et la communication menant à la transaction de PMPV. Les portefeuilles électroniques sont accessibles *via* un téléphone intelligent²⁷. Habituellement, le créateur du portefeuille gère la technologie et le consommateur à la liberté d'utiliser cet outil à sa convenance.²⁸

Dans le cas des APMPV, l'accès aux fonds peut se faire par le paiement de substitutions ou par le paiement de proximité. « Les paiements de substitution pour des biens et des services sont effectués au moyen d'applications propres aux commerçants qui désignent l'appareil mobile du payeur comme un compte de carte de crédit de substitution »; les applications de café et de stationnement en sont des exemples²⁹. Pour leur part, les paiements de proximité « sont

²³ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10 et DOLCOURT. J., « *Making Sense of Mobile Payments* », CENT, 2010

²⁴ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10 et DOLCOURT. J., « *Making Sense of Mobile Payments* », CENT, 2010

²⁵ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10 et DOLCOURT. J., « *Making Sense of Mobile Payments* », CENT, 2010

²⁶ Pour les besoins de ce rapport, nous avons choisi de désigner le terme « paiements mobiles au point de vente » par l'acronyme PMPV.

²⁷ <http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-overview-on-mobile-payments-initiatives-edition-december-2014/epc091-14-v20-epc-overview-on-mobile-payments-initiatives/> page 16

²⁸ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10

²⁹ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 13

effectués au moyen d'une application mobile qui accède au compte du consommateur dans les institutions financières et sur les cartes de crédits»³⁰.

1.3. Les acteurs dans l'écosystème de paiements mobiles

Carlisle Adams identifie 10 différents acteurs faisant partie de l'écosystème des paiements mobiles. Un grand nombre d'entre eux joue un rôle important et peut avoir un impact significatif sur la vie privée des consommateurs qui utilisent les APMPV. Il est donc pertinent de tous les étudier dans cette recherche.

- Les acteurs permettant les paiements et participant aux opérations de paiements

Les institutions financières entrent dans cette catégorie. Dans le monde des paiements mobiles, leur rôle est similaire à celui qu'elles jouent lors d'une transaction de débit. Les paiements mobiles peuvent augmenter le nombre de leurs transactions et fidéliser leur clientèle.

Les « marques de paiement »³¹ qui jouent le rôle du fournisseur ou du propriétaire de l'application, entrent aussi dans cette catégorie. Cela est vrai tant pour les cartes sans contact que pour les APMPV³². « Il est possible d'accroître la variété et le nombre de marques de paiements à la disposition de l'utilisateur (...), notamment, les émetteurs de coupons, de cartes de fidélités et de cartes de réductions pour les membres. »

- Les fournisseurs de cartes non bancaires

Ils offrent des cartes cadeaux, des cartes de transports et d'autres produits prépayés. Ils offrent aussi des comptes en ligne à valeur stockée (c'est ce qu'offre l'entreprise PayPal)³³.

- Les fournisseurs de portefeuilles électroniques

Via une interface, les portefeuilles électroniques permettent aux consommateurs d'avoir accès à différentes sources pour effectuer leurs paiements; ceci inclut les cartes de crédit, les cartes prépayées, les cartes de fidélité et les coupons sur support numérique. Ils peuvent avoir la forme d'une application ou d'un service pour gérer les cartes et permettre le PMPV³⁴. Certains

³⁰ TRITES steve et als., Agence de la consommation en matière financière du Canada, « Les paiements mobiles et la protection des consommateurs au Canada », décembre 2013, page 13 et Dahlberg, Mallat, Ondrus et Zmijewska, 2006; Kim, Mirusmonov et Lee, 2010; Groupe de travail sur l'examen du système de paiements, 2011

³¹ Les marques de paiements peuvent inclure par exemple Visa, Mastercard et Amex. ADAMS Carlisle, « *Les paiements mobiles en tout temps en tout lieu : bref survol du paysage des paiements mobiles* », Commissariat à la protection de la vie privée du Canada, juin 2013, page 13

³² ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 13

et CHAIX Laetitia, « Le paiement mobile : perspectives économiques, modèles d'affaires et enjeux concurrentiels », *Thèse en vue de l'obtention du Doctorat en Sciences Économiques*, Université Nice Sophia Antipolis, 2013, page 40-45

³³ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 27

³⁴ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles page », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013,

utilisent la technologie infonuagique, d'autres la technologie NFC, d'autres encore les codes à barres. Avec les technologies infonuagiques, les données et les logiciels sont extraites de serveurs à distance qui utilisent des applications et des applications web. Les identifiants pour fin de paiements³⁵ ne se trouvent pas sur le téléphone intelligent, ce qui fait que les portefeuilles ne dépendent pas d'une technologie particulière³⁶.

- Les utilisateurs

Ce sont les consommateurs qui se servent des paiements mobiles. Ils choisissent le type d'application et la carte de paiements qu'ils veulent utiliser³⁷.

- Les différents acteurs qui jouent un rôle dans la prestation du service de paiements

Les fabricants d'appareils entrent dans cette catégorie. Ils ont l'avantage compétitif d'offrir aux consommateurs qui ont un appareil assez récent la possibilité d'effectuer des PMPV.³⁸ Les fabricants de terminaux au point de vente (PDV) y sont également. Leurs terminaux offrent la possibilité d'effectuer des transactions par PMPV³⁹.

- Les gestionnaires de services de confiance (GSC).

Ils jouent un rôle fondamental dans le processus de PMPV, et ce, même s'ils ne participent pas directement au paiement. Le *Canadian NFC Payments Reference Model*⁴⁰ oblige les institutions financières, les marques de paiements et les détaillants qui veulent offrir une application sur un appareil NFC de le faire par le biais d'un GSC. Lors d'une transaction, le GSC recueille les données de l'appareil et les renseignements personnels de l'utilisateur (son nom, son numéro de carte de crédit et la date d'expiration de cette carte). Le GSC assure les services de téléchargement et de gestion du cycle de vie des données des applications de paiement NFC et

page 14 et CHAIX Laetitia, « Le paiement mobile : perspectives économiques, modèles d'affaires et enjeux concurrentiels », *Thèse en vue de l'obtention du Doctorat en Sciences Économiques*, Université Nice Sophia Antipolis, 2013, page 40-45

³⁶ TRITES Steve et al., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 28 et CROWE M. et TAVILLA E., « Federal Reserve Bank of Boston, Mobile Phone Technology: "Smarter" Thank We Thought: How Technology Platforms are Security Mobile Payments in the U.S. », 16 novembre 2012

³⁷ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles page », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 14 et CHAIX Laetitia, « Le paiement mobile : perspectives économiques, modèles d'affaires et enjeux concurrentiels », *Thèse en vue de l'obtention du Doctorat en Sciences Économiques*, Université Nice Sophia Antipolis, 2013, page 40-45

³⁸ Ibid.

³⁹ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles page », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 15 et CHAIX Laetitia, « Le paiement mobile : perspectives économiques, modèles d'affaires et enjeux concurrentiels », *Thèse en vue de l'obtention du Doctorat en Sciences Économiques*, Université Nice Sophia Antipolis, 2013, page 40-45

⁴⁰ Il s'agit d'un ensemble de lignes directrices visant à assurer un réseau sécurisé et conviviale aux consommateurs et aux commerçants. À noter : le *Canadian NFC Mobile Payments Reference Model* provient d'une initiative du secteur financier canadien avec la participation des banques et des coopératives de crédit. Toutefois, ce ne sont pas toutes les institutions financières qui y sont participantes. La conformité au modèle est facultative et n'est pas assujéti à un organisme de surveillance.

des renseignements personnels des consommateurs. De façon générale, les marques de paiement imposent des obligations de sécurité. Le GSC doit gérer adéquatement les clés de chiffrement⁴¹ pour sécuriser la communication entre l'institution financière et le téléphone du consommateur. Les marques de paiement peuvent choisir un GSC ou en devenir un.

- Les exploitants de réseau mobile (Bell, Rogers et Telus)

Ils jouent un rôle important en fournissant des appareils aux consommateurs et en les activant. Ils exploitent le réseau sans fil par lequel les données des applications de paiement et les renseignements des consommateurs sont transmis à l'institution financière, aux marques de paiement ou à l'élément de sécurité de l'appareil⁴². Les exploitants de réseau mobiles ont tendance à s'associer aux institutions financières⁴³.

- Les participants aux opérations de paiement

Ce sont les commerçants. Les APMPV les aident à fidéliser leur clientèle (pensons notamment aux programmes de loyauté). Elles leur permettent également d'avoir moins de marchandise en magasin (et donc moins d'employés), ce qui leur procure des bénéfices économiques. Enfin, elles facilitent la mise en place de leurs stratégies marketing (voir sections 2 et 3). Les APMPV procurent aussi des avantages aux consommateurs, qui peuvent les utiliser pour payer leurs achats à distance (même en magasin) et les faire livrer chez eux; ils n'ont pas à attendre à la caisse.

- Les publicitaires

Ils ne participent pas au processus de PMPV directement, mais ils jouent y un rôle important (voir sections 3 et 4).

1.4. Coup d'œil sur les applications de paiements mobiles offertes aux Canadiens

De plus en plus d'APMPV sont offertes aux consommateurs canadiens. Le premier type est celui offert par les commerçants, particulièrement par des grandes chaînes de café – au moment de réaliser notre recherche, ce sont surtout les grandes chaînes de café qui l'offraient. Le deuxième type est celui offert par les institutions financières (banques ou coopératives de crédit)⁴⁴. Nous

⁴¹ Le chiffrement est défini par l'OQLF comme étant une opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale. Synonyme de cryptage.

⁴² ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles page », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 16 et CHAIX Laetitia, « Le paiement mobile : perspectives économiques, modèles d'affaires et enjeux concurrentiels », *Thèse en vue de l'obtention du Doctorat en Sciences Économiques*, Université Nice Sophia Antipolis, 2013, page 40-45

⁴³ À noter, les trois exploitants de réseau mobile nommés ci-dessus sont copropriétaires du portefeuille électronique Suretap.

⁴⁴ Dans le cadre de cette étude, nous avons exclu les institutions financières qui offraient des PMPV sans l'utilisation d'application mobile, notamment la Banque de Montréal.

avons analysé les APMPV offertes par les plus grandes banques et la coopérative Desjardins. Nous avons exclu les institutions financières où il était difficile d'utiliser des APMPV, notamment Canadian Tire.

Les portefeuilles électroniques constituent le troisième type d'APMPV. Développés par des entreprises, ils permettent aux consommateurs d'enregistrer leurs cartes de paiements et de fidélités dans un portefeuille numérique.

Nous avons également ajouté des applications offertes par des commerçants. Ces applications permettent aux consommateurs de « scanner » un article en magasin, de l'acheter puis de le faire livrer à domicile. L'article provient généralement d'un entrepôt.

1.4.1. Les APMPV offertes par les commerçants

La plupart de ces APMPV fonctionnent *via* l'utilisation d'un compte client ou d'une carte pouvant être rechargée. Au moment de réaliser notre étude, elles étaient principalement offertes chez Starbucks, Second Cup et Tim Hortons. Souvent, elles permettent aux consommateurs d'accumuler des points qu'ils échangeront contre des boissons, des aliments ou des biens (par exemple, une tasse).

Le programme de récompense de Second Cup offre au consommateur dix points par dollar dépensé. Lorsque le consommateur a accumulé 500 points, il peut les échanger contre une boisson; lorsqu'il en a accumulé 1000, il peut obtenir un sac de café moulu⁴⁵.

Le programme de fidélité de Starbucks permet aux consommateurs d'accumuler une étoile pour chaque deux dollars dépensés, puis d'échanger ces étoiles pour des boissons. Le consommateur peut également obtenir une boisson gratuite le jour de son anniversaire⁴⁶. Les APMPV offertes par des entreprises misent sur la rapidité et l'aspect pratique. Grâce à *Mobile Order & Pay*, offert par Starbucks à Toronto au moment de la réalisation de notre recherche, le consommateur peut commander et payer son café avant même d'avoir mis les pieds dans l'établissement. Ce programme devrait être offert partout au Canada (sauf au Québec) à partir du 15 mars 2016⁴⁷.

Tim Hortons offre également la possibilité d'utiliser une APMPV. *Via* cette application, il offre au consommateur la possibilité de recharger sa carte, de trouver le magasin Tim Hortons le plus près ainsi que d'obtenir de l'information nutritionnelle et le service *Timmy Run*. Ce dernier facilite la commande et l'achat de cafés pour des groupes⁴⁸. Selon certains de nos participants aux groupes de discussion réalisés à Toronto, le restaurant Pizza Pizza offre une APMPV. Nous n'avons pas été capables de l'utiliser à Montréal⁴⁹.

⁴⁵ <https://www.secondcup.com/perks/HowItWorks.html?lang=fr>.

⁴⁶ <http://www.starbucks.ca/promo/rewards>

⁴⁷ <http://mobilesyrup.com/2016/03/08/starbucks-mobile-order-pay-now-available-across-all-canadian-provinces-except-quebec/>

⁴⁸ <http://www.timhortons.com/ca/en/about/timmyme.php> et <https://www.timhortons.com/ca/en/corporate/news-release.php?id=8205>

⁴⁹ Plusieurs participants des groupes de discussion de Toronto ont dit utiliser l'application Pizza Pizza pour faire des achats.

1.4.2. Les applications APMPV offertes par les institutions financières

Depuis peu, certaines institutions financières ont développé des applications permettant de faire des PMPV. Dans le cadre de cette étude, nous avons étudié les applications mobiles des banques suivantes : CIBC, RBC, Scotia et TD. Nous avons également étudié l'application Desjardins.

Ces applications permettent aux consommateurs de faire des achats dans des commerces avec leur téléphone. Généralement, elles sont liées à une carte de crédit émise par une institution financière⁵⁰. Les cartes de débit de l'institution financière participante peuvent aussi être liées au portefeuille⁵¹. Le portefeuille RBC permet également d'ajouter des cartes de fidélité et des cartes cadeaux au portefeuille⁵².

Les portefeuilles de TD, CIBC, Scotia et Desjardins ne sont offerts qu'aux utilisateurs d'Android⁵³; le portefeuille RBC est le seul pouvant être utilisé par ceux qui ont un iPhone. Par ailleurs, certains portefeuilles ne sont offerts qu'au client de certains exploitants de réseau mobile. Par exemple, les clients de Vidéotron et de Fido ne peuvent pas utiliser le portefeuille Desjardins⁵⁴. Qui plus est, l'accès à un portefeuille électronique peut aussi être impossible pour les détenteurs de certains appareils. Généralement, les institutions financières énoncent, sur leur site web, quels modèles de téléphone peuvent utiliser leur portefeuille électronique⁵⁵. Enfin, certains consommateurs doivent acheter une carte NFC pour utiliser un portefeuille électronique⁵⁶.

Les portefeuilles électroniques permettent aux consommateurs d'utiliser leurs téléphones intelligents pour faire des achats, et ce, dans des magasins différents. Le portefeuille de CIBC, qui a fait son apparition avant la fin de notre recherche, peut être utilisé dans de nombreuses succursales des magasins Loblaws, Petro-Canada, Tim Hortons et Real Canadian Superstore. Les portefeuilles émis par les autres institutions financières peuvent être utilisés dans de nombreux autres magasins. Par contre, lorsque nous avons tenté d'utiliser des portefeuilles électroniques dans des magasins, nous avons eu du mal à effectuer des paiements; ou bien les employés ne savaient pas quoi faire, ou bien l'équipement n'était pas adéquat. Nous avons remarqué qu'il est généralement plus facile d'utiliser les portefeuilles électroniques dans des restaurants de type Fastfood, des cafés et des pharmacies.

⁵⁰ <https://www.desjardins.com/particuliers/prets-marges-cartes-credit/cartes-credit/paiement-mobile/index.jsp> et <https://www.cibc.com/ca/features/mobile-payment.html>

⁵¹ <http://www.scotiabank.com/ca/en/0,,8100,00.html>

⁵² <http://www.rbcroyalbank.com/mobile/wallet/#payment-cards>

⁵³ <https://www.desjardins.com/particuliers/prets-marges-cartes-credit/cartes-credit/paiement-mobile/index.jsp> et <https://www.cibc.com/ca/features/mobile-payment.html> et <http://www.scotiabank.com/ca/en/0,,8100,00.html> et <https://www.tdcanadatrust.com/francais/produits-et-services/operations-bancaires/services-electroniques/services-de-paiement/paiement-mobile.jsp>

⁵⁴ <https://www.desjardins.com/particuliers/prets-marges-cartes-credit/cartes-credit/paiement-mobile/index.jsp>

⁵⁵ <https://www.cibc.com/ca/features/mobile-payment.html> et <http://www.scotiabank.com/ca/en/0,,8100,00.html>

⁵⁶ <https://www.desjardins.com/particuliers/prets-marges-cartes-credit/cartes-credit/paiement-mobile/index.jsp>

1.4.3. Les portefeuilles électroniques non émis par des institutions financières

Les consommateurs canadiens ont aussi accès à des portefeuilles créés par des entreprises qui ne sont pas des institutions financières. Ils peuvent y ajouter des cartes de paiements tels que des cartes de crédit, des cartes cadeaux, et des cartes de fidélités. Cela leur permet de regrouper au même endroit toutes ces cartes et de les utiliser lors d'un PMPV. Les consommateurs peuvent les télécharger et les utiliser sans frais.

Dans le cadre de cette étude, nous avons choisi et utilisé 11 portefeuilles électroniques offerts aux Canadiens. Nous avons sélectionné tous les portefeuilles électroniques que nous avons pu télécharger et utiliser à Montréal. Ces portefeuilles étaient acceptés par les commerçants et fonctionnaient bien. Il s'agit des portefeuilles ApplePay, Beep'nGo, Fidme, MobilePocket, Pass2Uwallet, Passwallet, PayPal, Smatwallet, Stocard, Suretap et Ugo. Certains d'entre eux utilisent la technologie infonuagique (notamment Ugo) alors que d'autres utilisent la technologie des codes à barres (notamment Fidme et Mobile Pocket).

En matière de portefeuilles électroniques, les utilisateurs d'Android ont beaucoup de choix alors que les utilisateurs d'iPhone n'ont accès qu'à Stocard, Ugo et Zoompass. Lorsque les portefeuilles étaient offerts sur les Android et les iPhone, nous étudions leur fonctionnalité et convivialité (facilité d'utilisation); nous regardions également comment les consommateurs étaient informés de la collecte de leurs renseignements personnels. Nous avons également analysé le portefeuille d'ApplePay. Même si ApplePay n'est pas une application en soi, puisqu'elle est disponible directement sur le téléphone, nous avons décidé de l'inclure en raison de son importance dans le marché des PMPV aux États-Unis et de son arrivée récente au Canada.

Nous avons utilisé tous les portefeuilles électroniques à l'aide de cartes prépayées que nous avons utilisées dans les commerces de café. Ces portefeuilles sont très bien acceptés comme mode de paiement par ces entreprises. Par contre, nous avons remarqué que certains commerçants hésitaient à les accepter, surtout s'il ne connaissait pas bien le portefeuille.

1.4.4. Les applications de paiements offertes par les commerçants de vente de détails

Les consommateurs qui les utilisent en magasin peuvent « scanner » le code à barres d'un produit. Cela leur procure de l'information sur le produit et leur donne accès au même produit dans d'autres tailles ou d'autres couleurs que celles offertes en magasin. Cela leur permet aussi d'acheter le bien sans passer à la caisse et de se le faire livrer où ils veulent (ou presque). Selon certains des experts que nous avons interviewés, il s'agit là d'un nouveau modèle d'affaire dans le milieu du commerce de détail; il a d'ailleurs été question de ce modèle d'affaires lors du Rendez-vous du commerce de détail de 2015 organisé par le Conseil canadien de commerce de détail.⁵⁷ Les détaillants qui offrent ce type d'applications aux consommateurs canadiens sont American Eagle Outfitters, Apple Store, Canadian Tire, Indigo, ToysRus, Urban Outfitters et Zara.

⁵⁷ Cet événement a eu lieu en octobre 2015 au Palais des congrès de Montréal.

1.5. Survol de l'encadrement législatif des paiements mobiles au Canada

Avec l'arrivée des PMPV, les consommateurs ont un nouveau mode de paiement pour payer leurs achats. Qui dit nouveaux modes de paiements dit aussi nouveaux risques. L'ACFC identifie six nouveaux défis spécifiquement liés aux paiements mobiles. Nous les résumerons ci-dessous. Ce faisant, nous porterons tout particulièrement attention aux enjeux de vie privée en lien avec les APMPV.

- Des protections inégales

Selon la provenance des fonds (carte de débit, carte de crédit ou cartes cadeaux, par exemple) les protections varient⁵⁸. Les règles de l'Association canadienne des paiements s'appliquent lorsque les fonds sont transférés d'une institution financière à une autre. En matière de cartes de paiement, les règles d'Interac, de Visa et de Mastercard s'appliquent dès qu'une opération transige par l'un de ces réseaux. Des codes volontaires peuvent aussi s'appliquer dans certains cas, notamment lors des opérations par carte de débit qui sont couvertes par le Code de pratique canadien des services de cartes de débit⁵⁹.

Pour leur part, les cartes cadeaux sont encadrées par les lois provinciales. Même si certaines règles sont similaires partout au Canada – c'est le cas de la règle selon laquelle une carte cadeau émise par un marchand ne peut pas expirer –, il n'y a pas d'harmonisation entre les diverses législations provinciales. En conséquence, les lois peuvent varier d'une province à l'autre, et ce, même pour une même carte émise par une même entreprise⁶⁰.

En 2014, le Règlement sur les produits de paiement prépayés est entré en vigueur⁶¹. Ce règlement s'applique aux cartes prépayées utilisant le réseau Visa et Mastercard, qui sont souvent émises par une institution financière (de compétence fédérale). Depuis que ce règlement existe, certaines provinces ont affirmé que leurs lois provinciales encadrant ces cartes cadeaux ne s'appliquaient plus. Il y a donc des différences d'une province à l'autre. Dans ce contexte, l'encadrement des APMPV comporte de nombreux défis.

- Une divulgation qui comporte un défi

Les émetteurs de fonds doivent divulguer de l'information aux consommateurs, notamment les termes et conditions de l'entente qu'ils ont avec eux. Au Canada, il n'est pas obligatoire que la divulgation soit optimisée pour un téléphone intelligent (voir sections 2 et 3)⁶².

⁵⁸ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 6

⁵⁹ Option consommateurs, « *La surveillance des systèmes nationaux de paiements de détail* », Commentaires présentés au ministère des Finances du Canada, Juin 2015

⁶⁰ Annik Bélanger-Krams, « *Le point de vue des Canadiens sur l'harmonisation des normes de protection du consommateur* », rapport présenté à Innovation, Sciences et Développement Économique Canada par Option consommateurs, mars 2015

⁶¹ Règlement sur les produits de paiement prépayés DORS/2013-209

⁶² TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 7

- Un risque de fraude et de mauvais usage des biens des consommateurs

Selon l'Agence de la consommation en matière financière du Canada (ACFC) l'utilisation des applications de paiements mobiles sans l'utilisation de numéro d'identifiant personnel (NIP) fait surgir une ambiguïté en matière de responsabilité zéro⁶³. La responsabilité zéro implique que, si la carte de crédit est volée ou perdue ou encore si elle est utilisée sans autorisation et qu'une transaction est effectuée, le consommateur pourra être remboursé. Elle s'applique généralement aux transactions faites par Internet, par téléphone ou chez le commerçant.⁶⁴ De plus, les consommateurs ont certaines craintes en matière de sécurité, notamment dans le cadre de l'utilisation de PMPV utilisant la technologie NFC. Il est en effet préoccupant que les fournisseurs n'aient pas d'obligations particulières. À noter, le Canadian NFC Mobile Payments Reference Model encadre les institutions financières y adhérant, ce qui a pour effet d'augmenter la protection des consommateurs. Toutefois, ce modèle comporte certaines lacunes, notamment parce que son adhésion est volontaire et qu'il n'y a aucun organisme de surveillance qui veille au respect de ce modèle⁶⁵.

- La responsabilité du règlement des différends

Selon l'ACFC, le principe de l'accessibilité à des mécanismes de règlements et de recours n'est pas uniformément appliqué aux paiements mobiles⁶⁶.

