RAPPORT DE CONCLUSIONS DE L'ENQUÊTE
MENÉE À LA SUITE DE LA PLAINTE DÉPOSÉE PAR
LA CLINIQUE D'INTÉRÊT PUBLIC ET DE POLITIQUE D'INTERNET
DU CANADA (CIPPIC)
contre
FACEBOOK INC.
AUX TERMES DE LA
LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET LES DOCUMENTS ÉLECTRONIQUES

PAR
ELIZABETH DENHAM
COMMISSAIRE ADJOINTE
À LA PROTECTION DE LA VIE PRIVÉE DU CANADA

Le 16 juillet 2009

Table des matières

Sommaire

La plainte

La plainte que la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) a déposée contre Facebook comprenait 24 allégations portant sur 11 aspects distincts. Parmi ceux-ci, on retrouve les paramètres de confidentialité par défaut, la collecte et l'utilisation des renseignements personnels des utilisateurs à des fins publicitaires, la communication des renseignements personnels des utilisateurs aux tiers développeurs d'applications, et la collecte et l'utilisation des renseignements personnels des non-utilisateurs.

Les enjeux

L'enjeu de la **connaissance et du consentement** était au cœur des allégations de la CIPPIC. Dans le cadre de son enquête, le Commissariat s'est penché sur la question de savoir si Facebook donnait suffisamment d'information pour soutenir le consentement valable des utilisateurs en documentant les fins de la collecte, de l'utilisation et de la communication des renseignements personnels et en portant ces fins à l'attention des personnes de manière raisonnablement directe et transparente. La question de la **conservation** des renseignements personnels fait plus précisément surface dans les allégations relatives à la désactivation et à la suppression des comptes ainsi qu'aux renseignements des non-utilisateurs. La question des **mesures de sécurité** occupait une place importante dans les allégations relatives aux applications de tiers et à Facebook Mobile.

Constatations et conclusions

La commissaire adjointe n'a trouvé aucune preuve d'infraction à la *Loi sur la protection des renseignements personnels et les documents électroniques* (la *Loi*) relativement à quatre des sujets (par exemple, tromperie et fausse représentation, Facebook Mobile); elle a donc conclu que les allégations n'étaient **pas fondées**. Pour quatre autres sujets (par exemple, les paramètres de confidentialité par défaut et la publicité), la commissaire adjointe a constaté que Facebook contrevenait à la *Loi*, mais a conclu que les allégations étaient **fondées et résolues** à la lumière des mesures correctives que Facebook proposait en réponse à ses recommandations.

En ce qui a trait aux autres sujets, soit les applications de tiers, la désactivation et la

suppression du compte, les comptes des utilisateurs décédés, et les renseignements personnels des non-utilisateurs, la commissaire adjointe a également constaté que Facebook contrevenait à la *Loi* et a conclu que les allégations étaient **fondées**. En ce qui concerne ces quatre éléments, des questions demeurent irrésolues dans la mesure où Facebook n'a pas encore accepté d'adopter ses recommandations. Plus particulièrement à l'égard des applications de tiers, la commissaire adjointe a déterminé que Facebook n'avait pas mis en place des mesures de sécurité adéquates pour empêcher les développeurs d'applications d'accéder sans autorisation aux renseignements personnels des utilisateurs. De plus, l'organisation ne fait pas des efforts suffisants pour obtenir le consentement valable des personnes à la communication de leurs renseignements personnels aux développeurs d'applications.

Suivi

Lorsqu'elle jugeait que les allégations fondées étaient résolues, la commissaire adjointe a avisé Facebook que le Commissariat effectuerait un suivi 30 jours après la présentation du rapport pour vérifier si les mesures correctives proposées avaient été mises en œuvre. Pour ce qui est des allégations fondées qui demeurent non résolues, la commissaire adjointe a demandé à Facebook de reconsidérer ses recommandations et l'a avisée que le Commissariat, dans le cadre du suivi qu'il effectuerait 30 jours après la présentation du rapport, chercherait également des preuves que les recommandations en suspens, ou des solutions de rechange acceptables, ont été acceptées et mises en œuvre.

Rapport de conclusions

Plainte déposée en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la *Loi*)

1. Dans une lettre datée du 30 mai 2008, des représentants de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) ont déposé une plainte à multiples volets contre Facebook Inc. portant sur des questions allant de la collecte de la date de naissance au moment de l'inscription jusqu'à la communication de renseignements personnels à des tiers développeurs d'applications. En raison de la complexité de la plainte, le présent rapport a été divisé en une série de petits rapports abordant les diverses allégations regroupées par thème. Nous avons informé Facebook du dépôt de la plainte le 3 juin 2008.

2. Le 20 juin 2008, la CIPPIC a fourni des renseignements supplémentaires sur les allégations liées aux applications de tiers, notamment en ce qui concerne la tendance des tiers développeurs d'applications à commercialiser leurs produits par la publicité.

3. Facebook a présenté ses observations le 14 juillet 2008 et a offert une présentation technique au personnel du Commissariat à la protection de la vie privée du Canada le 21 août 2008.

4. Le Commissariat a présenté un rapport préliminaire aux deux parties le 27 mars 2009. Dans le rapport que nous avons remis à Facebook, nous avons fait état de plusieurs de nos inquiétudes et émis 20 recommandations.

5. Nous avons ensuite eu deux rencontres avec des représentants de Facebook, les 15 avril et 8 mai 2009, afin de discuter de notre rapport préliminaire et des préoccupations que nous avons formulées dans le rapport préliminaire. À la suite de chaque rencontre, Facebook a présenté des réponses écrites aux recommandations formulées dans le rapport préliminaire. Le présent rapport de conclusions est le résultat de notre enquête et de nos discussions avec Facebook.

Introduction

6. Le réseautage social en ligne est un phénomène culturel. La popularité de ces sites a explosé au cours des cinq dernières années — des millions de personnes partout dans le monde s'y inscrivent pour rester en relation avec leurs amis et leur famille et pour rencontrer des gens. Ces sites représentent un tournant spectaculaire dans la façon dont les gens communiquent, et ils soulèvent d'intéressantes questions par rapport à l'idée qui prévaut depuis longtemps de la vie privée et de la protection de cette dernière.

7. À une époque où tout le monde semble laisser l'empreinte numérique de ses points de vue, photos, croyances et parfois même de ses aléas amoureux, notre notion du contrôle de ses propres renseignements personnels — qui constitue le fondement de la *Loi sur la protection des renseignements personnels et les documents électroniques* — se trouve sérieusement ébranlée.

8. Facebook est le site de réseautage social le plus populaire au monde — il compte plus de 200 millions d'utilisateurs à travers le monde et environ 10 millions d'utilisateurs au Canada seulement. Facebook se définit comme « un utilitaire social qui facilite la communication entre amis, parents et collègues de travail » [traduction]. Son slogan est « Facebook vous aide à garder contact avec les personnes de votre entourage » [traduction].

9. À titre de défenseur du droit à la vie privée et de responsable de la conscientisation à ce sujet, notre rôle est clair. Les utilisateurs et les employeurs ont besoin d'un système de signalisation pour les aider à naviguer dans cet univers de façon à atteindre un équilibre entre les avantages que le réseautage social procure à plusieurs et la prise de conscience que ce qu'on affiche en ligne n'est jamais complètement privé.

10. De notre point de vue d'organisme de réglementation, les sites de réseautage social comme Facebook posent un défi intéressant. L'objectif de la *Loi* est de trouver un équilibre entre le besoin d'une organisation de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins appropriées et le droit des personnes à la vie privée relativement à leurs renseignements personnels. Dans l'univers hors ligne, les organisations peuvent recueillir certains renseignements personnels, les utiliser et les communiquer, en vue de

fournir un service particulier. Les utilisateurs de Facebook choisissent les renseignements qu'ils fournissent de façon à répondre à leurs propres besoins de réseautage social. Lorsqu'une personne souhaite s'inscrire à Facebook, l'entreprise lui demande de fournir seulement quatre renseignements personnels : le nom, l'adresse de courriel, la date de naissance et le sexe. Un utilisateur peut choisir de fournir volontairement d'autres renseignements précisément aux fins d'échange avec d'autres utilisateurs.

11. Bien sûr, les personnes en question affichent des renseignements personnels à des fins purement personnelles. Toutefois, si les renseignements qu'une personne affiche à des fins purement personnelles échapperaient normalement à la portée de la *Loi*, ils y sont bel et bien assujettis et la *Loi* impose des obligations à Facebook dans la mesure où Facebook utilise ces renseignements personnels dans le cadre de ses activités commerciales. Ce n'est pas conflictuel : les mêmes renseignements peuvent servir à la fois à des fins personnelles et commerciales. De telles situations sont présentées de façon très claire dans les sections du rapport qui traitent de la publicité et des renseignements des non-utilisateurs.