- L'éducation des consommateurs de produits financiers

Il est important que les consommateurs connaissent leurs droits et leurs obligations. Un consommateur bien informé est en mesure de prendre des décisions en toute connaissance de cause⁶⁷. Or, selon plusieurs rapports d'Option consommateurs, il y a une asymétrie informationnelle chronique entre les consommateurs et les fournisseurs de services⁶⁸. Les consommateurs connaissent mal les règles applicables, le fonctionnement, les coûts et les avantages comparatifs des modes de paiement qu'ils utilisent. Pire, ils confondent parfois les modes de paiement. Plusieurs consommateurs croient avoir les mêmes droits et obligations lorsqu'ils utilisent une carte prépayée, une carte de débit ou une carte de crédit⁶⁹. La situation devient plus complexe lorsque, afin d'attirer les clients, le fournisseur de services offre des taux

⁶³ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 8

⁶⁴ <http://www.fcac-acfc.gc.ca/Fra/ressources/publications/vosDroits/Pages/CreditCa-Lescarte-4.aspx> et <http://www.fcac-acfc.gc.ca/fra/consommateurs/sujets/vosDroits/Pages/CreditCa-Fraudepa.aspx>

⁶⁵ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 8

⁶⁶ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 8

⁶⁷ TRITES steve et als., Agence de la consommation en matière financière du Canada, « *Les paiements mobiles et la protection des consommateurs au Canada* », décembre 2013, page 8

⁶⁸ Option consommateurs, « *La surveillance des systèmes nationaux de paiements de détails* », commentaires au Ministère des finances du Canada, juin 2015, page 8 et Karine Robillard et Alexandre Plourde, « *Carte de débit virtuelle : Les consommateurs sont-ils bien protégés?* », rapport de recherche de Option consommateurs présenté à Innovation, Sciences et Développement Économique Canada, 2014

⁶⁹ Karine Robillard et Alexandre Plourde, « *Carte de débit virtuelle : Les consommateurs sont-ils bien protégés?* », rapport de recherche de Option consommateurs présenté à Innovation, Sciences et Développement Économique Canada, 2014

préférentiels, des programmes de fidélisation et des congés d'intérêts⁷⁰. Les recherches d'Option consommateurs démontrent que les consommateurs manifestent une grande confiance envers les réseaux de paiements et les institutions financières. On ne s'étonnera pas que les consommateurs soient peu enthousiastes à lire de longs documents écrits dans un jargon juridique⁷¹ que sont généralement les contrats d'adhésion⁷².

Nous croyons que les difficultés rencontrées envers les modes de paiements traditionnels sont amplifiées dans un contexte de paiement mobile, notamment en raison de la présence de nombreux acteurs, de technologies complexes et du défi que peut comporter la lecture d'un long document sur le petit écran d'un téléphone intelligent⁷³.

- L'éducation La protection des renseignements personnels et le profilage des consommateurs

À l'ère du *Big data*, utiliser une APMPV pour acheter un latté équivaut-il à révéler sa vie privée⁷⁴ ? Choses certaines : avec les APMPV, les entreprises peuvent recueillir plus de renseignements sur les consommateurs qu'avec les modes de paiement traditionnels⁷⁵. Et elles peuvent utiliser ces informations pour faire de la publicité ciblée (voir sections 2 et 3). Les avantages de ces nouveaux modes de paiement en valent-elle la peine? C'est la question qu'il faut se poser.

⁷⁰ Élise Thériault, « *Les cartes de crédits; de nouvelles solutions afin de mieux protéger les consommateurs* », rapport de recherche d'Option consommateurs, présenté à Innovation, Sciences et Développement Économique Canada, 2014

⁷¹ Option consommateurs, « *La surveillance des systèmes nationaux de paiements de détail* », Commentaire présenté au Ministère des Finances du Canada, page 9

⁷² La majorité des contrats de consommations conclus sur Internet sont des contrats d'adhésion, c'est-à-dire qu'une partie (le commerçant) impose les modalités du contrat à l'autre partie (le consommateur). Ce dernier n'a alors pas la possibilité de négocier les termes du contrat.

⁷³ ADAMS Carlisle, « *Les paiements mobiles en tout temps en tout lieu : bref survol du paysage des paiements mobiles* », Commissariat à la protection de la vie privée du Canada, juin 2013 et FTC Staff Report, « *Mobile Privacy Disclosures: Building Trust Through Transparency* », February 2013 et FTC Staff Report, « *Paper, Plastic...or Mobile?* An FTC Workshop on Mobile Payments » March 2013

⁷⁴ Option consommateurs, « *La surveillance des systèmes nationaux de paiements de détail* », Commentaire présenté au Ministère des Finances du Canada.

⁷⁵ FTC Staff Report, « *Mobile Privacy Disclosures: Building Trust through Transparency* », February 2013 et FTC Staff Report, « *Paper, Plastic...or Mobile?* An FTC Workshop on Mobile Payments » March 2013

Section 2. Les APMPV : bref survol de la problématique de vie privée

2.1. Point soulevé par les experts

Dans le cadre de notre recherche, nous avons interviewé de nombreux experts⁷⁶ afin de connaître leur opinion sur les enjeux de vie privée associés aux APMPV. À noter, les entrevues avec les deux entrepreneurs en informatique ont servi à nous éclairer sur le fonctionnement technique des applications, sur les enjeux et sur les tendances dans l'industrie. Ces experts nous ont aussi parlé du fonctionnement des normes existantes en matière de sécurité et de l'intérêt des entreprises à assurer la sécurité. Les experts en droit et en protection de la vie privée ont identifié plusieurs problèmes.

Voici la liste des enjeux identifiés :

- La sécurité

Un grand nombre d'entre eux sont inquiets des nouveaux enjeux de sécurité que pourraient avoir les APMPV. Certains le sont en raison du type de renseignements personnels recueillis, notamment des informations de nature financière. D'autres pointent du doigt les transferts d'informations. Plusieurs craignent l'augmentation de maliciels⁷⁷. La plupart s'entendent pour dire que les entreprises ont intérêt à assurer la protection des renseignements personnels des consommateurs, mais s'inquiètent de ce qui se produirait advenant une brèche de sécurité. D'autres encore craignent que, avec les PMPV, les vols de téléphones intelligents augmentent; chaque appareil mobile donnant accès aux outils de paiements de son propriétaire.

- Le grand nombre de renseignements personnels recueillis

Plusieurs de nos experts se préoccupent du très grand nombre de renseignements personnels pouvant être recueillis par ces APMPV. Ils craignent que ces renseignements ne soient pas conservés comme le requiert leur degré de sensibilité. Plusieurs experts soulèvent également la possibilité de recueillir des renseignements de nature financière. Ils mentionnent que, comme le consommateur a toujours son téléphone intelligent avec lui, il est aisé de découvrir son comportement et ses habitudes. Dans le même ordre d'idée, la possibilité d'utiliser la géolocalisation préoccupe plusieurs experts. Certains s'inquiètent également de la cueillette des identifiants biométriques des consommateurs (comme les empreintes digitales) à des fins d'identification.

- Le partage des renseignements personnels à des tiers pour des fins de marketing

Autre préoccupation : les APMPV partagent ou vendent les renseignements des consommateurs à des fins de marketing et de publicité ciblée. Certains reconnaissent que certains consommateurs aiment recevoir de la publicité ciblée. L'inquiétude porte sur les mécanismes

⁷⁶ La liste des experts interviewés se trouve à la section Remerciements.

⁷⁷ Les maliciels (ou logiciels malveillants) sont conçus pour infiltrer les ordinateurs ou les téléphones intelligents afin d'y effectuer des opérations non-autorisées.

utilisés pour créer le profil des consommateurs ainsi que sur l'envoi de certaines publicités ciblées à une clientèle vulnérable (par exemple l'envoi d'une publicité sur des produits amaigrissants à une personne ayant des troubles alimentaires).

- Les politiques de confidentialités

Les experts déplorent le fait que les politiques de confidentialité ainsi que les termes et conditions de l'entente soient de longs documents écrits dans un langage difficile à comprendre. Ils expriment l'importance d'ajuster ces documents à l'environnement des téléphones intelligents, ce qui est tout un défi, notamment en raison de la taille de l'écran et des comportements des consommateurs (ils utilisent les PMPV en tout temps et en tout lieu). Les consommateurs, disent-ils, peuvent être distraits ou pressés, ce qui les rend moins attentifs.

Selon plusieurs experts, la longueur et la complexité des politiques de confidentialité incite un très grand nombre de consommateurs à ne pas lire ces documents. Les entreprises, disent-ils, doivent rédiger des politiques de confidentialité succinctes, claires et faciles à comprendre. Si possible, les clauses pourraient même devenir attrayantes grâce à l'utilisation de résumés, de pop-up, de présentations sous forme multi strate⁷⁸, de listes, de couleurs et de sous-titres. Certains mentionnent l'importance de sensibiliser les consommateurs à l'importance de lire ces documents.

- L'impact sur les consommateurs

Plusieurs experts mentionnent que, dans l'état actuel des choses, le consommateur est désavantagé. D'une part, il ne comprend pas les mécanismes derrière les paiements mobiles. D'autre part, il en sait peu sur la collecte d'informations effectuée et la publicité ciblée. En fait, il y a des consommateurs qui sont capables d'identifier certains renseignements nominatifs comme étant des renseignements personnels, mais un grand nombre d'entre eux ne comprend pas les mécanismes du profilage. Certains experts affirment que le manque d'information peut porter atteinte au consentement des consommateurs, voire les empêcher de prendre leurs décisions en toute connaissance de cause.

Selon plusieurs experts, les consommateurs sont désavantagés puisqu'ils croient, à tort ou à raison, que le seul choix qui s'offre à eux est d'accepter et d'utiliser l'application ou de refuser et de ne pas l'utiliser. S'ils refusent, ils ne peuvent utiliser l'application. Ce qui n'aide pas, c'est que les consommateurs voient généralement la politique de confidentialité après avoir décidé qu'ils voulaient le produit mais avant de pouvoir l'utiliser.

Les consommateurs se trouvent souvent à devoir faire un choix de compromis en matière de vie privée (*privacy tradeoff*.) S'ils veulent vraiment utiliser l'application parce qu'ils en retirent des avantages, ils sont alors plus enclins à donner des renseignements personnels. Parmi les avantages de l'APMPV, mentionnons son aspect pratique, sa rapidité ou la possibilité qu'elle offre d'accumuler des points échangeables contre des récompenses. Par contre, les

⁷⁸ Une politique multi strate présente les informations sous une forme condensée. Si le consommateur veut obtenir plus d'information, il peut en obtenir en cliquant sur un lien. CHASSIGNEUX Cynthia, « *Guide pour l'élaboration d'une politique de confidentialité* », Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008, page 10 et the Center for Information and Policy Leadership, 2011

consommateurs peuvent choisir d'utiliser une APMPV sans savoir quels renseignements personnels sont recueillis à leur sujet ni ce qu'implique cette cueillette d'informations. Cette asymétrie d'information peut nuire aux consommateurs.

Toujours selon nos experts, les consommateurs ont souvent tendance à faire confiance aux entreprises et à penser que ces dernières sont de bonne foi ou qu'elles agissent dans leur intérêt lors de la collecte, la conservation et la divulgation de leurs renseignements personnels. Par ailleurs, ils n'ont pas tous les mêmes connaissances et la même perception de la vie privée. Certains sont beaucoup plus préoccupés par celle-ci que d'autres.

- Le manque de transparence des entreprises

Un autre point soulevé par plusieurs experts est le manque de transparence des entreprises, tant dans les politiques de confidentialité (elles n'énoncent pas clairement à qui elles transmettent les informations recueillies et comment elles le font) qu'au sujet des mécanismes derrière le traitement et le stockage des données.

- L'accessibilité des renseignements personnels par les autorités américaines

Plusieurs experts craignent que les renseignements personnels des consommateurs soient recueillis par une entreprise américaine ou soient stockés dans des serveurs situés aux États-Unis. Ils craignent que les renseignements des consommateurs canadiens y soient moins bien protégés, notamment en raison de la faiblesse et du caractère multisectoriel des lois américaines.

- Les solutions envisagées

Enfin, plusieurs experts croient que certaines entreprises n'appliquent pas la loi alors que d'autres croient que les lois devraient être plus sévères. D^{re} Anne Cavoukian, directrice Générale, du Privacy & Big Data Institute, de l'Université Ryerson, mentionne l'importance de la *Privacy by design* (la Protection intégrée de la vie privée), selon laquelle le respect de la vie privée doit être une préoccupation lors de la création des applications et non pas après.

2.2. Les enjeux de vie privée spécifique aux téléphones intelligents

Le téléphone intelligent présente quelques particularités en matière de protection de la vie privée. Contrairement à d'autres types d'appareil, comme l'ordinateur, il est généralement utilisé par une seule personne qui l'a sur elle ou près d'elle en tout temps⁷⁹. Cette personne l'utilise pour chercher de l'information en ligne, effectuer des opérations bancaires, envoyer des courriels, texter, clavarder, prendre des photos et les poster sur les réseaux sociaux. Selon un sondage américain de 2013, plus de la moitié des consommateurs utilisent leur téléphone intelligent pour surfer sur le web et, pour près du tiers des consommateurs qui utilisent un téléphone intelligent, il s'agit là du seul moyen d'accéder à Internet⁸⁰. Les téléphones

⁷⁹ FTC Staff Report, « Mobile Privacy Disclosures: Building Trust through Transparency », February 2013, page 2

⁸⁰ Kamala D. Harris, Attorney General California Department of Justice, « Privacy on the Go: Recommendations for the Mobile Ecosystem », January 2013

intelligents génèrent un nombre astronomique de données qui peuvent donner de l'information sur sa santé, ses intérêts politiques ou ses pratiques intimes (voir section 3). Or, ces données peuvent potentiellement être partagées avec les fournisseurs de réseaux sans fil, les systèmes d'exploitation mobiles, les fabricants de divers services liés au mobile, les développeurs d'applications, les entreprises d'analyse et les publicitaires. Avec un téléphone intelligent, tout ceci peut atteindre un sommet inégalé.⁸¹

Autre particularité : la petite taille des écrans des téléphones intelligents. Ceci pose un défi aux entreprises, qui ont des obligations de divulgation sur la collecte, l'utilisation, et la communication des renseignements personnels, ainsi que sur les fins de ladite collecte⁸². Sur un écran de téléphone intelligent, une politique de confidentialité peut paraître plus longue que sur un ordinateur. Elle apparaîtra aussi en caractères plus petits, ce qui risque de la rendre plus difficile à lire.

De plus, à cause du caractère de portabilité du téléphone intelligent, le consommateur peut télécharger une application partout et en tout temps. Il se peut qu'alors, il soit trop pressé pour lire la politique de confidentialité ou qu'il le fasse distraitemment, d'autant plus que ce document peut lui paraître long, fastidieux et difficile à comprendre. Les entreprises qui rédigent des clauses de confidentialité doivent s'assurer que leurs politiques de confidentialité tiennent compte de l'environnement particulier des téléphones intelligents.

2.3. ... et aux paiements électroniques

Que ce soit pour s'acheter un café, payer un titre de transport, ou pour faire ses courses, le consommateur fait des transactions presque tous les jours. La Banque mondiale écrit : « Les systèmes de paiements comprennent tous les systèmes imprimés et électroniques utilisés pour l'échange de valeur financière afin d'acquitter des obligations. Ils peuvent être simples (paiement en argent comptant pour les petits achats en personne) ou complexes (paiement électronique important, envoyé ou reçu par les institutions financières) »⁸³.

Lorsque le consommateur paie un achat ou un service, il y a un transfert d'argent entre celui-ci et le commerçant qui, à son tour transfère le bien ou le service au consommateur. Lorsqu'un consommateur fait un paiement électronique, il n'y a pas seulement un transfert de biens ou de service en échange d'espèces. Il y a également un transfert de renseignements personnels – ceux liés aux cartes de débit et de crédit, aux numéros de compte bancaires, aux cartes de fidélité, à l'historique d'achats et aux numéros d'identification personnels (NIP). Lorsqu'un paiement est effectué dans un environnement mobile ou numérique, les renseignements

⁸¹ FTC Staff Report, « Mobile Privacy Disclosures: Building Trust Through Disclosures », February 2013

⁸² FTC Staff Report, « Mobile Privacy Disclosures: Building Trust through Transparency », February 2013,

⁸³ Rapport de recherche de la Banque mondiale no 1519, « Payment Systems in Latin American » et Commissariat à la protection de la vie privée du Canada, « La transformation du système de paiements canadiens: pourquoi la protection de la vie privée est essentielle à la confiance à l'égard du système de paiements et son innovation », présentation du Commissariat à la protection de la vie privée du Canada au Groupe de travail sur l'examen du système de paiements, septembre 2011, page 3

personnels peuvent aussi inclure des données géographiques, notamment le moment des transactions, les adresses électroniques, l'historique de la navigation et les adresses IP⁸⁴.

Les consommateurs canadiens utilisent souvent une carte pour payer leurs achats. Selon l'Association des banquiers canadiens (ci-après ABC), 89 % des consommateurs ont une carte de débit⁸⁵. Selon Interac, en 2014, le nombre de transactions par débit approchait les 4900 millions de dollars⁸⁶. Les Canadiens sont parmi ceux qui utilisent le plus de cartes de débit au monde⁸⁷. Selon l'ABC, en 2014, il y avait 72 millions de cartes de crédit en circulation⁸⁸. Les consommateurs canadiens utilisent beaucoup les paiements de cartes sans contacts⁸⁹. Ces cartes sont offertes notamment par Interac FlashMD, Visa PayWaveMD, Mastercard PayPassMD. Différente des cartes de paiement ordinaire, elles sont munies d'une puce couplée à une antenne électronique qui utilise les ondes NFC pour transmettre l'information qui servira à la transaction sans que l'utilisateur n'ait à entrer un NIP ou à signer un reçu⁹⁰. Plusieurs experts considèrent les cartes sans contact comme un paiement mobile. Dans le cadre de notre étude, nous ne les étudions pas car nous nous limitons aux APMPV.

Par ailleurs, les consommateurs canadiens achètent de plus en plus en ligne. En 2012, la valeur du commerce électronique était de 22,3 billions de dollars⁹¹. En 2011, un groupe de travail a été formé pour étudier les enjeux de la modernisation du système de paiement canadien. Ce dernier a établi 12 principes, qui sont au «cœur d'une intendance avisée de l'écosystème de paiements», la protection des renseignements personnels est incluse dans ces principes⁹².

⁸⁴ Commissariat à la protection de la vie privée du Canada, « La transformation du système de paiements canadiens: pourquoi la protection de la vie privée est essentielle à la confiance à l'égard du système de paiements et son innovation », Mémoire du Commissariat non destinés au Parlement concernant des enjeux liés à la vie privée, Septembre 2011, page 3

⁸⁵ <http://www.cba.ca/fr/media-room/50-backgrounders-on-banking-issues/123-credit-cards> et Abacus Data, décembre 2014

⁸⁶ Commissariat à la protection de la vie privée du Canada, « La transformation du système de paiements canadiens: pourquoi la protection de la vie privée est essentielle à la confiance à l'égard du système de paiements et son innovation », Mémoire du Commissariat non destinés au Parlement concernant des enjeux liés à la vie privée, Septembre 2011, page 3

et <http://www.interac.ca/fr/debit-interac-statistics.html#no-de-transactions-par-debit-interac-de-commerçants-de-terminaux-d-utilisateurs-par-année-et-valeur-annuelle-en>

⁸⁷ Banque du Canada, printemps 2015 <http://www.banqueducanada.ca/wp-content/uploads/2015/05/revue-bdc-printemps15-fung.pdf>

⁸⁸ <http://www.cba.ca/fr/media-room/50-backgrounders-on-banking-issues/123-credit-cards>

⁸⁹ Les paiements sans contact peuvent être faits avec une carte de débit ou de crédit, sans qu'il soit nécessaire de l'insérer dans le terminal et composer son NIP.

⁹⁰ <http://www.cba.ca/fr/consumer-information/42-safeguarding-your-money/622-contactless-payment-card-security-an-faq>

⁹¹ CIRA <https://cira.ca/factbook/2014/fr/the-canadian-internet.html>

⁹² Commissariat à la protection de la vie privée du Canada, « La transformation du système de paiements canadiens: pourquoi la protection de la vie privée est essentielle à la confiance à l'égard du système de paiements et son innovation », Mémoire du Commissariat non destinés au Parlement concernant des enjeux liés à la vie privée, Septembre 2011, page 5 et Groupe de travail sur l'examen du système de paiement, « Nos modes de paiements : vers un système de paiements moderne » 2011, p 3

2.4. Le défi des APMPV

Lors d'un PMPV, il ne se produit pas qu'une transaction financière entre un consommateur et un commerçant. Il se produit aussi un échange d'informations. Parmi les informations transmises, il y a notamment les habitudes d'achats, l'historique de navigation et, parfois, contacts et activités sur les réseaux sociaux. En conséquence, les PMPV comportent beaucoup plus de risques en matière de vie privée que les paiements en espèces. Ils en comportent aussi davantage que les paiements par carte de débit ou de crédit. De plus, la plupart des acteurs qui font partie de l'écosystème des APMPV peuvent potentiellement avoir accès aux renseignements personnels du consommateur qui fait une transaction. Lorsqu'un consommateur achète un chandail et qu'il paie avec une carte de débit, le commerçant sait quel modèle de chandail il a acheté et de quelle couleur est ce chandail mais il ne connaît pas les données nominatives du consommateur, par exemple ses renseignements de contact. À l'inverse, la banque émettrice de la carte de débit connaît les informations de contact du consommateur et le nom du commerçant où l'achat a été effectué, mais elle ignore quel chandail il a acheté. Les APMPV permettent à l'ensemble des acteurs de l'écosystème de paiements mobile de recueillir des renseignements personnels et l'historique des achats du consommateur, puis de les regrouper. Selon la Federal Trade Commission (FTC), cela peut apporter des bienfaits, par exemple les commerçants peuvent offrir des produits adaptés aux goûts et aux préférences du consommateur. Par contre cela soulève des problèmes en matière de respect de la vie privée ainsi que des problèmes de sécurité⁹³.

⁹³ FTC Staff Report, « Paper, Plastic...or Mobile? » an FTC Workshop on Mobile Payments, March 2013

Section 3. Cadre juridique

3.1. Le droit à la vie privée

Le droit à la vie privée tel que nous le connaissons aujourd'hui est une conséquence directe de la révolution industrielle et de l'urbanisation du XIX^e siècle. Ces dernières ont amené la distinction entre la sphère privée et la sphère publique, tant pour les pays de Common Law que pour ceux de droit civil⁹⁴. Dans *Privacy and Freedom*, Alan Westin définit l'utilisation de l'information dans le contexte de la vie privée comme étant « *le droit d'une personne de contrôler, de gérer, de réviser et de supprimer de l'information sur elle-même et de décider quand, comment et dans quelle mesure cette information est communiquée à des tiers* » (traduction libre)⁹⁵. Ce faisant, il a pris le « Right to privacy »⁹⁶ de Samuel D. Warren et de Louis D. Brandeis, considéré comme la reconnaissance du droit à la vie privée américain, pour le transférer au contexte moderne des ordinateurs, des cartes de crédit et de la publicité ciblée⁹⁷. La conception de la vie privée de Westin a été incorporée dans les lois visant la protection des renseignements personnels des consommateurs⁹⁸.

3.2. Le contexte économique et protections des données

Les applications et les portefeuilles électroniques permettant les PMPV ont été développés par différents types d'entreprises dont des commerçants et des institutions financières. Dans l'écosystème des paiements mobiles, un grand nombre d'acteurs peuvent avoir accès aux renseignements personnels des consommateurs (voir section 2). En raison du contexte économique et de la mondialisation, plusieurs de ces entreprises sont américaines ou transfèrent et conservent les données des consommateurs aux États-Unis (voir section 3.8).

3.3. Champ d'application général

Au Canada, les consommateurs sont protégés par des lois qui offrent une protection complète⁹⁹. La Loi sur la protection des renseignements personnels et les documents électroniques (ci-après

⁹⁴ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 3

⁹⁵ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 6 et 7 et FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015, page 76

⁹⁶ Nous avons choisi de conserver le terme utilisé par l'auteur.

⁹⁷ WARREN Samuel & BRANDEIS Louis, « *The Right to Privacy* », 4 Harv. Law Review 193, 195-96 (1890) et CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 6 et 7

⁹⁸ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 6 et 7 et FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015, page 76

⁹⁹ FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015, page 76

LPRPDE) protège les Canadiens. On y trouve (à l'annexe 1) les 10 principes¹⁰⁰ encadrant les renseignements qui sont recueillis, utilisés et communiqués. La loi est également uniforme quant à son application. La LPRPDE protège les Canadiens puisqu'elle s'applique à toute « organisation », et ce, indépendamment de son secteur d'activité¹⁰¹. La LPRPDE assure une même protection minimale à tous les Canadiens.

La LPRPDE s'applique aussi à toute organisation qui recueille, utilise et communique des renseignements personnels et dont les activités sont interprovinciales¹⁰². Elle s'applique aussi aux entreprises de juridiction fédérale¹⁰³ ainsi qu'aux entreprises locales ou provinciales situées dans une province qui n'a pas adopté de loi essentiellement similaire à la LPRPDE¹⁰⁴.