12. On peut raisonnablement supposer que les fonctions du site n'ayant pas de lien évident avec le modèle opérationnel de ce dernier sont proposées afin de rehausser l'expérience de l'utilisateur sur Facebook. Il est fort possible que de rehausser l'expérience du site encouragera les membres existants à continuer d'utiliser le site et encouragera possiblement d'autres personnes à s'inscrire — contribuant ainsi indirectement au succès de Facebook à titre d'entreprise commerciale. Aussi, la collecte, l'utilisation et la communication de renseignements personnels en relation à une fonction du site et sans lien direct, commercial et apparent peuvent tout de même être considérées comme se déroulant « dans le cadre d'activités commerciales » aux termes de la *Loi*.

13. Le contrôle qu'exerce une personne sur ses propres renseignements personnels est l'une des principales notions qui sous-tend la *Loi*. De même, la connaissance et le consentement sont les pierres angulaires de la loi. Plusieurs des plaintes déposées auprès du Commissariat se rapportent essentiellement à des questions de consentement; je me suis donc penchée sur la question de savoir si le consentement, pour n'importe quel cas donné, était valable. Auparavant, le Commissariat jugeait le consentement valable lorsque la personne concernée était informée en termes clairs et compréhensibles des fins de la collecte, de l'utilisation et de la communication des renseignements personnels avant même que la collecte, l'utilisation ou la communication n'aient lieu. Il est relativement simple de décrire la façon selon laquelle Facebook

satisfait à cette exigence en informant les utilisateurs de ses fins par l'entremise de sa Politique de confidentialité, ses conditions de service et d'autres documents. Nous avons fait plusieurs recommandations à Facebook — ils en ont accepté plusieurs et, dans d'autres cas, ont proposé des solutions de rechange acceptables — afin de s'assurer que les utilisateurs disposent de l'information nécessaire pour prendre des décisions valables par rapport à la mesure dans laquelle ils sont prêts à échanger des renseignements personnels. Si nous sommes partisans de la notification « en temps réel », nous n'oublions pas, et nous apprécions, que Facebook souhaite proposer à ses utilisateurs une expérience sans heurts.

14. Toutefois, à l'instar de toute enquête sur une plainte, nous étudions le cas en fonction des preuves présentées et le modèle de cette entreprise est différent de ceux étudiés dans le passé. Notre point de vue sur la publicité s'est adapté au modèle opérationnel des sites de réseautage social. Nous reconnaissons que les utilisateurs doivent accepter la publicité dans une certaine mesure, puisque le site est offert gratuitement et l'entreprise doit générer des revenus. Toutefois, nous faisons une distinction (Facebook aussi, d'ailleurs) entre les différents types de publicité et de consentement. En ce qui a trait aux tierces parties, une organisation ayant un modèle traditionnel peut sous-traiter une partie de ses opérations à des tiers (confiant donc des renseignements personnels à une autre entité), ou communiquer des renseignements personnels à une autre entreprise qui achète des listes de clients à des fins de marketing, par exemple. Dans le cadre de cette enquête, nous constatons que l'entreprise procure en effet à des tiers développeurs d'applications la capacité de récupérer les renseignements personnels des utilisateurs (et de leurs amis) qui s'inscrivent à ces applications. Nous entretenons des préoccupations relativement aux mesures de sécurité que Facebook a mises en places; selon nous, elles pourraient être plus efficaces. Nous croyons également que Facebook devrait en faire beaucoup plus pour s'assurer que le consentement des utilisateurs est bel et bien obtenu quand les développeurs d'applications accèdent aux renseignements personnels de ces utilisateurs.

15. Quelques commentaires sur l'enquête et les conclusions : nous avons limité la portée de l'enquête aux utilisateurs ayant plus de 18 ans. Nos commentaires et nos conclusions ne tiennent donc pas compte de l'expérience des mineurs qui utilisent le site.