Il est pertinent de noter que les entreprises fédérales incluent les banques au sens de l'article 2 de la Loi sur les banques¹⁰⁵. De plus, les entreprises de télégraphes sont des entreprises fédérales au sens de l'article 92 (10) (a) et 91 (29) de la Loi constitutionnelle. Les entreprises de services vocaux et de données sans fil mobile de détails (entreprise de réseau cellulaire) sont des entreprises de juridiction fédérale en raison de la métaphore de l'arbre vivant. Cette métaphore est une interprétation constitutionnelle qui dit que la constitution doit être interprétée de façon large et libérale de façon à s'adapter à l'évolution de la société canadienne¹⁰⁶.

Par ailleurs, les provinces ont compétence pour adopter des lois encadrant certains domaines d'activités et ce, en raison de leur compétence pour encadrer le droit civil au sens de l'article 92 (13) Loi constitutionnelle et le commerce local au sens de l'article 92 (10). Il est possible pour les deux paliers de gouvernement d'encadrer un même domaine d'activité tout en respectant le principe du partage des compétences.

En 2007, dans l'arrêt *Banque Canadienne de l'Ouest*, la Cour suprême a reconnu qu'une loi provinciale peut encadrer une entreprise fédérale (dans le cas en l'espèce, les banques) pourvu que la loi provinciale ne touche pas le cœur de l'activité de la banque. Dans ce cas, il était question d'une loi encadrant la vente de produit d'assurance (provinciale) par les banques¹⁰⁷.

En 2014, dans l'arrêt *Marcotte*, la Cour Suprême a réaffirmé le principe, qu'une loi provinciale pouvait s'appliquer aux banques pourvu qu'elle n'atteint pas le cœur des activités de l'entreprise. Dans cette cause, la Cour Suprême a conclu que la loi sur la protection du consommateur (une loi du Québec) visant la divulgation de frais de crédit pouvait s'appliquer aux banques¹⁰⁸.

¹⁰⁰ Certains auteurs parlent de 11 principes. Dans le cadre de cette étude, nous avons choisi d'étudier les dix principes de l'annexe 1 et d'aborder l'article 5 (3) de la LPRPDE séparément.

¹⁰¹ Article 3 et 4 Loi sur la protection des renseignements personnel et les documents électronique, L.C. 2000, ch. 5 (ci-après LPRPDE)

¹⁰² Art 4 LPRDPE

¹⁰³ Art 2 LPRDPE et Art. 91 Loi constitutionnelle de 1867, 30 & 31 Victoria, c 3 (ci-après Loi constitutionnelle)

¹⁰⁴ Art 26 (2) b) LPRDPE

¹⁰⁵ Loi sur les banques¹⁰⁵, LC 1991, c 46

¹⁰⁶ RYAN Michael, «Telecommunications and the Constitution : Re-Setting the Bounds of Federal Authority », 2010, vol. 89, La revue du Barreau Canada, page 695-727

¹⁰⁷ *Banque Canadienne de l'Ouest c. c. Alberta*, [2007] 2 RCS 3

¹⁰⁸ *Banque de Montréal c. Marcotte* 2 RCS 725

En matière de vie privée, le commissariat à la protection de la vie privée a été saisi de plusieurs dossiers contre des entreprises de télécommunications, notamment la collecte sans consentement des clients de Bell pour fins de publicité ciblée¹⁰⁹.

Par contre, plusieurs décisions démontrent que la Loi québécoise peut s'appliquer à ces entreprises. La Commission d'accès à l'information a rendu des décisions contre des entreprises de télécommunications en raison de violation de la Loi québécoise. La CAI a reconnu avoir compétence pour entendre une plainte et appliquer la Loi québécoise¹¹⁰. De plus, de nombreuses décisions ont été rendues sur l'application de la Loi québécoise à des entreprises de compétence fédérale¹¹¹. Les entreprises fédérales pourraient être encadrées par les deux Loi. Ces deux lois sont « essentiellement similaires », même s'il peut y avoir entre elles quelques différences mineures¹¹².

Par ailleurs, la LPRPDE s'applique lorsqu'une organisation divulgue de l'information à l'extérieur de la province où elle l'a recueillie¹¹³. Pour que la loi fédérale s'applique, les renseignements doivent être vendus pour de l'argent ou une équivalence monétaire. L'information pourra être considérée comme ayant été vendue si elle a été fournie avec d'autres produits et services moyennant un paiement. Il n'y a pas vente d'information si le transfert d'information est secondaire ou fait pour d'autres considérations. La LPRPDE ne s'appliquera pas si les informations ont été accessoirement transférées. Selon les commentaires du CPVP, les organisations qui sont assujetties aux lois provinciales, essentiellement semblables au sens de l'article 26 (2) b) de la LPRPDE, sont néanmoins sujet à l'application de la LPRPDE en ce qui concerne les transferts inter provinciaux¹¹⁴. Le législateur du Québec, de l'Alberta et de la Colombie-Britannique sont intervenus pour encadrer la protection des renseignements recueillis par les organisations du secteur privé, ces lois provinciales sont reconnues comme étant essentiellement semblables à la LPRPDE¹¹⁵. 116 117 118 119

3.3.1. Les principes relatifs à l'équité dans le traitement de renseignements

Ces quatre lois (la loi fédérale et les trois lois provinciales) protègent les renseignements personnels des Canadiens à travers le Canada selon les 10 principes relatifs à l'équité dans le

¹⁰⁹ LPRPDE No: 2015-001

¹¹⁰ X. c. *Rogers Communications inc.* Commission d'accès à l'information du Québec, 11310 et Bell décision 1005977

¹¹¹ *Nadler c. Rogers Communications Inc.*, 2014 QCCQ 5609, *Lamarre c. Banque Laurentienne*, C.A.I. 99 09 63, *Boissonot, Laporte et Stoddart*, Z-5014474, *Pierre c. Fédéral Express Canada Ltée*, 2003 CAI 139

¹¹² Art 26 (2) b) LPRDPE

¹¹³ Art 30 (1) LPRDPE. Ceci est fondé sur le pouvoir constitutionnel du fédéral de réglementer les relations et le commerce interprovinciale. MCNAIRN H.H. Colin, « A guide to the Personal Information Protection Act », Lexis Nexis, 2013, Second edition, page 17

¹¹⁴ *Ibid.* et commentaire du CPVP

¹¹⁵ Art 26 (2) b) LPRDPE

¹¹⁶ Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1 (ci-après loi québécoise)

¹¹⁷ Personal Information Protection Act, S.A. 2003, c.P-6.5, (ci-après Alta PIPA)

¹¹⁸ Personal Information Protection Act, S.B.C. 2003, c. 63 (ci-après BC PIPA)

¹¹⁹ Trois autres provinces ont adopté des lois essentiellement équivalente, ces dernières sont uniquement applicables aux dépositaires de renseignements sur la santé. Il s'agit de l'Ontario avec la Loi de 2004 sur la protection des renseignements personnels sur la santé, L.O. 2004, c. 3, annexe A, le Nouveau Brunswick, avec la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé, L.N.-B., 2009, c. P-7.05 et Terre-Neuve-et-Labrador avec Personal Health Information Act, S.N.L. 2008, c. P-7.01

traitement des renseignements personnels¹²⁰. Ces principes ont été codifiés pour la première fois dans *Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de caractère personnel* de l'OCDE en 1980¹²¹. Le Canada a adhéré à ces lignes directrices en 1984. Les lignes directrices ont inspiré le Canada qui a développé des outils législatifs pour encadrer la protection de la vie privée. Puis, le Code type sur la protection des renseignements personnels du CSA a été créé. Celui-ci a été approuvé par le Conseil canadien des normes en 1996¹²². Puis, en 1998, la Directive 95/46/CE sur la protection de données personnelles est entrée en vigueur en Union européenne. Les pays membres de l'Union européenne doivent adopter des lois encadrant la collecte de renseignements personnels. Ceci est important pour le Canada car la directive empêche le transfert de renseignements personnels à des pays externes qui n'ont pas un niveau de protection adéquat¹²³. C'est dans ce contexte que la LPRDPE a été adoptée. À noter, les 10 principes de la CSA se trouvent à l'annexe 1 de la LPRDPE¹²⁴. Les voici.

Premier principe : la responsabilité

Les organisations sont responsables des renseignements personnels dont elles ont la gestion. Elles doivent désigner une personne qui s'assurera du respect des principes. Elles doivent également s'assurer que les tiers à qui elle transfère des renseignements respectent la LPRDPE¹²⁵.

Deuxième principe : la détermination des fins de la collecte des renseignements

L'organisation doit informer les consommateurs des fins de la collecte, et ce avant la collecte ou au moment celle-ci. L'organisation doit documenter les fins de la collecte pour se conformer aux principes de transparence. Elle doit limiter la collecte aux fins précisées. Ce principe est étroitement lié à l'article 5 (3) de la LPRDPE qui énonce que la collecte, l'utilisation et la communication des renseignements personnels doivent être faites selon les fins qu'une personne considérerait raisonnable eu égard aux circonstances¹²⁶. Le principe de déterminer les fins de la collecte est étroitement limité avec les principes de limitations de la collecte (annexe article 4.4) et de la limitation de l'utilisation de la collecte de renseignements¹²⁷.

¹²⁰FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015, page 76

¹²¹ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 87

¹²² Colin H.H. MCNAIRN, « A Guide to the Personal Information Protection and Electronic Document Act », Lexis Nexis, 2013, Second edition, page 3

¹²³ Colin H.H. MCNAIRN, « A Guide to the Personal Information Protection and Electronic Document Act », Lexis Nexis, 2013, Second edition, page 6 et SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 88

¹²⁴ FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015

¹²⁵ Annexe 1 clause 4.1.3. et SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 131 et 132 et Article 6 LPRDPE

¹²⁶ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 132

¹²⁷ Annexe 1 4.2.1. à 4.2.6 LPRDPE

Troisième principe : le consentement

C'est la pierre angulaire du régime législatif canadien. Toute personne doit être informée et consentir à la collecte ainsi qu'à l'utilisation et à la communication des renseignements recueillis, sous réserve des exceptions prévues par la loi, notamment à la suite de l'obtention d'un subpoena, pour des raisons de sécurité nationale ou lors d'une enquête demandée par un tribunal. La clause 4.3.2 (annexe 1 de la LPRPDE) met l'accent sur le consentement. Elle énonce que «pour que le consentement soit valable, les fins doivent être énoncées de façon à ce que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués». L'information doit donc être divulguée clairement et avec concision. Le CPVP a déjà accepté des plaintes lorsque les fins de la collecte étaient trop vagues¹²⁸.

La forme du consentement peut varier selon les circonstances et la nature des renseignements personnels. Afin de déterminer la forme du consentement, il faut regarder la sensibilité des renseignements personnels. Imaginez une échelle pour la mesurer. À un extrême, on trouverait les renseignements personnels qui sont toujours considérés comme sensibles, par exemple ceux liés à la santé ou au revenu (numéro de compte de banque, NIP, etc.¹²⁹) et, à l'autre extrême, on trouverait ceux qui le sont moins, comme le nom et l'adresse¹³⁰. À noter : le contexte doit aussi être pris en considération. Le nom et l'adresse d'une personne qui s'abonne à un magazine érotique peut être considéré comme un renseignement sensible¹³¹.

L'organisation qui recueille des renseignements sensibles doit les protéger selon leur niveau de sensibilité. Elle doit faire de même lorsqu'elle les utilise et les communique. L'historique des transactions est également un renseignement personnel¹³². Nous croyons que l'historique des achats peut également être un renseignement sensible. Le fait qu'un consommateur achète un café dans un restaurant n'est pas nécessairement un renseignement sensible. Par contre, le fait qu'il achète beaucoup de jetons au casino pourrait être un renseignement sensible¹³³. Selon nous, l'ensemble des achats faits par un consommateur grâce à son portefeuille électronique devrait être considéré comme sensible. Cet ensemble de renseignements sur les achats effectués permet de créer un profil très précis du consommateur.

Il faut aussi regarder les attentes du consommateur et de l'entreprise. La LPRPDE donne l'exemple d'une personne qui s'abonne à un périodique qui lui sera livré à la maison. Cette personne peut s'attendre à ce que son nom et son adresse soit utilisés pour des fins de facturation. L'organisation peut s'attendre à ce que la personne ait donné son consentement. Par contre, une personne ne s'attendra pas à ce que des renseignements personnels liés à sa santé soient divulgués à des tiers, par exemple une entreprise qui vend des produits pour la santé¹³⁴. Un consommateur qui utilise l'application d'un commerçant et se fait livrer un bien

¹²⁸ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 132 et LPRPDE No 2003-192

¹²⁹ LPRPDE No 2006-335 et LPRPDE 2006-356 et https://www.priv.gc.ca/leg_c/interpretations_02_f.asp#fn33

¹³⁰ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 139

¹³¹ Annexe 1 4.3.4 LPRPDE

¹³² LPRPDE No 2006-356 et https://www.priv.gc.ca/leg_c/interpretations_02_f.asp#fn33

¹³³ Annexe 1 4.3.4 LPRPDE

¹³⁴ Annexe 1 4.3.5 LPRPDE

peut s'attendre à ce qu'on lui demande son adresse. Il ne s'attend pas à ce que son portefeuille électronique divulgue à des tiers l'ensemble de ses transactions.

Une organisation devrait chercher à obtenir un consentement explicite si les renseignements personnels sont considérés sensibles. Dans le cas de renseignement peu sensibles, un consentement implicite (opt-out) peut être suffisant¹³⁵. Les spécialistes en vie privée préfèrent le consentement explicite (opt-in). Ce dernier oblige les organisations à bien informer les utilisateurs de leurs pratiques.

Le consentement implicite est permis par le CPVP si l'information ainsi obtenue n'est pas sensible eu égard à sa nature et à son contexte. L'utilisation et la divulgation de l'information est alors limitée aux fins de la collecte. Ces fins doivent être clairement expliquées et ces explications doivent être facilement accessibles. Le consentement est obtenu avant la collecte (si possible). De plus, il est facile pour les utilisateurs de retirer leur consentement¹³⁶. Le CPVP a énoncé des lignes directrices pour la publicité comportementale en ligne (PCL) (voir section 3.6). Selon celles-ci, il est possible d'obtenir un consentement implicite pour des fins de marketing si les renseignements ne sont pas sensibles¹³⁷. Le principe du consentement est également lié au principe de la détermination des fins de la collecte, cela pour que la personne soit en mesure de réellement consentir à la collecte.

De plus, une organisation ne peut pas exiger qu'une personne donne son consentement à la collecte, à l'utilisation ou à la communication de ses renseignements personnels afin de lui permettre d'obtenir le bien et le service, à moins que ces renseignements soient « légitimes » pour réaliser les fins légitimes qui sont explicitement indiquées¹³⁸. Ce que nous venons de mentionner devrait être lu conjointement avec l'article 5 (3) de la LPRPDE, qui se lit ainsi : « L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »¹³⁹

Par ailleurs, une personne peut retirer son consentement, à moins de restrictions légales ou contractuelles et à condition de donner un préavis raisonnable. L'organisation doit informer le consommateur des conséquences du retrait de son consentement¹⁴⁰.

Quatrième principe : la limitation de la collecte

L'organisation ne peut recueillir que les renseignements personnels nécessaires à la fin de la collecte. Cette collecte doit être faite de façon licite et honnête. Le principe de la limitation des fins de collecte est étroitement lié au consentement et à la détermination des fins de la collecte¹⁴¹. Ce principe doit être lu conjointement avec l'article 5 (3) de la LPRPDE. La clause

¹³⁵ Annexe 1 4.3.6 LPRPDE

¹³⁶ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 139

¹³⁷ FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, page 77 et MCNAIRN Colin H.H. « A Guide to the Personal Information Protection and Electronic Document Act », Lexis Nexis, 2013, Second edition et Annexe 1 4.3.1. à 4.3.8 LPRPDE

¹³⁸ Annexe 1 4.3.3. LPRPDE

¹³⁹ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 137

¹⁴⁰ Annexe 1 4.3.8 LPRPDE

¹⁴¹ Annexe 1 4.4.1 à 4.4.3 LPRPDE

4.4.1 de l'annexe 1 énonce que, si de l'information est recueillie mais non utilisée, le principe de la limitation de la collecte est enfreint¹⁴².

Cinquième principe : la limitation de l'utilisation, de la communication et de la conservation

Les renseignements personnels recueillis ne peuvent être divulgués que pour les fins auxquelles ils ont été recueillis, à moins que la personne ait donné son consentement ou que cela soit requis par la loi. L'article 7 de la LPRPDE énonce les cas où les renseignements personnels peuvent être divulgués à des tiers, à l'insu de la personne, notamment lors d'une enquête en contravention à une loi fédérale ou provinciale ou pour des fins de statistique¹⁴³. L'information recueillie ne peut être conservée que prévue pour les fins de la collecte. Pour ce faire, les entreprises doivent élaborer des directives quant à la durée de la conservation, puis les appliquer. Elles doivent faire de même en ce qui a trait à la destruction des renseignements personnels. Ce principe est étroitement lié à celui du consentement, de la détermination des fins de la collecte et à l'accès individuel aux données¹⁴⁴.

Sixième principe : l'exactitude

Les renseignements personnels doivent être exacts, complets et à jour eu égard aux fins de la collecte. Le degré d'exactitude, la mise à jour et le caractère complet qu'exigent les fins de la collecte de ces renseignements, compte tenu des intérêts de la personne¹⁴⁵. Les informations doivent être le plus complètes possible de façon à éviter leur utilisation inappropriée. Une organisation ne doit pas systématiquement mettre à jour les renseignements qu'elle possède, à moins que cela soit nécessaire pour atteindre les fins de la collecte pour lesquelles les informations ont été recueillies¹⁴⁶.

Septième principe : les mesures de sécurité

Ces mesures sont destinées à empêcher le vol, mais aussi la consultation, la communication, la copie et la modification non autorisée. L'organisation qui recueille les informations prend l'entière responsabilité lorsqu'elle partage des renseignements à des tiers pour des fins de traitement¹⁴⁷. L'environnement numérique, notamment l'infonuagique¹⁴⁸, crée de nouveaux défis en matière de sécurité. Par ailleurs, le CPVP indique que les consommateurs ont aussi un rôle à jouer pour protéger leurs renseignements personnels. Par exemple, s'il est indiqué que le

¹⁴² SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 162

¹⁴³ Art 7 (2) a) et c) LPRPDE

¹⁴⁴ Annexe 1 4.5.1 à 4.5.4 LPRPDE

¹⁴⁵ Annexe 1 4.6.1 LPRPDE

¹⁴⁶ Annexe 1 4.6.1 à 4.6.1. LPRPDE

¹⁴⁷ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 168

¹⁴⁸ L'U.S. National Institute of Standards and Technology (NIST) le définit *par* « L'infonuagique est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur de services. Ce modèle, qui favorise l'accessibilité, est composé de cinq caractéristiques essentielles, de trois modèles de service et de quatre modèles de mise en œuvre »

consommateur doit saisir un mot de passe sécuritaire pour accéder à son compte et qu'il ne le fait pas, l'organisation pourrait ne pas être tenue responsable¹⁴⁹.

Huitième principe : la transparence

Une organisation doit s'assurer que les renseignements précis sur ses politiques et pratiques concernant les renseignements personnels soient facilement accessibles. Une personne doit être capable d'obtenir de l'information sans effort déraisonnable. Elle doit également obtenir de l'information compréhensible¹⁵⁰. Une organisation peut choisir la façon dont elle rend accessibles les informations concernant sa politique et ses pratiques. La méthode choisie doit prendre en compte la nature des activités de l'organisation. Par exemple, offrir une ligne sans frais pour obtenir plus d'informations¹⁵¹. Par ailleurs, l'obligation de transparence prévoit que les entreprises doivent faire savoir aux consommateurs que leurs renseignements personnels sont stockés à l'étranger et qu'ils pourraient être sujets aux lois d'une autre juridiction¹⁵².

Neuvième principe : l'accès aux renseignements personnels

Une personne doit pouvoir obtenir de l'information sur l'existence, l'utilisation et la divulgation de ses renseignements personnels. Par ailleurs, si les informations sont inexactes, elle peut demander à ce qu'elles soient modifiées¹⁵³.

Dixième principe : la possibilité de porter plainte

Une personne peut porter plainte du non-respect des principes (art 4.1.1.). Les organisations doivent établir une procédure pour recevoir les plaintes et les demandes de renseignements.

3.3.2. La limitation de la finalité

Les organisations peuvent recueillir des renseignements personnels seulement pour des motifs qu'une personne raisonnable trouverait appropriés eu égard aux circonstances¹⁵⁴. Lorsqu'une personne donne son consentement, elle s'attend à ce que ce soit le cas. La LPRDPE prévoit d'ailleurs que le consentement éclairé constitue la pierre angulaire du régime de protection des renseignements personnels¹⁵⁵.

Les lois provinciales qui encadrent la protection des renseignements personnels indiquent ce que les organisations peuvent recueillir comme informations si le motif est raisonnable. Le législateur québécois ne mentionne pas explicitement le caractère raisonnable; il réfère plutôt

¹⁴⁹ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 172 et LPRDPE No 2005-315

¹⁵⁰ Annexe 1 4.8.2. LPRDPE

¹⁵¹ Annexe 1 4.8.3 LPRDPE

¹⁵² SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 174

¹⁵³ Annexe 1 4.9.1 à 4.9.6. LPRDPE

¹⁵⁴ Art 5.3. LPRDPE

¹⁵⁵ FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015, page 77

aux articles 35 à 40 du Code civil du Québec (CcQ). L'article 37 du CcQ énonce que « toute personne » qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime pour le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et ne peut, sans le consentement de la personne intéressée ou par la loi, les communiquer à des tiers ou encore les utiliser à des fins incompatibles avec celle de sa constitution ou de l'utilisation du dossier. Elle ne peut non plus porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation¹⁵⁶.

Au Québec, la Charte des droits et libertés de la personne permet de trancher des litiges en matière de vie privée. Cette charte est une loi quasi constitutionnelle. En ce sens, elle a préséance sur les autres lois adoptées par le législateur québécois. Elle s'applique non seulement à l'État, mais également aux entreprises privées. Dans plusieurs causes invoquant des violations à la vie privée, il s'agit de savoir si l'atteinte à la vie privée est raisonnable dans une société juste et démocratique. Il faudra ainsi s'assurer que l'objectif est suffisamment important (préoccupation urgente et réelle) et que ses effets sont proportionnels entre la mesure restrictive et l'objectif à atteindre tel qu'énoncé dans l'arrêt *Oakes*¹⁵⁷.

En Colombie-Britannique, la *Personal Information Protection Act* (PIPA) énonce à l'article 4 que, pour respecter ses obligations légales, l'organisation doit se demander ce qu'une personne raisonnable considérerait approprié eu égard aux circonstances (traduction libre). Par ailleurs, les articles 11 (2), 16 (2) et 19 (2) de la PIPA limitent les fins de la collecte. À noter : à l'article 2 de sa loi, l'Alberta utilise une définition similaire¹⁵⁸.

3.4. Les renseignements personnels

La LPRPDE et les lois provinciales sont semblables. Elles protègent les renseignements personnels des utilisateurs. On l'a dit plus tôt : les renseignements personnels sont définis comme des renseignements permettant d'identifier un individu¹⁵⁹. Or, le terme « renseignement personnel » doit être interprété largement¹⁶⁰. Il désigne les renseignements nominatifs, mais aussi les renseignements qui, liés à d'autres, permettent d'identifier une personne¹⁶¹. Le CPVP écrivait qu'un renseignement peut constituer un renseignement personnel lorsqu'il existe une possibilité sérieuse que la personne puisse être identifiée au moyen de ce renseignement ou si celui-ci est combiné à d'autres renseignements disponibles¹⁶².

Dans le cadre d'un résumé d'enquête, le CPVP écrivait que « des renseignements qui, à eux

¹⁵⁶FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015 page 78

¹⁵⁷ *Ibid.* et *R. c. Oakes*, [1986] 1 RCS 103

¹⁵⁸ *Ibid.*

¹⁵⁹ Art 2 (1) LPRPDE et FIFA, *supra* note 152 et MCNAIRN *Ibid.* et CHASSIGNEUX *Ibid.*

¹⁶⁰ *Canada (Commissaire à l'information) c. Canada* (Commissaire de la Gendarmerie royale du Canada), [2003] 1 R. S. C. 66, par. 23

¹⁶¹ FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015 page 80

¹⁶² *Gordon c. Canada (Santé)*, 2008 CF 258,

seuls, peuvent ne pas être considérés comme personnels peuvent être considérés comme personnels lorsqu’une organisation a la capacité d’établir un lien entre ces renseignements et un individu identifiable ».¹⁶³ Les tribunaux ont une interprétation similaire. Dans l’arrêt Gordon, la cour fédérale écrit « il existe des précédents selon lesquels un individu “identifiable” est une personne dont il est raisonnable de croire qu’elle pourra être identifiée à l’aide des renseignements en cause s’ils sont combinés avec des renseignements d’autres sources »¹⁶⁴.

Autres considérations : un renseignement n’a pas à être consigné pour être un renseignement personnel; il suffit qu’il porte sur un individu identifiable¹⁶⁵. Un renseignement personnel n’a pas non plus besoin d’être directement attribuable à une personne; il suffit que la personne puisse être suivie et retracée¹⁶⁶. Les informations liées à la santé sont des renseignements personnels, et ce, même s’ils ont été dépersonnalisés s’il y a une possibilité élevée que les données dépersonnalisées soient associées à une personne identifiable¹⁶⁷. Les renseignements financiers tels que ceux sur les comptes de banque, les transactions, les soldes, les investissements et les dettes, sont considérés comme des renseignements personnels¹⁶⁸.

Dans le secteur informatique aussi, de nombreuses informations peuvent être qualifiées de renseignements personnels. Ainsi, l’adresse IP¹⁶⁹ peut être considérée comme un renseignement personnel si elle peut être associée à un individu identifiable¹⁷⁰. Une adresse IP peut révéler beaucoup d’informations, notamment les services en lignes d’abonnement et les intérêts personnels – en fonction des sites web visités ou des déplacements (géolocalisation). Les renseignements collectés peuvent être très sensibles¹⁷¹. La géolocalisation est également reconnue comme un renseignement personnel. Dans une cause où un employeur suivait les déplacements d’un employé à bord d’un véhicule, le Commissaire a reconnu que la géolocalisation était un renseignement personnel¹⁷². L’augmentation fulgurante de la popularité des appareils permettant la géolocalisation, notamment les téléphones intelligents, soulève d’importantes des questions en matière de vie privée. Désormais, il est plus facile que jamais de suivre les consommateurs sans que ceux-ci ne s’en rendent compte. Souvent, ils ne savent pas non plus que cela peut se produire. Cette information peut être fort utile pour les autorités policières, les malfaiteurs, les employeurs et même les membres d’une même famille¹⁷³.

La géolocalisation permet aussi d’obtenir des informations qui seront utilisées à des fins de marketing (voir section 3.6). Le numéro unique d’un appareil électronique ne permet pas à lui seul d’identifier l’utilisateur de l’appareil, mais il peut être associé à un compte qui, lui, contient

¹⁶³ LPRPDE No 2013-017, para 34

¹⁶⁴ *Gordon c. Canada (Santé)*, 2008 CF 258, para 32

¹⁶⁵ *Morgan c. Alta Flights Inc.* 2006 CAF 121

¹⁶⁶ FIFA (BC Freedom of Information and Privacy Association), « The Connected Car: Who is in the driver’s seat? A study on privacy and onboard vehicle telematics technology », project funded by the Office of the Privacy Commissioner of Canada, 2015, page 82

¹⁶⁷ LPRPDE No 2009-018

¹⁶⁸ LPRPDE No 2006-35, LPRPDE No 2006-332 et LPRPDE No 2006-356

¹⁶⁹ Une adresse IP (Internet Protocol) est un numéro d’identification attribué à chaque appareil utilisant le réseau Internet et qui rend possible la communication des informations sur le réseau

¹⁷⁰ LPRPDE 2001-25, LPRPDE 2001-35 et LPRPDE 209-010

¹⁷¹ CPVP, « Ce qu’une adresse IP peut révéler à votre sujet », mai 2013

¹⁷² LPRPDE No 2006-351

¹⁷³ SCASSA Teresa, « Electronic Commerce and Internet Law », 2nd Edition, CCH Canadian, Toronto, 2012, page 174

des informations qui permettent d'identifier le titulaire du compte¹⁷⁴. Les renseignements obtenus grâce au suivi d'étiquette par radiofréquence (RFID)¹⁷⁵ peuvent être des renseignements personnels¹⁷⁶.

Par ailleurs, les informations biométriques, comme les empreintes digitales, sont des renseignements personnels. L'ampleur ce qu'elles révèlent dépendra de la façon dont elles sont utilisées¹⁷⁷. Certains portefeuilles électroniques utilisent les empreintes digitales des consommateurs comme identifiant personnels lors de transactions; c'est notamment le cas d'ApplePay.

Le contenu des messages transmis sur les médias sociaux est aussi considéré comme un renseignement personnel¹⁷⁸. Il en va parfois de même des recherches effectuées sur des moteurs de recherches. En 2014, le CPVP a conclu que Google avait collecté des renseignements personnels sensibles sur un utilisateur; il s'agissait de ses recherches sur les troubles du sommeil. On lui avait fait parvenir de la publicité ciblée sur des appareils médicaux prétendument susceptibles de régler son problème¹⁷⁹.

3.5. La confiance

La confiance est au cœur du commerce électronique et des paiements mobiles. Car lors de ces transactions, il y a la communication des renseignements personnels à une entreprise en ligne¹⁸⁰. Les Lois comme la LPRDPE et ses contreparties provinciales s'assurent d'encadrer les pratiques, ce qui peut avoir un impact positif sur la confiance. Les contrats jouent également un rôle en édictant les règles du jeu¹⁸¹. Ceux-ci doivent respecter les lois visant à protéger les renseignements personnels et les lois provinciales de protection du consommateur. La confiance est importante puisqu'elle est étroitement liée au consentement éclairé. Pour que la relation contractuelle existe, il faut qu'il y ait un échange de consentements¹⁸².

Les politiques de confidentialité « formalisent les engagements des commerçants électroniques envers les consommateurs. Elles indiquent aux consommateurs les engagements de l'entreprise relativement à la collecte des données. (...) Par conséquent, elles doivent non seulement être crédibles, claires, mais également accessibles »¹⁸³. Les commerçants doivent y faire référence dans les termes et conditions de l'entente. Les politiques de confidentialité doivent respecter et inclure les principes requis dans les lois de protection de renseignements personnels. L'intégration de ces principes légaux aux politiques de confidentialité démontre comment les

¹⁷⁴ LPRPDE No 2013-017

¹⁷⁵ La radio-identification ou Radio Frequency Identification (RFID) est une méthode pour mémoriser et récupérer les données à distance grâce à l'utilisateur de marqueurs de radio-étiquettes

¹⁷⁶ https://www.priv.gc.ca/information/research-recherche/consultations/2008/rfid_f.asp

¹⁷⁷ *Wansinck c. Telus Communications Inc.*, 2007 CFA 21

¹⁷⁸ LPRPDE no 2013-001

¹⁷⁹ LPRPDE no 2014-001

¹⁸⁰ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 67

¹⁸¹ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 87

¹⁸² CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 94

¹⁸³ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 97

normes de protection des renseignements personnels sont interreliées». ¹⁸⁴

La confiance joue un rôle fondamental en matière de paiements. Plusieurs études démontrent que les consommateurs canadiens font confiance au système bancaire et aux institutions financières. Les entreprises doivent favoriser le respect de la vie privée au risque de voir les consommateurs perdre confiance. D'ailleurs, selon le CPVP, si les entreprises doivent se conformer à la Loi, c'est notamment pour ne pas miner la confiance des consommateurs ¹⁸⁵.

De son côté, la FTC indique que, pour augmenter la confiance des consommateurs, les entreprises doivent avoir des pratiques transparentes. D'ailleurs, lorsqu'elles ont de telles pratiques, les consommateurs sont plus susceptibles de faire affaire avec elles ¹⁸⁶. En 2014, 90 % des répondants à un sondage du CPVP étaient inquiets de la protection de leurs renseignements personnels, 73 % d'entre eux croyaient que leurs renseignements personnels étaient moins bien protégés qu'il y a dix ans et 56 % d'entre eux ne croyaient pas avoir les connaissances suffisantes pour comprendre comment les nouvelles technologies affectaient leur vie privée. De plus, le trois quart des répondants étaient préoccupés par ce qu'il pourrait advenir des renseignements personnels stockés sur les appareils mobiles en cas de perte ou de vol. Par ailleurs, les trois quarts des répondants ont refusé de télécharger ou ont désinstallé une application en raison de leurs inquiétudes vis-à-vis leur vie privée. Une hausse de 20 % par rapport à un sondage de 2012 ¹⁸⁷.

3.6. La publicité comportementale en ligne

Certaines applications sont offertes par des entreprises. D'autres applications sont offertes par des institutions financières alors que les portefeuilles électroniques sont offerts par des entreprises. Toutes ces applications permettent aux consommateurs de faire des PMPV ou de payer un bien en magasin et de se le faire livrer subséquemment. Elles peuvent toutes être téléchargées gratuitement.

Certaines applications donnent aussi des bienfaits directs et identifiables aux commerçants ¹⁸⁸. Elles permettent aux consommateurs de faire des achats plus rapidement et de limiter leur temps d'attente à la caisse (et donc leur risque de partir avant d'avoir fait leur transaction). Elles permettent aux commerçants, de réduire leur inventaire, d'offrir des services adaptés aux besoins de leur clientèle, de mieux connaître les habitudes d'achat de celle-ci, qu'elles contribuent d'ailleurs à fidéliser. ¹⁸⁹ Tout cela leur procure des bénéfices économiques.

¹⁸⁴ *Ibid.*

¹⁸⁵ CPVP, « La transformation du système de paiements canadiens: pourquoi la protection de la vie privée est essentielle à la confiance à l'égard du système de paiements et son innovation », Mémoire du Commissariat non destinés au Parlement concernant des enjeux liés à la protection de la vie privée, page 6

¹⁸⁶ FTC Staff Report, « Paper, Plastic...or Mobile? », An FTC Workshop on Mobile Payments, March 2013, page 15

¹⁸⁷ CPVP, « Sondage auprès des Canadiens sur la protection de la vie privée », décembre 2014 et Entrevue avec le CPVP

¹⁸⁸ Ce n'est pas le cas pour les portefeuilles électroniques. Ces derniers procurent également des bénéfices, mais certains fonctionnent selon un autre modèle d'affaires.

¹⁸⁹ FTC Staff Report, « Paper, Plastic...or Mobile? », An FTC Workshop on Mobile Payments, March 2013, page 14

Le profilage à des fins commerciales et la publicité ciblée sont des techniques de marketing qui visent à recueillir des informations sur le consommateur pour pouvoir lui offrir des publicités susceptibles de l'intéresser. Le profilage se fait par la collecte des données générées au fil de visites du consommateur sur un site donné ainsi que par l'observation de son comportement sur Internet¹⁹⁰. Dans le profil d'une consommatrice, on pourrait notamment trouver les informations suivantes : femme dans la vingtaine, habite au centre-ville d'une grande ville, est propriétaire d'un chien et est adepte de jogging. Cette femme pourrait recevoir de la publicité d'une entreprise vendant des laisse conçues pour permettre de faire du jogging avec un chien.

Il existe plusieurs formes de publicité en ligne. Il y a la publicité contextuelle affichée en fonction des pages où se trouve le consommateur. Par exemple, une consommatrice est sur le site d'un magazine de mode féminine, elle pourrait y voir une publicité de sac à main. Il y a la publicité sociodémographique qui cible les consommateurs en fonction de leur âge, leur sexe ou tout autre critère démographique. La publicité peut aussi être géo localisée, elle va s'adapter en fonction du lieu où se trouve le consommateur¹⁹¹.

Les téléphones intelligents peuvent aussi révéler de l'information précise sur la location en temps réel du consommateur (géolocalisation). Et cette information peut elle aussi être utilisée à des fins de marketing. Dans ce contexte, elle permet « de révéler les habitudes et les tendances du consommateur, qui font la distinction entre une journée dans la vie et le mode de vie »¹⁹². Selon l'ACFC, les APMPV procurent de nombreux avantages aux annonceurs. L'un d'eux est de leur permettre de cibler un consommateur au moment où il s'apprête à faire un paiement¹⁹³. Ceci pourrait avoir un impact important sur son choix. Par exemple, un consommateur qui achète souvent des lattés et qui préfère se procurer des produits biologiques pourrait recevoir de la publicité ciblée d'un café qui offre des lattés biologiques et qui est situé à deux pas de son bureau.

Le CPVP a établi des lignes directrices sur la protection de la vie privée et de la publicité comportementale en ligne (PCL). Il énonce que la PCL, qui peut aider à financer des services gratuits, peut être considéré comme une activité raisonnable en vertu de la LPRPDE, pourvu qu'elle suive certains paramètres, et qu'elle ne soit pas une « condition de service généralisée » pour accéder à Internet. Le consommateur doit consentir à la PCL. Les pratiques de collecte, d'utilisation et de communication des renseignements doivent être transparentes. Le CPVP dit que la forme peut varier, c'est-à-dire qu'elle doit être explicite lorsque les renseignements sont sensibles mais qu'elle peut être implicite lorsqu'ils ne le sont pas. Le consentement implicite à la PCL peut être jugé acceptable si les consommateurs sont avisés des objectifs de la PCL de façon claire et compréhensible et si les objectifs sont manifestes.

¹⁹⁰ http://www.cai.gouv.qc.ca/documents/CAI_FI_profilage.pdf

¹⁹¹ PLOURDE Alexandre, « *Le Prix de la gratuité : Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne* », rapport de recherche d'Option consommateurs, présenté à Recherche, Innovation et Développement Économique Canada, Juin 2015

¹⁹² Traduction Libre « reveal the habits and patterns that mark the distinction between a day in the life and a way of life » *United States v. Maynard*, 615 F. 3d 544, 562 (D.C. Cir. 2010) et FTC Staff Report

¹⁹³ GIBNEY Charles et als. ACFC, « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, Janvier 2015, page 15 et FTC Staff Report, « Paper, Plastic...or Mobile? », An FTC Workshop on Mobile Payments, March 2013, page 15

Autre chose : les politiques de confidentialité ne doivent pas être difficiles à trouver. Les organisations doivent être transparentes et informer efficacement les consommateurs de l'existence de ces politiques et de leur contenu. Cela doit se faire au plus tard au moment de la collecte. De plus, la PCL est raisonnable si les consommateurs peuvent facilement renoncer à la pratique. Cette renonciation est durable et immédiate. Les renseignements demandés ne doivent pas être des renseignements sensibles. Ils doivent être détruits dans les plus brefs délais après leur utilisation. Une personne peut refuser le suivi et le ciblage. Ce dernier ne doit pas être une condition pour accéder à Internet¹⁹⁴. À noter, les lignes directrices ont été rédigées dans un contexte d'utilisation de sites web. La PCL peut aider à financer la gratuité des services¹⁹⁵.

La publicité ciblée est perçue positivement par certains. Selon un sondage de Pew, 28 % des consommateurs sont d'accord pour recevoir de la publicité ciblée puisqu'elle cerne leurs intérêts alors que 68 % des consommateurs n'aiment pas en recevoir et n'aiment pas le suivi en ligne¹⁹⁶. Une autre étude, rapporte que la moitié des consommateurs ne veulent pas partager des renseignements personnels pour des fins de PCL alors que l'autre moitié est prête à partager certains renseignements (âge, numéro, numéro de l'appareil, « location générale (peu précise) », historique des sites web visités, etc.)¹⁹⁷. En 2015, Option consommateurs a étudié les politiques de confidentialité de site web offrant des services « gratuits ». Dans cette étude, l'organisme révèle que, contrairement à ce que laissent entendre certaines des politiques de confidentialité analysées, les renseignements recueillis sur les internautes dans le cadre de la PCL sont généralement considérés comme des renseignements personnels au sens de la LPRPDE. De plus, malgré l'obligation de ne recueillir que les renseignements nécessaires aux fins énoncés par l'entreprise, on collecte un nombre presque illimité de renseignements personnels. Aussi, au lieu d'utiliser une définition contextuelle des renseignements sensibles tels que prévu dans la LPRPDE, des entreprises déterminent elles-mêmes ce qu'est un renseignement sensible; l'interprétation varie donc d'une entreprise à l'autre¹⁹⁸.

3.7. La protection intégrée de la vie privée¹⁹⁹ (Privacy by design)

Le concept de la protection des renseignements personnels a évolué au fil des ans. Dans les années 1970 et 1980, on énonce les principes généraux de protection de la vie privée et cela

¹⁹⁴ CPVP, « Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne », décembre 2015

¹⁹⁵ CPVP, « Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne », décembre 2015

¹⁹⁶ <http://www.pewinternet.org/2012/03/09/main-findings-11/#targeted-advertising-59-of-internet-users-have-noticed-it-but-most-dont-like-it>

¹⁹⁷ PLOURDE Alexandre, « *Le Prix de la gratuité : Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne* », rapport de recherche d'Option consommateurs, présenté à Recherche, Innovation et Développement Économique Canada, Juin 2015

¹⁹⁸ PLOURDE Alexandre, « *Le Prix de la gratuité : Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne* », rapport de recherche d'Option consommateurs, présenté à Recherche, Innovation et Développement Économique Canada, Juin 2015

¹⁹⁹ Traduction du Dr. Ann Cavoukian. L'Union européenne utilise l'expression protection de la vie privée dès la conception pour définir la Privacy by Design.

coïncide avec la prise en compte d'un régime général de protection²⁰⁰. Puis dans les années 1990, notamment avec la Directive 95/46/EC, on met en place des contrôles pour assurer le respect de la vie privée²⁰¹. Plus tard, on axe sur la prévention; c'est là qu'apparaît la protection intégrée de la vie privée. Cela se fait principalement par la réglementation de l'outil technique. Ces mesures assurent le respect des règles de droit dès le stade de la conception, avant même toute atteinte éventuelle et potentielle. « Les entreprises sont intégrées aux processus, cela mène à une idée de responsabilité par la flexibilité »²⁰². La protection intégrée de la vie privée vise à changer les règles en favorisant la «la lumière à l'obscurité»²⁰³.

La protection intégrée de la vie privée comme on la connaît aujourd'hui est un concept développé dans les années 1990 par Ann Cavoukian, alors Commissaire à l'information et à la protection de la vie privée de l'Ontario. Mais, ce n'est «qu'en 2010, lors de la 32^e conférence internationale des commissaires à la protection des données et de la vie privée que son concept est adopté par résolution ».

La protection intégrée de la vie privée est fondée sur sept principes. Premier principe : la protection intégrée de la vie privée est proactive et non réactive. Elle anticipe et prévient les atteintes à la vie privée avant qu'elles ne surviennent²⁰⁴. Deuxième principe : la vie privée fait partie des paramètres initiaux (default mode). Le but est de s'assurer du plus haut niveau de protection. Le consommateur n'a pas à faire quoi que ce soit, la protection est intégrée au système par défaut²⁰⁵. Troisième principe : la fonction de base de l'équipement est le respect de la vie privée. Quatrième principe : la pleine fonctionnalité, c'est-à-dire que toutes les parties y trouvent leur compte. Il n'est plus nécessaire pour les consommateurs de faire des compromis en matière de vie privée (*privacy tradeoff*)²⁰⁶. Cinquième principe : la sécurité absolue toute au long du cycle de vie des renseignements personnels, de la collecte jusqu'à la destruction. Sixième principe : la visibilité et la transparence. Tous les acteurs impliqués dans la collecte des données doivent respecter les règles auxquelles ils ont souscrit. On s'assure d'ailleurs que ces règles sont respectées, et ce, à toutes les étapes et par toutes les parties. « Faites confiance, mais vérifiez » (*Trust but verify*).²⁰⁷ Septième principe : respect de la visibilité du consommateur. Avant tout, la protection intégrée de la vie privée est fondée sur l'importance, pour les concepteurs et les opérateurs, de respecter les intérêts des utilisateurs. Cela se fait dans la

²⁰⁰ MOUCHARD Émilie, « La protection de la vie privée dès la conception ou l'intégration de la Privacy by Design comme mécanisme du régime général sur la protection des données en droit Européen », Lex Electronica. Vol. 18, No 2, 2013, page 4

²⁰¹ MOUCHARD Émilie, « La protection de la vie privée dès la conception ou l'intégration de la Privacy by Design comme mécanisme du régime général sur la protection des données en droit Européen », Lex Electronica. Vol. 18, No 2, 2013, page 6 ceci inclut la Directive 95 en Union européenne et la LPRPDE au Canada.

^{202 202} MOUCHARD Émilie, « La protection de la vie privée dès la conception ou l'intégration de la Privacy by Design comme mécanisme du régime général sur la protection des données en droit Européen », Lex Electronica. Vol. 18, No 2, 2013, page 10

²⁰³ MOUCHARD Émilie, « La protection de la vie privée dès la conception ou l'intégration de la Privacy by Design comme mécanisme du régime général sur la protection des données en droit Européen », Lex Electronica. Vol. 18, No 2, 2013, page 13. L'auteur fait référence au principe de Kerckhoffs en cryptographie qui selon lui la sécurité d'un cryptosystème doit résider dans le secret de la clé. Ici, va favoriser la lumière toujours en gardant la clé secrète, mais tous les autres paramètres vont être connus.

²⁰⁴ CAVOUKIAN Ann « Privacy by Design : The 7 Foundational Principles », Information and Privacy Commissioner of Ontario, 2011

²⁰⁵ *Ibid.*

²⁰⁶ *Ibid.*

²⁰⁷ *Ibid.* et CAVOUKIAN Ann, *supra* note 204

gestion des paramètres de défaut (qui respectent la vie privée), des politiques de confidentialité (qui sont appropriées au contexte) et de l'autonomisation des utilisateurs (auxquels on procure des options conviviales)²⁰⁸.

3.8. Les renseignements des consommateurs stockés aux États-Unis

En raison du contexte économique, un grand nombre des entreprises qui offrent des APMPV ou des portefeuilles électroniques sont des entreprises américaines. De plus, certaines entreprises d'ici stockent leurs renseignements personnels dans d'autres pays, notamment les États-Unis. En raison de l'obligation de transparence prévue dans la LPRPDE, les entreprises doivent indiquer dans leur politique de confidentialité que les renseignements personnels des consommateurs peuvent être stockés dans d'autres pays et être soumis aux juridictions de ces pays. Les entreprises doivent s'assurer que les renseignements personnels des consommateurs seront bien protégés.

Le problème, c'est que les lois américaines en matière de droit privé sont beaucoup plus faibles que la LPRPDE. De plus, les États-Unis n'ont pas de lois uniformes applicables à toutes les entreprises; elles ont plutôt différentes législations selon les secteurs d'activités²⁰⁹. Les renseignements personnels des Canadiens pourraient ne pas être aussi bien protégés aux États-Unis qu'au Canada. D'une part, les données des consommateurs canadiens n'ont pas les mêmes protections constitutionnelles aux États-Unis qu'au Canada. D'autre part, en vertu du droit américain, les données des consommateurs canadiens sont moins bien protégées que les données des consommateurs américains, notamment en matière d'accès par des tiers²¹⁰. Par ailleurs, depuis l'arrêt Microsoft, le gouvernement peut avoir accès aux données des consommateurs de partout dans le monde lorsqu'elles sont détenues par une entreprise américaine, et ce, même si ces données ne sont pas situées aux États-Unis.²¹¹

3.9. Portrait du droit étranger

À l'étranger, la collecte, l'utilisation et la communication des renseignements personnels des consommateurs utilisant une application de paiement mobile sont également des enjeux importants. Les États-Unis et l'Union européenne ont choisi de les encadrer de façon différente : l'UE protège les consommateurs de manière uniforme alors que les États-Unis ont différentes législations selon les secteurs d'activités.

²⁰⁸ Ibid.

²⁰⁹ BOHACKER Heidi, « Seeing through the Cloud : National Jurisdiction and Location of Data, Servers and Networks Still Matter in a Digitally Connected World », rapport de recherche financé par le programme de contribution, CPVP, 2015 et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, Janvier 2015, page 15

²¹⁰ BOHACKER Heidi, « Seeing through the Cloud : National Jurisdiction and Location of Data, Servers and Networks Still Matter in a Digitally Connected World », rapport de recherche financé par le programme de contribution, CPVP, 2015

²¹¹ In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation

3.9.1. Les États-Unis

Le droit américain reconnaît la protection de la vie privée au sens de l'identité individuelle. Ce droit fondamental protège contre les intrusions du gouvernement ou des entreprises. Les États-Unis n'ont pas de loi uniforme encadrant les entreprises en matière de protection des renseignements personnels. Plutôt, les lois diffèrent en fonction de l'intervenant, de l'industrie, du type de données et de la manière dont les renseignements sont entreposés²¹².

Aux États-Unis, il y a plusieurs organismes chargés de s'assurer du respect de la vie privée des consommateurs. Au plan fédéral, c'est la Federal Trade Commission (FTC) qui encadre bon nombre d'acteurs, notamment les fabricants de matériel, les annonceurs, les gestionnaires de données et les concepteurs d'applications. Elle a compétence, notamment, pour les protéger contre la fraude, les pratiques déloyales et les atteintes à la vie privée. Par contre, selon l'Agence de la consommation en matière financière du Canada (ACFC), elle ne semble pas avoir compétence à l'égard de la facturation directe par l'entreprise²¹³.

La Federal Communications Commission (FCC) encadre l'utilisation des services à large bande. Alors que le Consumer Financial Protection Bureau (CFPB) s'assure que les directives, les règlements et les lois sous sa compétence sont respectés par les entreprises qui fournissent des services financiers. Le champ de compétence de la CFPB inclut les paiements mobiles²¹⁴.

La FTC a la compétence pour surveiller l'application de plusieurs lois fédérales protégeant la protection de la vie privée : la Children Online Privacy Protection Act (COPPA), qui prévoit des normes minimales lors de la collecte de données d'enfants de moins de 13 ans²¹⁵ et la Gramm-Leach-Bliley Act Financial Service Modernization Act of 1999 (Gramm-Leach-Bliley Act)²¹⁶, qui s'applique aux institutions financières et impose des restrictions en matière de collecte d'information, notamment l'obligation de divulguer chaque année à ses clients les informations liées à sa politique de confidentialité. À noter, en 2016, un amendement à la Gramm-Leach-Bliley Act a eu pour effet, dans certaines circonstances, de dispenser une institution financière de l'obligation d'envoyer un avis annuel aux consommateurs²¹⁷.

Les institutions financières doivent divulguer leurs pratiques et politiques concernant le partage de renseignements personnels à des parties (liées ou non). De plus, elles doivent divulguer leur pratique concernant les renseignements non publics²¹⁸. Le consommateur doit avoir la possibilité de retirer son consentement et de ne pas participer aux activités de partage de

²¹² GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, Janvier 2015, page 17

²¹³ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, Janvier 2015, page 5

²¹⁴ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, Janvier 2015, page 6

²¹⁵ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 17

²¹⁶ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 17

²¹⁷ http://www.debevoise.com/~media/files/insights/publications/2016/01/20160106_changes_to_annual_privacy_notice_requirements.pdf

²¹⁸ Le terme non public est utilisé dans la législation américaine, plutôt que le terme renseignements personnels ou données personnelles.

renseignements non public avec des tiers²¹⁹. À noter, la FTC avait compétence pour faire des règlements en vertu du *Gramm-Leach-Bliley Act Financial Service Modernization Act of 1999*, mais la *Loi Dodd-Frank*²²⁰ a transféré certain de ses pouvoirs au CFPB.

Selon l'ACFC, les données recueillies par des agences de crédit sur les antécédents des consommateurs doivent respecter la *Fair Credit Reporting Act* (FCRA) et la *Fair and Accurate Credit Transaction Act* (FACTA). La surveillance de l'application de ces lois est soumise à la FTC. Par ailleurs, la collecte de renseignements personnels liés à la santé est assujettie à la *Health Insurance Portability Accountability Act* (HIPPA)²²¹. Il n'y a pas de loi encadrant la publicité ciblée en ligne. La FTC a élaboré les *Self-Regulatory Principle for Online Behavioural Advertizing*. Ces principes sont repris *grosso modo* dans de nombreux instruments d'autoréglementation créés par des regroupements d'entreprises, notamment les *Self-Regulatory Principles for Online Behavioral Advertizing* de la *Digital Advertizing Alliance* et le *Code of Conduct* du *Network Advertising Initiative*²²².

En ce qui a trait aux applications mobiles

La FTC a été très active dans le dossier des applications mobiles²²³, notamment des APMPV. Elle s'inquiète de la grande quantité de renseignements personnels pouvant être recueillis par ces applications. Dans un rapport, elle recommande des mesures afin d'instaurer la confiance des consommateurs et de favoriser la transparence. La FTC recommande de faire la divulgation en temps opportun, de présenter l'information sous forme multi strates et d'utiliser des pictogrammes. Elle dit également que le concepteur d'applications devrait limiter la collecte de renseignements sensible²²⁴.

Dans un rapport intitulé « *Paper, Plastic...or Mobile? An FTC Workshop on Mobile Payments* », la FTC énonce que les applications de paiements mobiles peuvent recueillir beaucoup de renseignements personnels et que les téléphones intelligents posent des défis particuliers en matière de divulgation des politiques de confidentialité. Elle formule trois recommandations : que les entreprises s'intéressent aux enjeux de vie privée et en tiennent compte au stade du développement (protection intégrée de la vie privée) (voir section 3.7), que les choix des consommateurs et des entreprises soient simplifiés, que la transparence soit favorisée²²⁵.

Chez nos voisins du Sud, les états ont aussi compétence pour régler la protection de la vie privée. Quarante-six états exigent que les consommateurs soient avisés lorsque leurs

²¹⁹ BUDNITZ Mark E., « The Legal Framework of Mobile Payments: Gaps, ambiguities and Overlap », February 10, 2016

²²⁰ La loi Dodd-Frank a été adoptée par l'administration Obama suite à la crise financière. Le nom complet de cette loi est la « An Act to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end "too big to fail", to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes ».

²²¹ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 18

²²² PLOURDE Alexandre, « *Le Prix de la gratuité : Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne* », rapport de recherche d'Option consommateurs, présenté à Recherche, Innovation et Développement Économique Canada, Juin 2015

²²³ FTC, « What's the deal: AN FTC Study on Mobile Shopping Apps », August 2014

²²⁴ FTC Staff Report, « Mobile Privacy Disclosures: Building Trust Through Transparency », February 2013

²²⁵ FTC Staff Report, « Paper, Plastic...or Mobile? An FTC Workshop on Mobile Payments » March 2013, page 14

renseignements personnels peuvent être divulgués à des tiers²²⁶. La Californie est particulièrement active en matière de vie privée. Elle a été le premier état à adopter une loi pour protéger la vie privée de ses habitants. Le champ d'application de la *California Online Privacy Protection Act* est large et étendu. Cette loi s'applique à toute entreprise américaine qui recueille des renseignements personnels identifiables de Californiens. Elle oblige l'utilisation de politique de confidentialité et définit les renseignements personnels identifiables de façon plus large que d'autres législations américaines. La Californie est également active en matière d'applications mobiles. Elle a aussi une déclaration de principes visant à s'assurer que les applications de paiements mobiles respectent sa loi, notamment que la politique de confidentialité est visible et apparente. De plus, la politique sera disponible dans le magasin d'application comme Google Play ou AppStore. Toutes les entreprises fournissant des magasins d'applications ont intégré ces principes²²⁷.

Dans un rapport, la Procureure générale de la Californie énonce des recommandations afin de faciliter l'accessibilité des politiques de confidentialité sur support mobile, de les rendre plus faciles à comprendre et de favoriser la transparence en impliquant un plus grand nombre de joueurs, notamment des entreprises facilitant le téléchargement des applications, notamment Google et Apple²²⁸. De plus, la Californie a modifié ses lois de transfert d'argent pour inclure les paiements mobiles²²⁹.

La Californie a aussi adopté la *Song-Beverly Credit Card Act*, qui interdit aux commerçants la cueillette de renseignements personnels liés aux cartes de crédit. Le but de cette loi est de protéger la vie privée des consommateurs qui paient par carte de crédit en empêchant les commerçants de recueillir des renseignements qui ne sont pas nécessaires pour la transaction²³⁰. Certains auteurs suggèrent qu'une façon de mieux protéger les consommateurs en matière de paiements mobiles serait d'amender la Song-Beverly Act pour ajouter les PMPV dans son champ d'application²³¹.

3.9.2. L'Union européenne

La protection de la vie privée est très importante pour les Européens. Dès 1950, le Conseil de l'Europe reconnaît le droit à la vie privée²³². En 1981, la Convention 108 est adoptée. Il s'agit d'un traité international sur la protection des données. Le but de cette convention est de garantir des droits fondamentaux, ce qui inclut la vie privée eu égard au traitement des données à caractère personnel, et ce, tant dans le secteur privé que dans le secteur public²³³.

²²⁶ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 18

²²⁷ HARRIS Kamala D., Attorney General, « Privacy on the GO: Recommendations for the Mobile Ecosystem », January 2013

²²⁸ HARRIS Kamala D., Attorney General, « Privacy on the GO: Recommendations for the Mobile Ecosystem », January 2013

²²⁹ BUDNITZ Mark E., « The Legal Framework of Mobile Payments: Gaps, ambiguities and Overlap », February 10, 2016

²²⁹ GIBNEY Charles., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 34

²³⁰ HOOFNAGLE Chris Jay et als., « Mobile Payments: Consumer Benefits & New Privacy Concerns », Berkeley Center for Law and Technology, April 2012, page 14-16

²³¹ *Ibid.*

²³² CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 114

²³³ CHASSIGNEUX Cynthia, « Vie privée et commerce électronique », Les Éditions Thémis, Montréal, 2005, page 115

Dans les années 1970, l'Union européenne a commencé à s'intéresser à la protection des données personnelles²³⁴. Elle a alors adopté la Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après Directive 95/46/EC).

La Directive est constituée de huit principes. Le premier est le principe directeur. Il a préséance sur les autres. « Il englobe les notions de respect et de loi et de loyauté. Le terme respect de la loi est assez explicite, mais le terme loyauté signifie que les organisations qui recueillent, traitent et contrôlent les données personnelles doivent tenir compte de l'intérêt de la personne dont les renseignements sont recueillis »²³⁵.

Le second principe est celui du respect des finalités. Les données ne peuvent être recueillies que pour des fins légitimes. La raison de la collecte doit être divulguée et elle doit être explicite. « Les données ne peuvent être utilisées que pour les fins de la collecte »²³⁶.

Le troisième principe est celui de la juste mesure et de la proportionnalité. « Les données recueillies doivent être limitées pour atteindre le but pour lesquelles elles ont été recueillies »²³⁷.

Le quatrième principe est celui de la qualité de l'information. « Les données recueillies doivent être exactes, à jour et valables à ce qu'elles sont censées représenter »²³⁸.

Le cinquième principe est lié au droit de contrôle et de participation de la personne dont les données sont recueillies. Il y existe l'obligation d'informer cette personne et d'obtenir son consentement éclairé quant à la collecte et au traitement de ses données²³⁹.

Le sixième principe indique « que la divulgation des données ne peut être faite que selon des circonstances précises et qu'il faut le consentement éclairé de la personne avant la divulgation des tiers »²⁴⁰.

Le septième principe exige que les gestionnaires de données prennent toutes les mesures nécessaires pour assurer la sécurité des données recueillies²⁴¹.

²³⁴ Ibid.

²³⁵ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 26

²³⁶ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²³⁷ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²³⁸ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²³⁹ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²⁴⁰ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²⁴¹ Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

Le huitième principe concerne le caractère délicat ou sensible des données recueillies, de façon à prendre des mesures adaptées aux caractéristiques de ces données²⁴²

En raison des avancées de la technologie et des dérives potentielles pouvant affecter la vie privée des consommateurs²⁴³, l'Union européenne a par la suite adopté la *Directive 2002/58/CE du Parlement européen et du conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques* (Directive 2002). « La Directive 2002 vise principalement les exploitants de réseaux mobiles et les fournisseurs d'accès Internet ». Ceux-ci doivent se conformer aux principes qui se trouvent dans la directive. Cette dernière oblige les annonceurs à avoir le consentement des consommateurs avant de leur envoyer de la publicité non sollicitée sur leur téléphone intelligent. De plus, elle définit ce qu'elle considère comme étant une information permettant l'identification d'une personne; les données liées à l'activité du mobile, l'historique de navigation des sites web et la géolocalisation en font partie. Pour pouvoir être utilisées, ces données doivent être dépersonnalisées. Il faut également que le consentement libre et éclairé du consommateur ait été obtenu. Les consommateurs peuvent refuser les logiciels permettant les suivis²⁴⁴.

Les deux directives offrent une protection uniforme aux consommateurs européens. Ces directives offrent des protections larges et étendues comme la LPRPDE. Cependant, on semble y demander un consentement légèrement plus explicite que ce qui est prévu dans la LPRPDE, particulièrement en matière de divulgation à des tiers²⁴⁵.

En 2010, la Commission européenne a présenté sa stratégie visant à renforcer la protection des données. En 1995, seulement 1 % des Européens utilisaient Internet alors qu'à l'heure actuelle, un nombre astronomique de données est échangé d'un continent à l'autre en quelques fractions de seconde. La Commission cherche à protéger les données à caractère personnel. En janvier 2012, la Commission européenne propose de modifier la Directive 95 de façon à renforcer la vie privée dans un contexte d'économie numérique. Il y aura également une mise à jour unique pour que les pays membres intègrent la Directive dans leurs droits nationaux²⁴⁶. Les modifications incluent un corpus unique de règles, qui permettent d'accroître la responsabilité de ceux qui gèrent les données, prévoient des nouvelles obligations en matière de consentement ainsi que l'obligation de dénoncer toute violation grave aux données personnelles dans les 24 heures, facilitent l'accès des personnes à leurs propres données. De plus, le pouvoir des autorités nationales sera renforcé et ce, eu égard au traitement de données. Qui plus est, la nouvelle directive prévoit que la protection des données sera intégrée aux biens dès sa conception (protection intégrée de la vie privée)²⁴⁷. Les textes de la réforme ont été entérinés en décembre 2015; la Directive devrait entrer en vigueur en 2018²⁴⁸.

²⁴² Directive 95/46/EC et GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²⁴³ CHASSIGNEUX Cynthia, « *Vie privée et commerce électronique* », Les Éditions Thémis, Montréal, 2005, page 118

²⁴⁴ GIBNEY Charles et als., « *Les paiements mobiles et la protection des consommateurs : Examen de la situation à l'échelle internationale* », ACFC, janvier 2015, page 27

²⁴⁵ Article 29 Data Protection Working Party, « *Opinion 15/2001 on the definition of consent* », adopted on July 13 2011

²⁴⁶ http://europa.eu/rapid/press-release_IP-15-6321_fr.htm

²⁴⁷ http://europa.eu/rapid/press-release_IP-15-6321_fr.htm

²⁴⁸ <http://www.consilium.europa.eu/fr/press/press-releases/2015/12/18-data-protection/>

Section 4. Analyse des politiques de confidentialité des applications de paiements mobiles

Dans le cadre de cette étude, nous cherchions à déterminer quels sont les renseignements personnels recueillis par les applications de paiements mobiles. Nous voulions également déterminer comment les consommateurs sont informés de la collecte, de l'utilisation et de la communication de leurs renseignements personnels. Pour ce faire, nous avons analysé les politiques de confidentialité des applications de paiements mobiles de notre échantillonnage. Pour constituer ce dernier, nous avons sélectionné les APMPV pouvant être téléchargées par les consommateurs canadiens et être utilisées à Montréal. Ces politiques présentent non seulement l'obligation de divulgation du commerçant envers les consommateurs, mais également ce que le commerçant peut faire avec les renseignements personnels du consommateur, une fois son consentement obtenu.

Pour les fins de notre étude, nous avons choisi d'utiliser la définition des paiements mobiles de l'Organisation de coopération et de développement économique (OCDE) (voir section 2)²⁴⁹. Nous utilisons aussi la définition des PMPV de Dolcourt, tel que rapportée par Carlisle Adams (voir section 2)²⁵⁰. Dans notre échantillonnage, nous avons des APMPV émises par des commerçants et des institutions financières (banque²⁵¹ et coopérative de crédit²⁵²) ainsi que des portefeuilles électroniques qui ne sont pas émis par des institutions financières traditionnelles. Nous avons aussi des applications de commerce de détail qui permettent de faire des achats en magasin, en scannant l'article puis en le payant; le bien est livré subséquemment au consommateur. Ces applications soulèvent des enjeux similaires aux APMPV en matière de vie privée.

Dans notre échantillon, nous avons choisi 30 applications offertes aux consommateurs canadiens et pouvant être utilisées en magasin, à Montréal – c'est là que nous avons réalisé notre enquête sur le terrain. Nous avons téléchargé et utilisé ces applications en 2016, de la première semaine de janvier à la première semaine de mars.

Nous nous sommes procuré deux téléphones intelligents (un Android²⁵³ et un iPhone²⁵⁴) pour télécharger les APMPV et les utiliser. Selon un sondage de 2014, 40 % des Québécois ont un Android alors que 39 % d'entre eux ont un iPhone²⁵⁵. Nous avons utilisé l'Android sur le réseau sans fil de Fido et le iPhone sur le réseau de Bell. Le modèle de téléphone est important, puisque ce ne sont pas tous les téléphones intelligents qui peuvent avoir accès aux APMPV. Le réseau sans fil est également important puisque certaines applications ne sont pas offertes aux clients

²⁴⁹ L'OCDE définit les paiements mobiles comme des paiements pour lesquels les données et l'ordre de paiement sont transmis *via* un téléphone mobile ou un autre équipement mobile. Les paiements mobiles peuvent être faits à distance ou en personne (au point de vente)

²⁵⁰ ADAMS Carlisle « Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles », rapport de recherche présenté au Commissariat à la protection de la vie privée du Canada, juin 2013, page 10 et DOLCOURT.

²⁵¹ Tel que défini à l'Art 2 de la Loi sur les banques

²⁵² Tel que défini par la Loi

²⁵³ Il s'agissait d'un Samsung Galaxy 3.

²⁵⁴ Il s'agissait d'un iPhone 6.

²⁵⁵ http://www.cefrio.qc.ca/media/uploader/Fascicule-Mobilit_Versionfinale.pdf

de certains réseaux; par exemple les clients de Vidéotron et de Fido n'ont pas accès à l'application de Desjardins. Nous avons testé ces deux téléphones pour utiliser les APMPV émises par les commerçants (à la caisse ou non) ainsi que les portefeuilles électroniques.

Pour utiliser les APMPV émises par les institutions financières, nous avons recruté des testeurs²⁵⁶ pouvant utiliser leur propre téléphone²⁵⁷ – comme il s'agissait d'opérations bancaires, cela nous semblait plus prudent. Les testeurs devaient avoir un téléphone intelligent compatible avec ces APMPV ainsi que les outils nécessaires pour effectuer les transactions (par exemple, une carte de crédit et un compte auprès de l'institution financière d'où provenait l'application). Ils devaient aussi savoir comment utiliser les APMPV.

D'emblée, nous avons remarqué que certaines APMPV sont bien plus présentes que d'autres sur le marché. C'est le cas de l'application Starbucks, qui accepte la très grande majorité des portefeuilles électroniques. Mentionnons que, malgré sa popularité, ApplePay, qui est arrivé au Canada en novembre 2015, n'est accessible que par les détenteurs d'une carte American Express; lors de notre étude, sa présence sur le marché canadien était donc limitée²⁵⁸.

4.1. Notre échantillonnage

Dans le cadre de cette étude, nous avons utilisé 30 APMPV. Ce faisant, nous avons téléchargé les politiques de confidentialité et nous les avons étudiées. Les applications faisant partie de notre échantillonnage sont énumérées dans les tableaux 1 et 2 (voir page suivante).

Une fois notre échantillonnage sélectionné, nous avons téléchargé les applications, nous avons créé un compte d'utilisateur et nous les avons utilisées. Ce faisant, nous avons noté à quel moment la politique de confidentialité était accessible aux consommateurs. Nous avons ainsi pu constater que, dans la grande majorité des cas, la politique de confidentialité s'affiche à l'étape de la création du compte. Elle se trouve tantôt dans les modalités de l'entente, tantôt dans un document à part.

À noter, avec notre téléphone Android, nous téléchargeons des APMPV dans Google Play avant de télécharger les applications, un message pop-up apparaissait; on y trouvait la liste des données du téléphone intelligent auxquelles l'application aurait accès une fois téléchargée. La liste, qui n'était pas toujours la même, contenait souvent l'identifiant de l'appareil, la géolocalisation, les fichiers enregistrés sur l'appareil et l'historique de navigation. Ces informations étaient présentées sous forme multi strates, ce qui permet au consommateur de cliquer sur chaque élément de la liste pour obtenir plus d'information.

²⁵⁶ C'est ainsi que nous avons choisi de nommer les personnes qui, pour les fins de cette recherche, ont utilisé les applications faisant partie de notre échantillonnage.

²⁵⁷ Puisque toutes les applications financières sauf celle de la RBC étaient offertes uniquement aux utilisateurs d'Android, nos testeurs avaient un téléphone Android.

²⁵⁸ Après la rédaction de ce rapport, mais avant de le mettre sous presse, le 10 mai 2016, RBC et CIBC ont conclu une entente avec ApplePay. Les consommateurs pourront utiliser une carte de débit ou de crédit émise par ces institutions bancaires pour payer leurs achats avec ApplePay. http://business.financialpost.com/fp-tech-desk/canadian-banks-including-the-big-five-sign-on-for-major-apple-pay-expansion?_lsa=6ce6-4a6a

Tableau 1 – Applications offertes aux utilisateurs d’Android (28 applications ont été analysées²⁵⁹)

APMPV émises par des commerçants	APMPV ou portefeuilles émis par une institution financière	Portefeuilles électroniques émis par des entreprises	Applications permettant PM sans passer à la caisse	Application de stationnement
Starbucks	TD	Ugo	American Eagle Outfitters	Stationnement Montréal
Second Cup	RBC	Suretap	Canadian Tire	Copilote
Tim Hortons	Scotia	Stocard	Indigo	Secunik
	CIBC	Stocard	ToysRus	
	Desjardins	Fidme	Urban Outfitters	
		Mobile-Pocket	Apple Store	
		Beep’nGo	Zara	
		PayPal		
		PassWallet		
		Pass2UWallet		

Tableau 2 – Applications offertes aux utilisateurs d’iPhone (19 applications ont été analysées²⁶⁰)

APMPV émises par des commerçants	APMPV ou portefeuilles émis par une institution financière	Portefeuilles électroniques émis par des entreprises	Applications permettant PM sans passer à la caisse	Application de stationnement
Starbucks	RBC	ApplePay	American Eagle Outfitters	Stationnement Montréal
Second Cup		Ugo	Canadian Tire	Copilote
Tim Hortons		Stocard	Indigo	Secunik
		PayPal	ToysRus	
		Zoompass	Urban Outfitters	
			Apple Store ²⁶¹	
			Zara	

²⁵⁹ Les applications ont été téléchargées, utilisées et analysées de janvier 2016 à la première semaine de mars 2016.

²⁶⁰ Les applications ont été téléchargées, utilisées et analysées de janvier 2016 à la première semaine de mars 2016.

²⁶¹ Nous avons utilisé Apple Pay et Apple Store. Mais comme elles proviennent de la même entreprise, nous ne l’avons comptée qu’une seule fois.

4.2. Notre analyse

Par souci méthodologique, nous avons analysé séparément les clauses offertes aux utilisateurs d'Android et celles offertes aux utilisateurs d'iPhone, et ce, même lorsque la politique de confidentialité provenait de la même application. Nous n'avons pas remarqué de différences significatives quant aux contenus des politiques de confidentialité. En fait, la seule différence que nous avons remarquée est en lien avec le pop-up qui apparaissant avant le téléchargement d'une application de Google Play avec l'Android (avec l'iPhone, il n'y avait pas de pop-up).

Au total, nous avons analysé les politiques des confidentialités des 30 applications²⁶² de paiements mobiles. Cette analyse a révélé six lacunes importantes. Nous avons décelé les problèmes qui étaient les plus communs dans les politiques de confidentialité de notre échantillonnage. Nous présentons ci-bas la liste des lacunes que nous avons identifiées.

4.2.1. Première lacune : les politiques de confidentialité ne sont pas toujours facilement accessibles

Certaines des politiques de confidentialités nous ont semblé difficiles à trouver. Or, elles auraient dû être facilement accessibles. L'accessibilité se définit comme « le fait de pouvoir prendre connaissance de quelque chose sans obstacle »²⁶³. Le manque d'accessibilité peut nuire au lien de confiance entre le commerçant qui offre l'application et le consommateur qui l'utilise. Même si les consommateurs ne lisent pas tous les politiques de confidentialité, il est important que celles-ci soient accessibles en tout temps. Le consommateur doit pouvoir s'y référer sans difficulté.²⁶⁴

Afin de vérifier si les politiques de confidentialités sont accessibles, nos testeurs ont téléchargé les applications, puis ont créé des comptes d'utilisateurs. Ce faisant, ils cherchaient les clauses et les politiques de confidentialité. Leur comportement n'était pas celui d'un consommateur qui veut simplement utiliser une APMPV. Lorsque le testeur n'était pas capable de trouver la clause de confidentialité, une validation était effectuée par un autre testeur (« testeur de secours »). Notre analyse démontre que, dans la majorité des cas, les consommateurs peuvent trouver relativement facilement les politiques de confidentialités ou les informations pertinentes équivalentes. Toutefois, certaines politiques de confidentialité ne sont pas facilement accessibles.

Nous avons aussi remarqué que les politiques de confidentialité que nous cherchions n'étaient pas toujours au même endroit. Parfois, elles étaient insérées dans les termes et conditions de l'entente, ce qui les rendait difficiles à repérer. Par exemple, le portefeuille Fidme met à la disposition des consommateurs les termes et conditions de l'entente. À l'intérieur de ce document, on trouve des informations sur la confidentialité. Le hic? Ce document fait 34

²⁶² Ce chiffre ne tient pas compte d'Apple Pay, que nous avons utilisé, mais qui n'est pas une application.

²⁶³ CHASSIGNEUX Cynthia, « *Guide pour l'élaboration d'une politique de confidentialité* », Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008

²⁶⁴ CHASSIGNEUX Cynthia, « *Guide pour l'élaboration d'une politique de confidentialité* », Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008

pages²⁶⁵. Il contient des sous-titres et une table des matières, mais la police et le caractère utilisé ne les mettent pas en évidence.

Un autre exemple est l'application de Tim Hortons²⁶⁶. Les termes et conditions de l'entente sont apparents lors de la création du compte. Mais pour y trouver la politique de confidentialité, le consommateur doit se rendre dans la section sur les conditions de la carte Tim (le lien vers la politique de confidentialité s'y trouve). Le hic? Les termes et conditions de l'entente font 16 pages. De plus, même si le texte est en caractère 16 lorsqu'on imprime la clause, sur un téléphone intelligent, il n'est pas facile de le lire. Le lien vers la politique de confidentialité est donc difficile à trouver.

multiples documents

Certaines applications financières réfèrent à plusieurs documents qui, ensembles, permettent au consommateur d'avoir accès à toute l'information nécessaire concernant la protection de ses renseignements personnels. La politique de confidentialité de TD utilise une présentation sous forme multi strates, ce qui est bien. De plus, lorsque le consommateur accède à la politique de confidentialité, il est dirigé au bas du document, à la section Code de protection de la vie privée pour les applications mobiles. Cette section s'applique à l'application de la Banque TD. Par contre, pour obtenir toute l'information, le consommateur doit également lire le Code de la protection en ligne, cette section s'applique à tous les services en ligne. Cette section se trouve plus haut dans la politique de confidentialité.²⁶⁷

Lorsque le testeur a téléchargé l'application de portefeuille électronique de la Banque RBC, il a vu un document d'une page sur lequel est écrit, en caractères gras, le mot « Privacy »²⁶⁸. Sous cette en-tête, il est indiqué que l'application peut avoir accès à la liste des contacts (ils pourraient par exemple recevoir une carte prépayée pour leur anniversaire). Quiconque veut plus d'information clique sur un lien qui le mène vers la section FAQ portant sur les applications mobiles. Cette section offre de l'information générale concernant l'utilisation de l'application selon le type de téléphone et procure d'autres liens (l'un mène vers des indications au sujet de la manière désinstaller l'application, l'autre vers la politique de la RBC digital Channel Privacy²⁶⁹). Sur ce dernier document, on trouve des informations en matière de vie privée, notamment les types d'information recueillies. Dans la section sur la géolocalisation, on explique comment gérer les paramètres. Ceci est très bien. Le problème, c'est que ce document semble incomplet. La raison? Au bas, il est indiqué qu'il doit être lu avec les conditions d'utilisations (Legal Terms of use) du site web. Mais il n'y a pas de lien menant à ce document²⁷⁰. En allant sur le site web, nous trouvons plusieurs de documents, notamment les conditions d'utilisation du site web et

²⁶⁵ http://fidme.com/entry/terms_of_service?lang=fr

²⁶⁶ <https://www.timhortons.com/ca/fr/timcard/timcard-terms-conditions.php> et <http://www.timhortons.com/ca/fr/privacy.php>

²⁶⁷ <http://www.td.com/francais/confidentialite-et-securite/confidentialite-et-securite/nos-engagements-a-legard-de-la-confidentialite/code-de-protection-de-la-vie-privee-td/privacy.jsp>

²⁶⁸ A noter, ce n'est pas un problème que cette clause soit en anglais puisque le testeur était anglophone. Les informations sont adaptées à ses besoins puisque son téléphone est en anglais et ses services bancaires sont fait en anglais. Le premier document ne peut être joint en note en bas de page. Voici les liens :

<http://www.rbcroyalbank.com/mobile/app-faqs.html?q=81#q81> ET <http://www.rbc.com/privacysecurity/ca/online-privacy.html>

²⁶⁹ Notre testeur étant anglophone, ce nom est apparu en anglais.

²⁷⁰ <http://www.rbc.com/canada.html>

une politique de confidentialité. Pour trouver cette dernière, il a fallu faire plusieurs recherches par mots clés et effectuer plusieurs clics. Nous pouvons nous demander si cela peut nuire à l'accessibilité. Par contre, la politique est présentée sous forme multi strates, ce qui la rend facile à lire et à comprendre. De plus, les informations sont données de façon claire et concise.

La politique de confidentialité de Second Cup semble peu accessible. Lorsque le consommateur créé son compte, il a accès aux modalités de l'entente. Dans ce document, il y a une référence à la divulgation de renseignements personnels. Par contre, il n'y a pas de lien menant à cette politique²⁷¹. Il faut faire une recherche par mot clés en ligne pour y arriver.

4.2.2. Deuxième lacune : les politiques de confidentialité ne sont pas toujours adaptées à la réalité des mobiles.

En raison de leurs petits écrans, les téléphones intelligents comportent un défi particulier²⁷². Les commerçants doivent divulguer toutes les informations requises par la Loi, tout en s'assurant d'être bien compris par les consommateurs. Pour qu'une information soit comprise, elle doit d'abord être lue. Si le document est très long, il est possible que le consommateur se décourage et ne le lise pas.

Il est aussi important que les commerçants rédigent des politiques de confidentialité concises. La concision se définit comme étant « ce qui s'exprime pour un contenu donné, en peu de mots »²⁷³. Pour ce faire, le commerçant doit se demander quelles sont les informations nécessaires aux fins de la collecte.

Plusieurs commerçants utilisent la présentation sous forme multi strates (*Multi-layered privacy notices*). Il s'agit d'une façon de communiquer de l'information de façon concise. Il est préférable de ne pas divulguer les informations liées à la protection des renseignements personnels dans un texte au long : c'est d'ailleurs pour éviter cela que la présentation sous forme multi strates est utilisée²⁷⁴. Avec cette méthode, les informations importantes sont exposées les unes à la suite des autres dans un document court. Elles sont alors plus faciles à repérer pour le consommateur. La présentation sous forme multi-strates lui permet de cerner l'essentiel du sujet et de prendre des décisions éclairées²⁷⁵. Si le consommateur veut avoir de l'information plus détaillée, il peut toujours consulter une version longue de la politique de confidentialité.

Cette dernière doit contenir tous les éléments permettant aux commerçants de s'acquitter de leurs obligations eu égard aux lois relatives à la protection de la vie privée. Cette approche

²⁷¹ Il n'est pas possible d'ajouter un lien puisque l'utilisation de cette AMPV a été faite à l'externe. Le testeur nous a envoyé les informations par courriel.

²⁷² FTC Staff Report, « Mobile Privacy Disclosures: Building Trust Through Transparency », February 2013

²⁷³ CHASSIGNEUX Cynthia, « Guide pour l'élaboration d'une politique de confidentialité », Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008

²⁷⁴ CHASSIGNEUX Cynthia, « Guide pour l'élaboration d'une politique de confidentialité » Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008

²⁷⁵ CHASSIGNEUX Cynthia, « Guide pour l'élaboration d'une politique de confidentialité » Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008 et *Berlin Privacy Notices Memorandum*, 2004

favorise la compréhension des consommateurs et le respect des obligations des commerçants prévues à la Loi. Ceci permet de donner de l'information compréhensible et appropriée au médium utilisé, dans ce cas le téléphone intelligent²⁷⁶.

Le *Groupe de travail de l'article 29 sur la protection des données* énonce que les avis présentés sous forme multi strates peuvent contribuer à améliorer la qualité de l'information sur la protection des renseignements personnels en faisant ressortir l'information nécessaire, facilitent la compréhension des consommateurs et leur permettent de prendre une décision éclairée en toute connaissance de cause. Le support mobile crée un contexte d'espace limité, mais aussi de temps limité. Puisque les consommateurs utilisent leurs mobiles en tout temps et en tout lieu, ils n'ont pas nécessairement le temps de lire un long document. Dans ce contexte, la présentation sous forme multi strates peut améliorer la lisibilité des avis²⁷⁷. Elle est préconisée par l'Organisation de Coopération et de Développement Économique²⁷⁸.

Il est possible pour les commerçants de rédiger des politiques de confidentialité faciles à lire et à comprendre, et ce, même sans utiliser une présentation sous forme multi strates. En effet, certaines entreprises optent pour une approche conviviale. Elles utilisent des tables des matières ainsi que des sous-titres en couleurs et en gros caractère. Parfois aussi, elles utilisent des listes à puces (point forms) ou des gros caractères. Dans le cadre de notre échantillonnage, certaines entreprises ont utilisé cette méthode, notamment Stocard et Suretap.²⁷⁹ Nous pensons qu'un consommateur sera plus susceptible de lire la politique de confidentialité si le texte est court, dynamique et convivial.

Au cours de notre analyse, nous avons aussi trouvé des politiques de confidentialité qui nous semblent mal adaptées au support mobile. Ces politiques sont soit très longues, soit présentées sous forme d'un texte continu, soit écrites en très petit caractère (caractère 8.5 et 9 lorsqu'imprimées). Nous remarquons que ces politiques sont difficiles à lire sur un écran d'ordinateur ou sur une feuille de papier; sur un téléphone mobile, cette difficulté ne peut qu'être amplifiée. Il est probable qu'un consommateur se trouvant devant une telle présentation se décourage avant même d'avoir commencé sa lecture.

Par exemple, dans le portefeuille Fidme, qui est inséré dans les termes et conditions de l'entente, un document de 34 pages²⁸⁰, on utilise une table des matières et des sous-titres, mais la police et le caractère utilisés partout sont petits et similaires; les sous-titres ne sont pas mis en évidence. Le document est excessivement long et fastidieux. Il n'est pas accrocheur pour le lecteur et l'information pertinente y est difficile à trouver.

Pour sa part, l'application de Second Cup ne fournissait pas de lien menant vers la politique de confidentialité²⁸¹. L'application de Tim Horton, qui insère des mentions de confidentialité dans

²⁷⁶ *Ibid.*

²⁷⁷ CHASSIGNEUX et Groupe de travail Article 29 sur la protection des données, Avis sur « Dispositions avantage harmonisées en matière d'information » WP 100, 25 novembre 2004

²⁷⁸ *Ibid.*

²⁷⁹ https://play.google.com/store/apps/details?id=com.suretap.suretap_wallet et <http://stocardapp.com/privacy-policy>

²⁸⁰ http://fidme.com/entry/terms_of_service?lang=fr

²⁸¹ <http://www.secondcup.com/privacy-terms-and-conditions?lang=fr>

les modalités du contrat, n'est peut-être pas la mieux adaptée au support mobile²⁸². C'est également le cas de l'application de RBC, où il faut beaucoup de clics pour trouver l'information complète²⁸³.

4.2.3. Troisième lacune : les politiques de confidentialité manquent parfois de clarté

La notion de clarté est étroitement liée au principe de transparence. Selon ce dernier, les consommateurs doivent avoir accès à l'information et être en mesure de la comprendre sans avoir à faire des efforts déraisonnables (Art. 4.8.1 LPRPDE). Or, certaines politiques de confidentialité de notre échantillonnage manquent de clarté et de transparence. La clarté se définit comme étant ce qui «est facilement intelligible»²⁸⁴. Afin que les consommateurs puissent comprendre l'information véhiculée dans les clauses de confidentialité, ces dernières doivent utiliser un vocabulaire approprié, avoir le contenu nécessaire et donner les informations pertinentes à la collecte des renseignements personnels²⁸⁵. Selon le Groupe de travail «article 29» sur la protection des données, la compréhension des consommateurs est un objectif important afin qu'ils puissent prendre des décisions éclairées²⁸⁶.

Parmi notre échantillonnage, certaines politiques de confidentialité semblent manquer de clarté. Celles-ci utilisent un langage très juridique qui pourrait limiter la compréhension. Parfois, les phrases et les paragraphes sont très longs (nous avons vues des phrases ayant jusqu'à 18 lignes). Ces phrases contiennent des inversions, plusieurs idées, plusieurs nuances, ce qui la rend peu claire. Souvent, plusieurs termes complexes ne sont pas définis, ce qui peut limiter la compréhension.²⁸⁷ De plus, il semble aussi y avoir des contradictions entre certaines sections, ce qui pourrait nuire à la compréhension.

Certaines politiques de confidentialité ne sont pas claires quant à la collecte des renseignements personnels. Par exemple, la politique de confidentialité divise les renseignements recueillis par activité (ce qui est collecté directement de l'utilisateur, ce qui est collecté lors de la transaction, ce qui est collecté sur les réseaux sociaux, etc.), ce qui pourrait faciliter la compréhension des consommateurs. Mais pour informer les consommateurs, on utilise des termes très larges, comme « les renseignements nécessaires pour faire l'opération », sans ajouter de précisions.²⁸⁸

Enfin, certaines politiques de confidentialité ne sont offertes qu'en anglais, et ce, même si ces dernières ont été téléchargées sur un téléphone intelligent sur lequel le français a été installé comme langue par défaut et qui est utilisé à Montréal. Il s'agit des portefeuilles MobilePocket²⁸⁹

²⁸² <https://www.timhortons.com/ca/fr/timcard/timcard-terms-conditions.php> et <http://www.timhortons.com/ca/fr/privacy.php>

²⁸³ <http://www.rbcroyalbank.com/mobile/app-faqs.html?q=81#q81> ET <http://www.rbc.com/privacysecurity/ca/online-privacy.html>

²⁸⁴ Chassigneux Cynthia, «Guide pour l'élaboration d'une politique de confidentialité» Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, faculté de droit, Université de Montréal, Juin 2008, page 3 et Le Petit robert

²⁸⁵ Chassigneux page 4

²⁸⁶ Chassigneux page 4 et Groupe de travail «article 29» sur la protection des données, Avis sur «Dispositions davantage harmonisées en matière d'informations », 2004

²⁸⁷ <http://www.toysrus.ca/helpdesk/panel/index.jsp?display=safety&subdisplay=privacy>

²⁸⁸ <https://www.ugo.ca/fr/confidentialite>

²⁸⁹ <http://www.mobile-pocket.com/terms-of-use-privacy-policy/?lang=en>

et Beep'nGo²⁹⁰. De plus, ces clauses mentionnent les droits que les citoyens européens auraient, notamment en matière du safe harbour²⁹¹.

4.2.4. Quatrième lacune : les politiques de confidentialité définissent souvent un renseignement personnel uniquement comme un renseignement nominatif

Au cours de notre analyse, nous remarquons que certaines entreprises n'indiquent pas ce qu'est un renseignement personnel et que celles qui l'indiquent ne proposent pas toutes la même définition. Par exemple, Starbucks n'offre pas de définition du renseignement personnel dans sa politique de confidentialité. Celle-ci ne fait qu'énumérer les renseignements que l'application peut recueillir. Plusieurs de ces renseignements ont été reconnus comme des renseignements personnels par le CPVP, notamment les informations liées aux cartes de paiements, les renseignements nominatifs l'adresse IP, l'identifiant de l'appareil et les renseignements liés aux comptes ainsi que les renseignements liés à l'emplacement (géolocalisation). Par ailleurs, dans sa politique de confidentialité, Starbucks dit partager les renseignements de façon agrégée, ce qui devrait empêcher de les rattacher à un individu²⁹².

D'autres entreprises donnent une définition limitée du renseignement personnel – c'est le cas du portefeuille MobilePocket qui mentionne : « according to the Austrian Data Privacy Act (DSG 2000), personal information which can be used to identify web users qualifies as personal data. Such information includes name, address, postal address, phone number etc »²⁹³.

Certaines entreprises donnent la définition de renseignement personnel, et fournissent une liste de renseignements nominaux, liste qui se termine par le mot « etc. »; c'est le cas du portefeuille Ugo²⁹⁴. Or, le portefeuille Ugo recueille des renseignements qui sont considérés comme des renseignements personnels par le CPVP, notamment l'adresse IP, l'identifiant de l'appareil et l'emplacement géographique. De plus, l'application Ugo recueille des informations sur les cartes qui sont stockées sur l'appareil; or, cela n'est pas spécifié. Il y est également mentionné que le nombre de points de récompenses (notamment les points accumulés sur les cartes) seront recueillis. Par ailleurs, l'application Zara définit les données personnelles comme étant les renseignements nominaux et les numéros de carte de débit ou de crédit, puis ajoute le mot « etc. »²⁹⁵. Par ailleurs, d'autres politiques de confidentialité donnent la définition du renseignement personnel en se référant la Loi applicable au Canada; c'est le cas notamment de Tim Hortons²⁹⁶ et de ToysRus²⁹⁷.

Dans le cadre de notre analyse, nous remarquons que plusieurs entreprises utilisent leur propre définition de ce qui constitue un renseignement personnel. Ceci est important, car les

²⁹⁰ <http://www.mobeam.com/privacy/>

²⁹¹ Le safe-harbour ou le mécanisme d'adéquation est un ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux États-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne et https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf

²⁹² <http://fr.starbucks.ca/about-us/company-information/online-policies/privacy-statement>

²⁹³ <http://www.mobile-pocket.com/terms-of-use-privacy-policy/?lang=en>

²⁹⁴ <https://www.ugo.ca/fr/confidentialite>

²⁹⁵ http://static.zara.net/static/pdfs/CA/privacy-policy/privacy-policy-fr_CA-20151030.pdf

²⁹⁶ <http://www.timhortons.com/ca/fr/privacy.php>

²⁹⁷ http://www.toysrus.ca/helpdesk/panel/index.jsp?display=safety&subdisplay=privacy&locale=fr_CA

entreprises utilisent cette définition dans le traitement et la protection des données des consommateurs. Or, on remarque que, dans plusieurs des politiques de confidentialité, des renseignements considérés comme des renseignements personnels par le CPVP ne sont pas considérés comme tels par les entreprises. Ceci est un problème puisque la majorité des consommateurs ne connaissent pas toutes les subtilités du droit de la vie privée et peuvent se fier aux définitions données par les entreprises pour prendre des décisions concernant leurs renseignements personnels.

4.2.5. Cinquième lacune : les politiques de confidentialité recueillent souvent trop d'informations

Au cours de notre analyse, nous avons remarqué que certaines APMPV recueillent beaucoup plus de renseignements personnels que nécessaire.²⁹⁸ En guise d'exemple, nous vous présentons les applications de Starbucks et de PayPal. Nous avons choisi ces deux applications parce qu'elles recueillent un très grand nombre de renseignements personnels. De plus, les entreprises qui les ont créées sont de gros joueurs et, donc, fréquentées par un très grand nombre de consommateurs.

L'exemple de Starbucks

L'application Starbucks permet au consommateur d'utiliser son téléphone mobile pour payer ses achats, recharger sa carte, accumuler des points, faire une commande personnalisée à l'avance et à distance. La politique de confidentialité qui l'accompagne est rédigée clairement et l'information y est facilement repérable grâce à l'utilisation de sous-titres et de listes à puces.

Pour offrir tous ces services, Starbucks recueille un vaste éventail de renseignements personnels,²⁹⁹ et ce, de trois types³⁰⁰ :

- Renseignements sur le consommateur – celui-ci fournit notamment son nom, son nom d'utilisateur, son mot de passe, son adresse courriel, son numéro de téléphone, des renseignements financiers (ceux liés à sa carte de crédit), sa date de naissance, sa ville de naissance et des données démographiques. Renseignements obtenus lors de l'utilisation de services. Entrent dans cette catégorie les renseignements sur les achats
- Renseignements sur l'appareil et l'utilisation des sites web. On trouve dans cette catégorie les renseignements sur l'appareil (type et modèle de l'appareil, son identifiant unique) ainsi que sur le système d'exploitation, le navigateur, le fournisseur d'accès Internet, le nom du domaine, l'adresse IP. Il fournit également le moment (date et heure) de l'accès au service, les sites web visités (à la demande du consommateur ou parce qu'il y a été dirigé), les publicités sur lesquelles le consommateur a cliqué et le moment de ce clic). Lors d'un achat, il fournit des renseignements sur le produit acheté et l'endroit de l'achat. Il fournit la fréquence des achats et les récompenses accumulées. Enfin, il fournit son emplacement de

²⁹⁸ <http://fr.starbucks.ca/about-us/company-information/online-policies/privacy-statement> et https://www.paypal.com/ca/webapps/mpp/ua/privacy-full?country.x=CA&locale.x=en_CA

²⁹⁹ <http://fr.starbucks.ca/about-us/company-information/online-policies/privacy-statement>

³⁰⁰ <http://fr.starbucks.ca/about-us/company-information/online-policies/privacy-statement>

l'appareil (géolocalisation³⁰¹) lors de l'utilisation des services. À noter : cette dernière information peut être combinée à d'autres comme l'adresse IP et le code postal de l'utilisateur, ce qui permet de faire connaître au consommateur les magasins situés à proximité

- Renseignements recueillis auprès d'autres sources : Starbucks y recueille des informations publiquement accessibles, comme celles publiées sur des blogues, des salons de clavardage ou des réseaux sociaux tels que Facebook, Twitter ou Google+. Les informations provenant de ces sources sont utilisées pour corriger des informations erronées, recommander des produits au consommateur ou lui proposer des offres.

Starbucks définit les fins de la collecte. Cette entreprise affirme que la collecte est utilisée pour traiter les achats, transmettre les informations sur les commandes, les programmes, les concours et les demandes d'information au service à la clientèle, publier des commentaires sur les sites web, faire parvenir de la promotion et des offres « spéciales personnalisées » aux consommateurs, faire connaître une marque, un produit ou un événement promotionnel, détecter ainsi que prévenir des atteintes de sécurité et assurer une saine gestion.

Starbucks partage les informations recueillies avec des tiers « pour des opérations internes, pour la collaboration avec des fournisseurs de services, pour la conduite d'opérations commerciales internes, pour la divulgation aux fins de protection des intérêts légitimes ». L'entreprise partage également les informations recueillies avec d'autres sociétés à des fins de marketing. Starbucks écrit : « Nous pouvons partager vos renseignements avec des fournisseurs de services en vue de vous faire parvenir des promotions et des offres spéciales. Nous pouvons également partager des statistiques globales anonymes concernant votre utilisation de nos sites Web et services avec d'autres sociétés ».

L'application de Starbucks recueille beaucoup trop de renseignements personnels. De plus, ces renseignements peuvent être partagés avec des fournisseurs. Le problème, c'est qu'il n'est pas indiqué si les informations partagées avec les fournisseurs seront toujours dépersonnalisées. De plus, on ne sait pas qui sont les fournisseurs; la portée pourrait être très large. À la seconde phrase de la clause portant sur ce sujet, on mentionne que les statistiques globales seront partagées avec des tiers de façon anonyme. Par ailleurs, il n'y a pas de définition des renseignements qui seront partagés. Il n'y a pas non plus de mention à l'effet que certains d'entre eux sont des renseignements sensibles et ce, même si Starbucks recueille des renseignements sensibles.

Par ailleurs, bien que la publicité comportementale en ligne (PCL) soit faite à des fins légitimes au sens de la LPRPDE, les entreprises ne doivent recueillir que ce qui est nécessaire aux fins de la collecte³⁰². De plus, en 2015, le CPVP a énoncé que les Lignes directrices concernant la publicité comportementale en ligne s'appliquent aux sites web gratuits, ce qui est nettement différent d'un Programme de publicité pertinente (PPP)³⁰³. Dans une cause, le CPVP avait reçu de

³⁰¹ <http://fr.starbucks.ca/about-us/company-information/online-policies/privacy-statement>

³⁰² https://www.priv.gc.ca/information/guide/2011/gl_ba_1112_f.asp

³⁰³ Dans cette cause, il est question du programme de PPP de Bell. Cette entreprise imposait des frais aux publicitaires participants au PPP pour les aider à présenter des publicités à ses clients (Bell mobilité). Il y a trois éléments à

nombreuses plaintes sur le fait que Bell recueillait des renseignements sur les activités et les comptes de ses clients afin de leur faire de la publicité ciblée. Le consentement des consommateurs avait été obtenu par consentement implicite (opt out). Le CPVP a conclu que Bell aurait dû obtenir le consentement explicite de ses clients en raison de la présence de renseignements sensibles et des attentes raisonnables des clients de Bell. Le CPVP a pris en considération que ces renseignements avaient été récoltés pour l'utilisation des services et étaient aussi utilisés pour des fins secondaires (marketing), qu'il s'agissait de services payants, que cela facilitait la publicité ciblée et que Bell est une entreprise de télécommunication³⁰⁴.

La situation de Starbucks n'est pas nécessairement la même que celle de Bell. Starbucks vend principalement des cafés, des boissons et de la nourriture à ses clients. L'APMPV est offerte par l'entreprise comme moyen de paiement. Cette application est populaire. Selon Starbucks, en mars 2016, 18 % de toutes les transactions faites en magasin l'étaient à l'aide de paiements mobiles. De plus, un millions de Canadiens utilisent le programme de récompenses de Starbucks³⁰⁵. Celui-ci permet notamment aux consommateurs d'accumuler des points de fidélité. Dans le cadre de son utilisation, les consommateurs fournissent des renseignements personnels. Or, il semble que Starbucks recueille beaucoup d'information et qu'elle partage des renseignements personnels avec des tiers (fournisseurs) pour plusieurs fins, notamment pour faire du marketing et de la publicité. Dans ce contexte, nous pouvons nous demander si le modèle d'affaire de Starbucks correspond au modèle de gratuité³⁰⁶.

L'exemple de PayPal

PayPal est un portefeuille électronique permettant de faire des PMPV. Le consommateur peut lier des cartes de paiement à ce portefeuille. La politique de confidentialité de PayPal est très conviviale³⁰⁷. Il est facile pour le consommateur de trouver l'information nécessaire. La politique de confidentialité s'applique tant au site web qu'à l'application. La politique de confidentialité à la certification TRUSTe pour les renseignements recueillis *via* le site web. TRUSTe est une entreprise américaine qui offre des services aux entreprises, notamment des services de certification et de rédaction de politiques de confidentialité. Cependant, PayPal semble recueillir trop de renseignements personnels eu égard aux fins de la collecte.

PayPal recueille des renseignements personnels de trois manières. D'abord, il recueille des renseignements envoyés automatiquement par le téléphone intelligent du consommateur, ce qui inclut notamment les pages visitées, l'adresse IP, l'identifiant de l'appareil, la géolocalisation, des informations sur la connexion Internet et le réseau sans fil, des statistiques sur les pages visitées et des publicités. La politique de confidentialité énonce que le

considérer dans le PPP. Le premier est le profil du client. Bell crée et tient à jour le profil du client associé au programme PPP. Le profil comprend des données démographiques, l'information sur le compte ainsi que les sites web fréquentés et les applications utilisées. Le profil comprend aussi les intérêts du consommateur. Le deuxième est le profil de publicités. Les publicitaires participants créent, à l'aide d'une interface Web distincte, un profil de publicités qui définit la clientèle à laquelle ils souhaitent présenter des publicités ciblées. Le troisième est la concordance des profils et le placement d'annonces publicitaires. Bell facilite la présentation des publicités ciblées produites par les publicitaires du PPP à ses clients (LPRPDE No: 2015-001, para 13)

³⁰⁴ LPRPDE No: 2015-001, para 44

³⁰⁵ <http://strategyonline.ca/2016/03/08/starbucks-expands-mobile-ordering-across-canada/>

³⁰⁶ CPVP, «Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne», décembre 2015

³⁰⁷ https://www.paypal.com/ca/webapps/mpp/ua/privacy-full?country.x=CA&locale.x=en_CA

consommateur peut décliner les témoins et les pixels. Elle invite le consommateur à contacter son fournisseur de service mobile pour obtenir des informations sur la manière de désactiver la géolocalisation.

PayPal recueille aussi les renseignements fournis par le consommateur incluant l'information de contact – nom, adresse, numéro de téléphone, adresse courriel, etc. –, certains renseignements de nature financière – numéros de cartes de paiement et numéros de compte – et certains renseignements personnels – date de naissance et numéro d'assurance sociale (NAS). À noter, lorsque notre testeur a créé son compte, son NAS lui a été demandé à deux reprises. Cette information n'est pas obligatoire pour obtenir le service de paiement mobile, mais cela n'est pas indiqué clairement.

Par ailleurs, PayPal recueille des renseignements d'autres sources *via* les interactions du consommateur avec PayPal, avec des entreprises faisant partie de la famille PayPal ou avec d'autres entreprises (tel que prévu par la loi et leur politique de confidentialité). L'entreprise fera de même avec d'autres comptes si elle a des motifs de croire que le consommateur les contrôle en tout ou en partie.

PayPal recueille aussi les renseignements personnels du consommateur à partir d'autres sources, telles que les bureaux de crédit et des services de vérification d'identité. De plus, le consommateur peut choisir de donner à PayPal l'accès à certains renseignements sur des sites web tiers, comme Facebook et Twitter. L'information reçue par PayPal varie en fonction de ces sites. En associant un compte lié à un site tiers, le consommateur accepte que PayPal ait accès à cette information conformément à la politique de confidentialité de PayPal.

Les fins de la collecte sont justifiées pour fournir les services et procéder aux transactions. Elles le sont aussi pour des fins de sécurité telle que vérifier l'identité, gérer des risques ou éviter les activités prohibées et détecter des violations des termes de l'entente. Enfin, elles sont justifiées pour améliorer les services PayPal, protéger l'infrastructure et la technologie, faire de la publicité ciblée et vérifier la solvabilité des consommateurs. PayPal ne vend les informations à des tiers pour des fins de marketing; elle ne le fait qu'avec le consentement des consommateurs. Le consommateur peut ajuster ses paramètres pour ne plus recevoir de publicité ciblée.

PayPal recueille un large éventail de renseignements sur les consommateurs qui utilisent son APMPV. La quantité de renseignements recueillie semble dépasser ce qui est nécessaire aux fins de la collecte. Par ailleurs, certains des renseignements recueillis sont très sensibles, notamment le niveau de solvabilité du consommateur et son NAS. Dans le contexte de l'utilisation d'une APMPV, nous pouvons nous demander si recueillir ces renseignements est nécessaire.

4.2.6. Sixième lacune : il y a parfois des problèmes sur le plan du consentement et de son retrait

Plusieurs des politiques de confidentialité prévoient que les consommateurs peuvent retirer leur consentement ou moduler les paramètres de leur mobile de façon à fournir moins de renseignements personnels. Les consommateurs peuvent notamment retirer leur consentement à recevoir de la publicité ciblée. Ils peuvent aussi gérer leurs paramètres de façon à ce que l'endroit où ils se trouvent (en personne ou sur le cyberspace) demeure inconnu.

Il y a cependant un hic. Dans certaines des politiques de confidentialité analysées, cette information n'est pas facilement accessible. Parfois, elle est glissée dans des longues politiques de confidentialité³⁰⁸. Parfois, elle n'est pas assez claire pour le consommateur puisse ajuster les paramètres de son téléphone.

Autre problème : certaines politiques de confidentialité permettent aux consommateurs de retirer son consentement, notamment en matière de géolocalisation et de publicité ciblée. Par contre, elles disent que certains services peuvent ne pas être garantis³⁰⁹.

³⁰⁸ http://fidme.com/entry/terms_of_service?lang=fr

³⁰⁹ La politique de confidentialité indique que, si le consommateur retire son consentement, il est possible que l'entreprise ne puisse entretenir de lien avec lui ou lui fournir le service.

http://www.toysrus.ca/helpdesk/panel/index.jsp?display=safety&subdisplay=privacy&locale=fr_CA

D'autres entreprises mentionnent qu'il est possible que cela affecte le fonctionnement des services, notamment PayPal et Ugo.

Section 5. Groupe de discussion avec les consommateurs

L'analyse des politiques révèle que la plusieurs des applications de paiements mobiles recueille une très grande quantité de données sur leurs utilisateurs, les partages avec des tiers partenaires et peut attribuer au profil du consommateur un nombre considérable d'étiquettes. Mais qu'en pensent les consommateurs ? Comment sont-ils informés de la collecte de leurs renseignements personnels dans un contexte d'application de paiements mobiles. Quelles sont leurs connaissances et perceptions au sujet de la collecte de leurs renseignements personnels dans le cadre de l'utilisation d'applications de paiements mobile ? Quels renseignements sont-ils prêts à divulguer pour pouvoir utiliser des applications de paiements mobiles ? La manière de faire des entreprises en matière de vie privée leur convient-elle ? Comment souhaitent-ils être informés de la collecte de leurs renseignements personnels ?

Pour le savoir, nous avons tenu six groupes de discussions³¹⁰, trois à Toronto et trois à Montréal. Au total, 42 personnes y ont participé. Dans chacune de villes, les groupes 1, 2 et 3 étaient composés de personnes ayant un profil d'utilisateur différent. Dans chacun, on a remis aux participants une politique de confidentialité différente. Dans ces deux villes, nous avons recruté des participants utilisant des APMPV différentes. Les questions ont été les mêmes d'un groupe à l'autre.

Ainsi, les participants du premier groupe utilisaient des applications de PMPV émises par des commerçants, notamment Starbucks et Tim Hortons. Ils avaient soit un iPhone, soit un Android. Nous leur avons remis la politique de confidentialité de Starbucks³¹¹. Nous avons choisi de présenter cette dernière car elle était celle dont le format convenait le plus à une utilisation lors de groupes de discussion.

Pour leur part, les participants du deuxième groupe utilisaient des portefeuilles électroniques, notamment ApplePay. Ils avaient tous un iPhone. Nous leur avons remis une politique de confidentialité d'Apple. Nous avons choisi cette politique en raison de l'importance d'Apple sur le marché, notamment le marché américain, ainsi que de l'arrivée récente d'ApplePay sur le marché canadien.

Enfin, les participants du troisième groupe utilisaient des applications de paiements mobiles émises par des institutions financières, notamment TD, RBC et Desjardins. La vaste majorité de ces applications sont offertes sur un Android; les participants avaient tous un téléphone Android. Nous leur avons présenté la politique de confidentialité de la Banque TD. Nous avons choisi cette politique en raison de l'importance de TD sur le marché.

³¹⁰ La version française du questionnaire des groupes de discussions se trouve à l'annexe 1; la version anglaise se trouve à l'annexe 2.

³¹¹ Tel que mentionné à la section 4.2.5, cette application est très utilisée par les consommateurs canadiens. Nous l'avons retenu pour cette raison et aussi parce que son format convenait bien à une utilisation lors de groupes de discussion.

5.1. Utilisation des applications de paiements mobiles au point de vente par les consommateurs

Les participants aux groupes de discussion utilisaient des APMPV. Il s'agissait des applications de Starbucks, Second Cup, Tim Horton, ApplePay, Suretap, PayPal, CIBC, TD, RBC, Desjardins et Scotia. La grande majorité des participants utilisaient également d'autres types d'applications, notamment des applications ayant accès aux médias sociaux, pour magasiner ou pour obtenir de l'information.

Les participants disent utiliser les applications de paiement mobile pour plusieurs raisons. Ils aiment la rapidité et l'utilité des APMPV. Ils disent que « c'est plus rapide que de chercher du change dans ses poches » ou que « de sortir une carte pour payer son café ». Un participant utilise la fonction précommandée avec l'application et, lorsqu'il passe en magasin il prend son café, son sandwich et son reçu. Ce dernier est à son nom, ce qui lui fait dire: « ... *if it wasn't my neighbourhood store, I might be a little more ooey about, but, you know, it's two blocks away, and I know the people there. I walk in and I know most of the people in the place. But if it was some place I don't know.* »

Les participants trouvent ces applications pratiques. Ils n'ont pas besoin d'apporter toutes leurs cartes (de paiement et de fidélité) avec eux, puisqu'ils peuvent utiliser leur téléphone. D'autres aiment ne pas avoir à apporter leur portefeuille avec eux. Cela est pratique pour les joggeurs, pour les personnes qui sortent danser ainsi que pour les personnes qui fréquentent des endroits achalandés, comme les salles de spectacles.

De façon générale, les participants savent que, lorsqu'ils utilisent les paiements mobiles, les commerçants recueillent certaines de leurs informations, notamment leurs informations de contact et leurs informations financières. Plusieurs participants se doutent que les entreprises recueillent des informations sur leurs habitudes d'achat en magasin. Ils croient que cela leur permet de mieux cibler leurs besoins et de leur proposer des produits qui leur conviennent davantage, d'améliorer leur service à la clientèle et augmenter leurs chiffres d'affaires.

5.2. Quelques inquiétudes

Tous les participants étaient des utilisateurs d'APMPV. Malgré cela, nous voulions savoir s'ils avaient des craintes face à l'utilisation de ce type d'application. La grande majorité des participants n'en avaient pas. Par contre, certains craignaient d'être victime d'une fraude ou de se faire voler leur identité. Notons que, si la majorité des participants affirmaient verrouiller leur téléphone intelligent, certains avouaient ne pas le faire. D'autres craignaient de ne pas pouvoir faire des achats avec ce type de paiement. Selon eux, cette technologie étant nouvelle, plusieurs commerçants ne veulent pas l'utiliser ou ne savent pas comment le faire.

5.3. Des connaissances de base

Nous cherchions à savoir quelles étaient les connaissances de nos participants au sujet des concepts généraux de la protection de la vie privée. Nous leur avons demandé de nous donner des exemples de renseignements personnels. Ils ont pu identifier des données nominatives telles que le nom, la date de naissance, le sexe, le courriel et l'adresse. Plusieurs participants pensaient que les informations financières telles que les numéros carte de débit et de crédit, le numéro de compte et le numéro d'identifiant personnel étaient également des renseignements personnels. Un nombre plus limité de participants considérait que la géolocalisation était un renseignement personnel puisqu'elle permettait d'obtenir de l'information sur les consommateurs, par exemple leur lieu de travail. D'autres considèrent les habitudes d'achat et le type de bien acheté comme des renseignements personnels.

Au moins un participant par groupe croyait qu'il existe des profils détaillés sur les consommateurs, ce qui permet de cibler directement les consommateurs avec de la publicité. Une consommatrice a dit que le profil est « *a snapshot of who you are* ». Parmi ceux qui pensaient qu'il existe des profils de consommateurs, certains croyaient que ces profils étaient créés à des fins d'évaluation de crédit alors que d'autres croyaient qu'ils étaient utiles pour des études de marché.

Par ailleurs, la majorité des participants étaient conscients de recevoir de la publicité ciblée en ligne. La plupart savaient que ce type de publicité existe. Certains participants aimaient recevoir de la publicité en ligne. L'un d'eux a dit : « tant qu'à recevoir de la publicité automatiquement, j'aime mieux en recevoir sur quelque chose qui m'intéresse ». D'autres n'aiment pas cela du tout et trouvent cela « *creepy* ».

5.4. Lecture des termes et conditions de l'entente ou de la clause de confidentialité

Nous voulions savoir si les participants lisent les termes et conditions de l'entente. La lecture de ce document est importante en droit de la consommation en général, et pertinente en matière de vie privée. Les réponses sont les mêmes dans tous les groupes : aucun des participants ne les lisent en entier. Seulement trois participants ont mentionné y jeter un coup d'oeil.

Les réponses concernant la non-lecture des termes et conditions de l'entente et les clauses de confidentialité sont très similaires. Plusieurs ont dit : « *personne ne lit ça* ». Une personne a dit : « *c'est dans la culture sociale de ne pas les lire* ». Une autre a dit : « je vois une clause de confidentialité, je déroule le menu jusqu'en bas et je clique « j'accepte ». Un autre a dit « je vois une longue clause, on s'entend, je déroule jusqu'à la fin et je clique « j'accepte ».

Sans trop de surprises, la longueur des politiques de confidentialité a un effet rebutant. Les participants les trouvent difficiles à comprendre. Plusieurs ont dit que ce document était « rédigé par et pour des avocats ». D'autres ont invoqué le manque de temps. Un participant a dit qu'il aimerait lire les politiques de confidentialité mais que, lorsqu'il télécharge une application dans l'autobus et qu'il n'a que 20 minutes, il ne peut le faire. D'autres ont dit que,

lorsqu'ils choisissent de télécharger une application, ils veulent l'utiliser. Une participante a dit : « je ne vais pas lire tout ça quand je suis dans la file d'attente pour acheter un café ».

Certains participants ont plutôt affirmé que c'est par choix qu'ils ne lisaient pas les politiques de confidentialité. « Cela ne change rien », ont dit plusieurs d'entre eux, car pour utiliser l'application, il faut accepter. Un participant a dit « si je ne suis pas d'accord, je ne peux rien y changer ». D'autres, plus fatalistes, ont dit que ces informations étaient déjà recueillies ailleurs et que les entreprises avaient déjà des renseignements sur eux.

Alors que des consommateurs semblent penser que ces clauses visent à contrôler leurs comportements, un participant dit « les documents disent comment utiliser l'appli, qu'ils doivent l'utiliser correctement et qu'il n'entend pas mal l'utiliser »; donc, il n'a pas à les lire. À l'opposé, un autre consommateur a dit : « ça ne sert à rien de les lire. Les lois de protection du consommateur vont me protéger, que j'ai lu la clause ou non ».

Des 42 participants, trois disent lire les politiques de confidentialité en diagonale ou à l'occasion. Un participant a dit qu'il agissait ainsi pour savoir s'il y a des frais de crédit associés à l'utilisation. Un autre a dit agir de même car il s'intéresse à la vie privée et est analyste en politique. Une participante a remarqué que, lorsqu'elle télécharge une application, elle voit un « tableau de bord » dans lequel sont inscrits les renseignements auxquels l'application aura accès. Lorsque cela la préoccupe, elle clique sur le lien pour en savoir davantage. Elle dit « *when I see something about my location, I'm going to click on that link to know more, why it wants to know this* ».

5.5. Les informations que les consommateurs sont prêts à divulguer

Nous voulions savoir quels sont les renseignements personnels que les consommateurs étaient prêts à divulguer. Pour ce faire, nous avons fait la liste de tous les renseignements personnels pouvant potentiellement être recueillis par une application, puis nous l'avons remise aux participants.

De façon générale, les participants étaient prêts à divulguer des informations nominatives tel que leur nom, leur adresse et leur courriel. Par contre, la majorité des participants étaient hésitants à dévoiler leur revenu et des informations financières. Les participants avaient des avis partagés au sujet de la collecte de l'historique de navigation effectuée sur les sites web. Certains n'aimaient pas le suivi en ligne et trouvaient cela intrusif alors que d'autres aimaient recevoir de la publicité ciblée. Plusieurs avaient remarqué avoir déjà reçu de la publicité ciblée provenant d'un site sur lequel ils étaient déjà allés.

Les participants avaient aussi des avis partagés face au suivi de leur emplacement (géolocalisation) en temps réel. Certains trouvaient que cela était justifié, particulièrement dans un contexte de paiement, « dans le but d'assurer la sécurité ». D'autres n'aimaient pas divulguer leur localisation. En général, les participants n'aimaient pas que les applications puissent avoir accès à leur liste de contact, au contenu de leurs messages texte ou de leurs photos. Ils n'aimaient pas non plus que les applications aient accès à ce qui est enregistré sur leur téléphone intelligent, notamment les photos et les vidéos.

5.6. Réaction des consommateurs à la suite de la lecture des politiques de confidentialité

Les participants ont été étonnés du nombre de renseignements personnels pouvant être recueilli par les APMPV. Quelques-uns, dont une grande utilisatrice d'APMPV, a dit qu'elle désinstallerait les applications.

Certains participants comprenaient que des informations puissent être recueillies, notamment les informations nominales et les informations nécessaires pour le paiement. Ces derniers comprenaient la nécessité de la collecte de renseignements personnels, incluant la géolocalisation, l'adresse IP; ils trouvaient même que cela pouvait être utile pour assurer la sécurité des paiements mobiles. D'autres étaient très mal à l'aise que leur géolocalisation soit recueillie. Les participants s'entendaient pour dire que la géolocalisation ne devrait pas être recueillie en tout temps.

Le fait que l'APMPV puisse recueillir l'historique de navigation (les sites web visités) rendait aussi plusieurs participants mal à l'aise. Certains croyaient que l'application pouvait savoir tout ce qu'ils faisaient, où ils allaient, etc. Une consommatrice trouvait ce suivi tellement poussé qu'elle a dit « c'est comme si Starbucks est dans ton salon ». Une autre consommatrice a ajouté, « et que tu l'invite à prendre un café avec ».

Par ailleurs, les participants n'aimaient pas que leurs renseignements personnels soient partagés avec des tiers. Une consommatrice a dit que la définition du mot « tiers » est tellement large que « cela n'est pas limité du tout ». Un autre participant a ajouté que le mot « tiers » pourrait englober n'importe qui. Un participant a dit que, lorsqu'il paie pour un service, il s'attend à ce que ses données ne soient pas partagées avec des tiers.

À la suite de la lecture de la politique de confidentialité, certains participants ont dit qu'ils pensaient plus que jamais ne pas avoir de choix : s'ils veulent utiliser l'application, ils doivent accepter la collecte de leurs renseignements personnels.

Dans un autre ordre d'idée, un participant a mentionné que, « en magasin (...), le vendeur encourage les consommateurs à ne pas lire les politiques de confidentialité ». Il a dit : « c'est une chose si tu es chez toi et que tu scroll down, mais s'en est tout autre pour le vendeur de dire scroll down et clique sur accepte, sans lire. »

5.7. Comment ces clauses peuvent être améliorées

Nous avons demandé aux participants comment les politiques de confidentialité pourraient être améliorées, c'est-à-dire comment faire pour augmenter la propension des consommateurs à lire ces documents et pour améliorer la clarté de ces documents.

Plusieurs participants ont dit qu'ils aimeraient trouver, au début de la politique de confidentialité, un résumé qui en explique les faits saillants. D'autres ont dit qu'ils aimeraient

obtenir une forme condensée de la politique de confidentialité, quitte à pouvoir consulter la version longue, si nécessaire. De plus, les participants ont mentionné qu'ils aimeraient que les informations sur les options de retrait se trouvent au début de la politique et qu'elles soient facilement identifiables. D'ailleurs, certains participants voulaient plus d'options et plus de choix pour gérer l'accès à leurs renseignements personnels tout en pouvant utiliser l'application. D'autres croyaient plutôt qu'il fallait attirer l'attention des consommateurs en utilisant des couleurs, des sous-titres et des pop-up.

Par ailleurs, nous avons demandé aux participants s'ils seraient plus portés à faire affaire avec une entreprise qui miserait sur la protection de la vie privée. La grande majorité d'entre eux ont répondu par l'affirmative. Ils croyaient que cela n'était pas offert présentement. Certains ont même dit qu'ils seraient prêts à laisser tomber une entreprise qu'ils aiment pour se tourner vers une entreprise respectueuse de leur vie privée. Une minorité des participants étaient plutôt fatalistes. Ils disaient que cela ne changerait rien puisqu'il est déjà trop tard, leurs renseignements personnels étant déjà « *out there* ».

Conclusion et recommandations

Parce que la taille de leur écran est toute petite, qu'ils peuvent facilement être utilisés n'importe où et que de nombreuses applications, notamment les APMPV auxquelles nous nous intéressons ici, peuvent y être téléchargées aisément et distraitemment, les téléphones intelligents posent des défis particuliers en matière de divulgation d'information.

En cherchant les politiques de confidentialité des APMPV, nous avons constaté qu'elles sont parfois difficiles à trouver. Il arrive qu'elles soient aussi très longues et écrites en petits caractères, ce qui rend leur lecture fastidieuse, surtout sur un téléphone intelligent,

Nous avons aussi constaté que certaines politiques de confidentialité manquent de clarté. Celles-là sont difficiles à comprendre en raison de la façon dont l'information y est communiquée. Les phrases y sont longues et difficiles à comprendre. On y utilise souvent un vocabulaire juridique ou des mots complexes (sans les définir).

La définition de ce qu'est un renseignement personnel varie d'une politique de confidentialité à une autre. On oublie souvent d'y mentionner des renseignements qui ont été reconnus par le CPVP comme étant des renseignements personnels. Conséquence : les consommateurs pourraient se fier à des définitions inexactes pour déterminer ce qui constitue un renseignement personnel.

Autre observation : le nombre de renseignements recueillis est considérable et ces renseignements ne sont pas toujours nécessaires aux fins de la collecte. Par contre, dans les politiques de confidentialité, il est rarement question des renseignements sensibles comme les numéros de cartes de paiements et les identifiants personnels. Or, c'est souvent ce type de renseignements que les applications de paiements mobiles recueillent et les entreprises ont l'obligation de protéger.

Quelques entreprises partagent les informations recueillies avec des tiers à des fins de promotion et de marketing. Il semble que ces informations ne soient pas toujours dépersonnalisées et, lorsqu'il en est question dans une politique, cela manque de précision.

Dans certaines politiques de confidentialité, il est difficile de ne pas donner son consentement. Par contre, il est parfois possible pour les consommateurs de moduler leurs paramètres afin de limiter la collecte de renseignements personnels, notamment la géolocalisation. Or, cette information n'est pas toujours facile à trouver.

Selon ce que nous avons pu constater dans nos groupes de discussions, les consommateurs ne lisent pas les politiques de confidentialité. Ils se justifient en invoquant la longueur des documents, le langage difficile à comprendre et le caractère fastidieux des politiques de confidentialité. Ils croient aussi avoir un choix binaire : celui de tout accepter ou de ne pas pouvoir utiliser l'application. Dans une telle situation, disent-ils, à quoi sert la lecture de la politique. À noter : la FTC reconnaît que les politiques de confidentialité multi strates favorisent la propagation de l'information en matière de divulgation. De plus, la FTC et d'autres experts croient que les politiques de confidentialités doivent être présentées sous la forme multi-strates et qu'elles doivent être courtes, conviviales, accessibles et dynamiques.

Les consommateurs n'ont pas tous les mêmes connaissances. Certains savent qu'ils peuvent être suivis en ligne et dans le monde réel (*via* la géolocalisation), d'autres l'ignorent. Presque tous sont surpris de la quantité des informations qui peuvent être recueillies. Plusieurs aimeraient être informés différemment de la gestion des paramètres de leur téléphone intelligent. Ils seraient plus portés à lire une politique de confidentialité si celle-ci était courte et conviviale ainsi que si elle contenait des sous-titres. De plus, ils préfèrent faire affaire avec une entreprise qui est soucieuse de leur vie privée et qui recueille peu de renseignements personnels.

Certes, dans le contexte actuel, il est normal que les applications recueillent les renseignements personnels nécessaires aux paiements mobiles. Mais certaines des APMPV étudiées en recueillent beaucoup. De plus, la compréhension du système des paiements mobiles n'est pas à la portée de tous. Il peut être difficile pour plusieurs consommateurs de comprendre comment leurs renseignements personnels seront traités dans le processus de paiement. Par conséquent, il est essentiel que les politiques de confidentialités soit transparentes et faciles à comprendre. Or, certaines d'entre-elles renseignent peu ou mal les consommateurs³¹². Il est important qu'elles améliorent leurs pratiques, notamment en se préoccupant de la vie privée dès la conception d'un appareil (conception de la vie privée intégrée). Ce n'est qu'ainsi qu'elles pourront bien protéger les consommateurs et s'assurer de leur confiance, une condition *sine qua non* au système des paiements mobiles.

Recommandation aux législateurs fédéral et provinciaux :

- **Option consommateurs recommande de contraindre les entreprises fournissant des applications de paiements mobiles au point de vente (APMPV) ou des applications de portefeuille électronique de mettre en œuvre des mécanismes simples, efficaces et harmonisés permettant aux consommateurs de donner un consentement à la collecte de leur renseignement personnel et de le faire lors de l'utilisation d'application de paiement mobile;**
- **Option consommateurs recommande d'étudier la possibilité de limiter la collecte de renseignement très sensibles utilisés dans le contexte d'une application de paiements mobiles à ce qui est nécessaire pour la transaction;**
- **Option consommateurs recommande d'étudier la possibilité de limiter le partage de renseignements sensibles liés à l'utilisation de paiements mobiles à ce qui est absolument nécessaire pour la transaction;**
- **Option consommateurs recommande d'étudier la possibilité d'intégrer des notions de protection intégrée de la vie privée comme obligations légales pour les entreprises;**
- **Option consommateurs recommande d'augmenter le financement et les pouvoirs des autorités chargées de l'application des lois en matière de protection des**

³¹² Entrevue CPVP, février 2016

renseignements personnels pour tenir compte des défis que présentent les nouvelles technologies;

- Option consommateurs recommande de développer et d'encourager des initiatives en littératie numérique et de promouvoir, chez les Canadiens, l'apprentissage du fonctionnement de leurs appareils mobiles.

Recommandations aux Commissariats à la protection de la vie privée canadiens et aux autorités chargées de l'application des lois en matière de protection des renseignements personnels :

- Option consommateurs recommande d'étudier la possibilité d'établir des lignes directrices concernant les applications de paiements mobiles au point de vente;
- Option consommateurs recommande d'enquêter sur la conformité au principe de la nécessité de la collecte prévue à la Loi sur la protection des renseignements personnels et les documents électroniques, en obtenant des entreprises qui fournissent aux consommateurs des applications de paiement mobiles des informations précises sur le traitement et l'utilisation de chaque renseignement personnel recueilli.

Recommandations aux entreprises :

- Option consommateurs recommande aux entreprises qui conçoivent des applications de paiements mobiles d'adapter les politiques de confidentialité à l'environnement des paiements mobiles;
- Option consommateurs recommande aux entreprises de maximiser les techniques de communication aux consommateurs de façon à mieux s'adapter à l'environnement des téléphones intelligents;
- Option consommateurs recommande aux entreprises qui permettent aux consommateurs de télécharger des applications d'utiliser des notifications pop-up afin de leur faire savoir à quels renseignements personnels l'application aura accès, et ce, avant que cette application ne soit téléchargée;
- Option consommateurs recommande à toutes les entreprises permettant aux consommateurs de télécharger des applications d'étudier la possibilité de les informer par pop-up des fins de la collecte et du partage avec les tiers de leurs renseignements personnels;
- Option consommateurs recommande aux entreprises qui fabriquent des applications de paiements mobiles de prendre en compte les besoins de la vie privée des utilisateurs au stade de la conception de l'application (protection intégrée de la vie privée);

- Option consommateurs recommande aux entreprises qui fabriquent le matériel et les appareils de prendre en comptes la vie privée des utilisateurs au stade de la conception de ces appareils (protection intégrée de la vie privée).

Recommandations aux consommateurs

- Option consommateurs recommande aux consommateurs de s'informer davantage au sujet des renseignements personnels que les APMPV recueillent et de l'utilisation qu'elles en font. Elle leur recommande également de s'informer des moyens mis à leur disposition pour ne pas être suivis.
- Option consommateurs recommande aux consommateurs de s'informer d'avantages sur les enjeux de vie privée associés à l'utilisation d'APMPV;
- Option consommateurs recommande aux consommateurs de porter plainte aux autorités compétentes s'ils estiment que leur vie privée n'est pas respectée par les entreprises qui fournissent des APMPV.

Annexe 1 – Guide de discussion (version française)

Présentation (10 minutes)

Bonjour et bienvenue. Ce groupe de discussion est organisé dans le cadre d'une recherche menée par Option consommateurs, un organisme voué à la défense des droits des consommateurs. La durée de la discussion est de deux heures.

Nous voudrions connaître vos opinions. Nous ne voulons pas dire ce que vous croyez que les autres pensent ou ce que vous pensez que nous voulons entendre, mais bien ce que vous, vous pensez.

Vous pouvez être d'accord, en désaccord ou sans opinion. Même si vous êtes la seule personne du groupe à être d'un certain avis, vous pouvez représenter des centaines de milliers de personnes au pays qui ont la même opinion que vous.

Vous n'êtes pas obligé de vous adresser directement à moi pour formuler vos commentaires. Vous pouvez aussi échanger des idées et des arguments entre vous.

Nous allons enregistrer les échanges d'aujourd'hui et des personnes vous observent derrière la vitre. Il est aussi possible que je prenne des notes. Tout cela m'aide à rédiger mon rapport. Toutes les données recueillies seront traitées de manière confidentielle; jamais ce que vous dites ne vous sera attribué personnellement.

À la fin de la séance, qui ne devrait pas durer plus de 2 heures, nous vous remettrons la somme prévue pour votre participation.

Maintenant, nous allons faire un tour de table pour que chacun d'entre vous se nomme et se décrive brièvement. Nous aimerions connaître votre prénom, votre occupation professionnelle et votre lieu de résidence. Puisque nous allons parler des enjeux qui entourent les applications de téléphones intelligents, nous voulons également savoir quels sont les types d'applications que vous utilisez le plus souvent.

1.0 Paiements mobiles au point de vente (PMPV) – utilisation et attitude générale (20 minutes)

Vous avez été sélectionné pour participer à ce groupe de discussion car vous avez déjà utilisé une application de paiement mobile au point de vente (PMPV) pour payer vos achats chez un marchand. Nous voulons connaître vos expériences avec cette technologie et votre opinion sur les divers enjeux qui l'entourent. (Faire un tour de table inversé)

1. Dites-moi simplement pourquoi vous utilisez une application de PMPV?
(si tous répondent la même chose) Y a-t-il d'autres raisons?
2. Quel type d'achats faites-vous avec une application de PMPV?
3. Selon vous, quels sont les avantages d'utiliser ce type de paiement?
4. Avez-vous eu des problèmes en utilisant ce type d'application de paiements mobiles?
5. Avant de devenir un usager des applications de PMPV, étiez-vous réticent à les utiliser? Pourquoi?
6. Maintenant, vous sentez-vous plus en confiance?
7. Lorsque vous téléchargez une application de PMPV, que faites-vous? Quels sont les premières étapes?

(Attendre que les gens aient répondu. Au besoin, poser une ou plusieurs des questions suivantes)

Est-ce que vous lisez les termes et conditions de l'entente? **Si oui**, qu'en reprenez-vous

Lisez-vous la politique de confidentialité? **Si oui**, qu'en reprenez-vous? Est-ce que certains d'entre vous ont cliqué sur « J'accepte » sans lire les termes et conditions de l'entente? **Si oui**, pourquoi?

8. Lorsque vous voyez une clause de confidentialité en téléchargeant une application, quelle est votre impression? Est-ce que vous avez l'impression d'avoir le choix?

2.0 Connaissances générales des consommateurs (30 minutes)

9. Selon vous, quand vous utilisez votre application de paiement mobile au point de vente, qu'est-ce qui se passe? En quoi c'est différent d'autres types de paiement?
10. Selon vous, qu'est-ce qu'un renseignement personnel?

La définition est ``Tout renseignement qui, directement ou indirectement, permet d'identifier un individu``.

11. Lorsque vous utiliser une application de paiement, croyez-vous que l'entreprise (l'entreprise ayant développé l'application – Starbucks ou Apple Pay ou Paypal ou l'institution financière) recueille des renseignements personnels à votre sujet? Selon vous, quels renseignements sont recueillis?
12. Pourquoi, selon vous, les entreprises veulent recueillir cette information?
13. Selon vous, est-ce que les entreprises peuvent faire ce qu'elles veulent avec les renseignements personnels qu'elles recueillent des utilisateurs ou y-a-t-il des restrictions ou des limites sur ce qu'elles peuvent faire?
- a. Y-existe-il des lois limitant ces pratiques? Est-ce prévu au contrat? Est-ce prévu dans la clause de confidentialité?
 - b. Si oui, quels mécanismes limitent les renseignements personnels qu'une entreprise peut recueillir?
14. Selon vous, chez un commerçant, est-il possible de recueillir davantage de renseignements personnels avec une application de PMPV qu'avec une carte de débit ou une carte de crédit?
- Si les gens répondent **oui** : quels renseignements supplémentaires est-il possible de recueillir?
- Si les gens répondent **non** : pourquoi les renseignements recueillis sont-ils les mêmes?
15. Est-ce différent lorsqu'on fait achat avec un ordinateur?
- Si les gens répondent **oui** : en quoi est-ce différent?
- Si les gens répondent **non** : pourquoi est-ce pareil?

3.0 Les renseignements personnels recueillis

16. Lorsque vous commencer à utiliser une application de paiement mobile, êtes-vous informés des renseignements personnels qui sont recueillis?
17. Si oui, à quel moment en êtes-vous informé?
- a. lorsque vous téléchargez une application de PMPV?
 - b. lorsque vous entrez vos renseignements personnels financiers dans l'application de PMPV?
18. Comment en êtes-vous informé?
19. Y-a-t-il des avantages à donner vos renseignements personnels pour utiliser l'application de PMPV?

20. Dans quelles autres situations seriez-vous prêts à divulguer ces mêmes informations? Pourquoi?

21. Voici une liste de renseignements personnels qui pourrait être recueillis par une application de paiement mobile. Pour chacun d'entre eux, j'aimerais que vous cochiez si vous êtes ``en accord`` ou ``en désaccord`` ou si vous êtes à l'aise avec le fait que ces renseignements soient recueillis par une application de paiements mobiles au point de vente

- Nom
- Adresse
- Code postal
- Numéro de téléphone
- Courriel
- Date de naissance
- Âge
- Historique des achats effectués
- Fréquence de vos achats
- Revenu(s)
- Dossier de crédit
- Comptes et données provenant de votre profil Google ou Apple
- Détails de votre connexion wifi
- Adresse IP
- Historique des sites sur lesquels vous avez navigué à partir de votre téléphone
- Votre liste de contact
- Vos messages textes
- Vos messages chats
- Vos photos ou vos vidéos se trouvant sur votre téléphone
- Votre géolocalisation (en temps réel)
- Information qui se trouve sur votre carte Sim

OBJET HISTORIQUE DE NAVIGATION : que pensez-vous du fait que votre historique de navigation peut-être connu? Est-ce que vous aimeriez que le fait que vous avez consulté certains sites reste privé? Vous préoccupez-vous du type d'entreprise qui peut recueillir cette information?

22. Selon vous, qui a accès aux renseignements personnels recueillis par une application de PMPV?

- a. Quels types d'information l'émetteur de la carte de crédit peut-il recueillir?
- b. Quels types d'information le commerçant peut-il recueillir?
- c. Qu'en est-il de votre fournisseur de téléphonie cellulaire?

23. Avez-vous déjà entendu parler de publicité comportementale en ligne (PCL) ? Si oui, pouvez-vous expliquer de quoi il s'agit?

Donner définition après : La PCL se définit comme le suivi des activités des personnes sur le web afin de déterminer leur profil, puis de leur présenter des publicités adaptées à leurs intérêts présumés.

24. Croyez-vous avoir déjà reçu de la publicité ciblée?

- a. Après avoir utilisé une application de paiements mobiles?
- b. Après avoir navigué sur certains sites?
 - 1. Si les gens répondent oui : comment savez-vous que cela se produit?
- c. Est-ce que cela vous dérange de recevoir tout type de publicité? Est-ce qu'il y a des types de publicité ciblée que vous n'aimez pas recevoir? Quand est-ce que cela vous dérange?

4.0 Sécurité (15 minutes)

25. Quelle mesure de sécurité avez-vous installée sur votre téléphone mobile?

(si les participants ne répondent pas)

Mot de passe pour débloquer le téléphone

Mot de passe pour utiliser l'application de PMVP

26. Avez-vous déjà utilisé votre empreinte digitale pour déverrouiller votre téléphone mobile ou pour confirmer une transaction?

Si les gens répondent **non** : pour quelle raison?

Si les gens répondent **oui** : pourquoi ou pourquoi pas?

27. Quelles sont vos inquiétudes au sujet des applications de paiements mobiles au point de vente en matière de sécurité?

28. Selon vous, les paiements effectués via une application de PMVP sont-ils aussi sécurisés que les transactions par cartes de débit ou par cartes de crédit?

- a. Avez-vous eu des hésitations face à la sécurité des applications de paiements mobiles?
- b. Si votre mobile se faisait voler ou que vous le perdiez et que vous aviez fait beaucoup de transaction avec des applications de PMVP, qu'est-ce qui vous inquiéterait?

29. Selon vous, dans l'éventualité où il y aurait une atteinte à la sécurité lors d'une transaction, qui est responsable? (le fournisseur de l'application? l'émetteur de carte de crédit?)

30. Selon vous, si vous payez à l'aide d'une application de PMPV au point de vente, est-ce que vous avez les mêmes protections que si vous aviez payé avec une carte de débit ou de crédit ?

4.0 Lecture des consommateurs d'une clause de confidentialité et discussion (30 minutes)

Voici une clause de confidentialité qui est liée à une application de paiements mobiles au point de vente. Pourriez-vous la parcourir? N'hésitez pas si vous voulez surligner des passages (20 min.)

31. Quelle sont vos premières impressions?

32. Êtes-vous surpris par les informations qui s'y trouvent?

33. D'après cette clause, quels renseignements peuvent être recueillis?

34. D'après vous, cette clause permet-elle à un tiers d'avoir accès à vos renseignements personnels?

35. Selon vous, lorsque vous cliquez « J'accepte », à quoi vous engagez-vous?

36. Est-ce que cela vous semble correct?

5.0. Souhaits des consommateurs (20 minutes)

37. Selon vous, comment les clauses de confidentialité devraient-elles être rédigées?

- a. pour être davantage lues par les consommateurs?
- b. pour être mieux comprises par les consommateurs?

38. Aimerez-vous avoir plus de contrôle pour moduler l'accès à vos renseignements personnels tout en étant capable d'utiliser l'application de PMPV ?

Si les gens répondent **oui** : comment?

Si les gens répondent **non** : pourquoi?

39. Est-ce que les entreprises devraient être plus transparentes au sujet de la façon de recueillir vos renseignements personnels? Si les gens répondent oui : comment peuvent-elles être plus transparentes?

40. Si une entreprise misait sur le respect de la vie privée de ses clients dans sa publicité ou dans la conception de son application de PMVP, seriez-vous plus porté à l'utiliser?

Merci pour votre participation!

Annexe 2 – Guide de discussion (version anglaise)

**Discussion Guide
Environics Research
Attitudes towards mobile payment apps
PN8694
Option Consommateurs**

Introduction to Procedures (10 minutes)

Welcome to the group. We are doing this research on behalf of Option Consommateurs which is an advocacy group that defends the rights of consumers.

We want to hear your opinions. Not what you think other people think – but what you think!

Feel free to agree or disagree. Even if you are just one person around the table that takes a certain point of view, you could represent many Canadians who feel the same way as you do.

You don't have to direct all your comments to me; you can exchange ideas and arguments with each other too.

You are being taped and observed to help me write my report and I may take some notes during the group to remind myself of things also. This is all confidential and nothing you say will be attributed to you personally.

The host/hostess will pay you your incentives at the end of the session, which should last no more than two hours.

Let's go around the table so that each of you can tell us your name and a little bit about yourself, such as what kind of work you do if you work outside the home and also since we are going to be discussing some issues around use of smart phone apps – what are some of the apps you each use most often.

1.0 Point of sale mobile payment apps – usage and general attitudes (20 minutes)

We invited each of you to this focus group because you have all used a mobile phone application that allows you to pay for things in person at point of sale (POS). We want to hear about your experiences with this technology and your views some issues around them.

1. First of all, I'd like to go around the table and have you each tell us which mobile payment apps you have used and why.
2. What types of purchases do you do this way?
3. What are the advantages of paying for things this way?
4. Have you ever had any problems or issues around using a mobile payment app?
5. Before you downloaded and used the app for the first time, were you hesitant at all? Why?
6. Do you have more confidence in using mobile payment apps now?
7. When you first download a mobile payment app, what do you do? What are the first steps?

PROBE IF NOT MENTIONED: Do you read the “terms and conditions”? IF YES, what do you recall from that?

Do you read the privacy policy? **IF YES**, what do you recall from that?

Do any of you just click “accept” without reading the terms and conditions and privacy policies? **IF YES**, why?

8. In general when you download a mobile payment app and you see a privacy policy what do you think? Do you have any choice about whether or to accept it?

2.0 Consumer awareness (30 minutes)

9. As far as you know, when you use your mobile payment app at a point of sale, what happens? Is it different from any other way of paying for something?
10. When people talk about “personal information” what do they mean? What is “personal information”?

The actual definition is “*any information that – directly or indirectly – allows a person to be identified*”.

11. When you use a mobile payment app, do you think the company (i.e. the company that developed the app – Starbucks or Apple/PayPal or the bank) is collecting any personal information about you? What information you think they collect?
12. Why do you think companies would want to collect this information?
13. As far as you know, can companies do whatever they want with any personal information they collect from mobile payment users or are there limits or restriction on what they can do?
 - a. PROBE: Are there laws limiting them? Is it in the contract? Is it in the privacy policy?
 - b. IF YES, What mechanisms actually limit companies in what they can do with the information they collect?
14. As far as you know is there is any difference in how much personal information businesses can collect from you if you use a mobile payment app compared to what they can collect if you pay for something using a debit card or a credit card?
 - a. IF YES, in what way can they get more information?
 - b. IF NO, what makes you think it would be the same?
15. What about comparing it with the information that can be collected from you if you pay for something online at your computer?
 - a. IF YES, in what way can they get more information?
 - b. IF NO, what makes you think it would be the same?

3.0 Collected personal information (15 minutes)

16. When you decide to start using a mobile payment app, are you ever informed about what sort of personal information about you may be collected?
17. IF YES, when and how does this happen?
 - a. Is it when you first download the app?
 - b. Is it when you enter your personal financial/payment information into the app? (i.e. your debit or credit card number)
18. How are you informed

19. Are there reasons why it's still advantageous to provide or give access to your personal information in exchange for being able to use the mobile payment app?
20. Where else would you be willing to give up this much information about yourself?
21. Here is a list of kinds of personal information that could be collected about you when you use a mobile payment app. For each one I want you to check off "OK" or "Not OK" as to whether or you are comfortable with having this collected when you use a mobile payment app.

Name
Address
Postal code
Phone number
E-mail address
Date of birth
Age
Purchase history
Frequency of purchases
Income bracket
Credit rating
Your accounts and history from your profile with Apple or Google
Your WiFi connection details
Your IP address
History of what sites you have visited with your phone
Your contact list
Your text messages
Your chat messages
Any photos or videos on your phone
Your real-time location through geo-locating your phone
Information on your SIM card*

PROBE RE BROWSING HISTORY: What do you think of the idea that your whole browsing history could be known? Are there some sites you visit that you might want to keep private? Does it matter what kind of company is collecting the information?

22. When your personal information gets collected after you use a mobile payment app, who has access to it?
- What information can be accessed by your credit card or debit card issuer?
 - What can the merchant access?

c. What can your cell phone provider access?

23. Have you ever heard of the term “online behavioural advertising”? IF YES, What is it?

Definition: “*Online behavioural advertising*” describes how by following your online activities and behaviour a profile is developed of you that means that online advertising you are exposed to gets customized to what they think are your interests.

24. Have any of you ever received any advertising that you think was targeted at you...

- a. After you had used a mobile payment app?
- b. After you had visited a certain website?
 - i. IF YES, how do you know this happened?
- c. Do you mind getting any of this sort of “targeted advertising” or has it ever bothered you? When has it bothered you?

3.0 Security (15 minutes)

25. What kinds of security features do you have on your smartphone that apply to your use of the mobile payment app?

PROBE: password/finger prints to open the phone? Password/finger prints to open the payment app? Other?

26. How many of you have ever used your fingerprint to open your phone or to confirm a transaction? **IF YES or NO**, Why? Why not?

27. What security related concerns do you have about using your mobile payment app at the point of sale, if any?

28. When you pay for something using a mobile payment app, is it as secure as it is when you pay using a credit card or a debit card?

- a. Have any of you hesitated about starting to use a mobile payment app because of security concerns?
- b. If you were someone who had performed lots of mobile payment transactions and you lost your phone or it was stolen, what would you have to worry about?

29. If there was some sort of a security breach when you are doing a mobile payment, who do you think is responsible? (i.e. app provider? Credit card provider?)
30. When you pay for something using a mobile payment app, do you have the same protections that you have when you pay using a credit card or a debit card?

4.0 Confidentiality clause reading and discussion (20 minutes)

Here is an example of a privacy policy associated with a mobile payment app. Could you each take a few minutes to read through it and feel free to underline anything that stands out to you.

31. What is your first impression of this?
32. Are you at all surprised by what you read here?
33. From what you read in this policy, what information about you can be collected?
34. From you can tell does this policy allow any “third parties” to have access to your information?
35. When you click “Accept”, what are you actually agreeing or committing to?
36. How do you feel about all this?

5.0 Consumers’ wishes (20 minutes)

37. In your opinion, do these confidentiality agreements need to be revised in any way?
- a. What can we do so that consumers are more likely to read them?
 - b. What can we do so that consumers are more likely to understand them?
38. Would you like to have more control and be able to adjust what kinds of personal information about you can be collected and still be able to use the mobile payment app? IF YES, in what way? IF NO, Why not?

39. Should companies be more transparent about how your personal information may be used when you use their mobile payment app? IF YES, in what way?
40. If a company put out a mobile payment app and they promoted the fact that they would respect your privacy, would you be more likely to want to use that app?

Thanks for your participation!