16. De plus, Facebook est un environnement dynamique qui a subi de nombreux changements, surtout en termes d'apparence et de documentation, depuis que la CIPPIC a déposé une plainte le 30 mai 2008. Par exemple, Facebook a

lancé une nouvelle interface-utilisateur à l'automne 2008 et, récemment, les Conditions d'utilisation ont été remplacées par la Déclaration des droits et responsabilités. Mes constatations se fondent sur le site tel qu'il apparaissait au moment du dépôt de la plainte. Toutefois, les sections Allégations et Constatations tiennent largement compte des changements relatifs au site et à la documentation.

17. Je tiens à souligner que les utilisateurs de Facebook sont réputés pour faire part à l'entreprise de leur opinion par rapport aux particularités du site (qu'ils aiment ou qu'ils n'aiment pas). Suite à nos recommandations, Facebook a indiqué qu'il leur faudrait consulter les utilisateurs sur tout changement qu'ils prévoyaient faire à la documentation du site en raison de nos demandes. Bien que nous appréciions que Facebook juge la rétroaction des utilisateurs importante, les exigences et obligations législatives en vertu de la *Loi* ne sont pas subordonnées à l'approbation des utilisateurs.

18. Cela dit, Facebook fait des efforts louables pour offrir à ses utilisateurs des mesures de protection de la vie privée détaillées. Elles renferment souvent le type d'information nécessaire pour que les utilisateurs prennent des décisions raisonnables, bien que l'information se retrouve un peu partout à travers le site. L'une de nos recommandations consiste à demander à Facebook de réunir cette information sous une seule rubrique par souci de commodité. À notre avis, cela ne nuira pas outre mesure à l'expérience de l'utilisateur — cela répondrait même aux attentes raisonnables des utilisateurs.

19. Nous — les sites de réseautage social, utilisateurs, employeurs, autorités de protection des données — commençons à peine à élaborer les règles d'engagement de ce nouvel univers. Le présent rapport est notre contribution à l'élaboration de ces règles. Nous sommes reconnaissants envers Facebook de leur coopération pendant toute la durée de l'enquête et nous apprécions son engagement manifeste à permettre aux utilisateurs d'exercer un contrôle sur leurs renseignements personnels tout en leur offrant la possibilité d'entrer en contact avec d'autres.

Section 1

Collecte de la date de naissance

Allégations

20. La CIPPIC a allégué dans sa plainte que Facebook :

    1) exigeait des utilisateurs qu'ils fournissent leur date de naissance comme condition d'inscription sans raison valable, en dérogation au principe 4.3.3[1];
    2) n'expliquait pas correctement aux utilisateurs la raison pour laquelle ils devaient fournir leur date de naissance et la façon dont celle-ci serait utilisée, en dérogation au principe 4.3.2.

Résumé de l'enquête

21. Au moment du dépôt de la plainte, un utilisateur devait fournir son nom, son adresse de courriel et sa date de naissance pour ouvrir un compte Facebook. Un lien « Pourquoi dois-je fournir ceci? » [traduction] se trouve sous le champ Date de naissance. Dans la fenêtre contextuelle intitulée « Pourquoi dois-je fournir ma date de naissance? » [traduction], on peut notamment lire ceci :

    « Facebook demande à tous ses utilisateurs de fournir leur vraie date de naissance par mesure de sécurité et pour assurer l'intégrité du site. Vous pourrez masquer cette information de votre profil, si vous le souhaitez » [traduction].

    Il est donc à noter que les utilisateurs peuvent masquer entièrement ou partiellement leur date de naissance de leur profil.

22. Dans ses observations écrites au Commissariat, Facebook affirme qu'elle se sert de la date de naissance pour calculer l'âge et ainsi faire respecter l'exigence concernant l'âge minimal de 13 ans, et appliquer des dispositions particulières aux adultes qui regardent le profil de mineurs.

[1] Tous les principes auxquels on fait référence dans le présent rapport sont tirés de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C., 2000, ch. 5.

23. Facebook affirme limiter l'inscription aux personnes de 13 ans et plus en vertu d'une exigence de la *Children's Online Privacy Protection Act* (COPPA) des États-Unis. En particulier, la COPPA interdit aux sites Internet de recueillir des renseignements personnels sur des enfants de moins de 13 ans sans le consentement parental vérifiable. Facebook indique qu'elle exige la date de naissance plutôt que de demander simplement à l'utilisateur s'il est âgé de 13 ans ou plus pour se conformer à une pratique exemplaire recommandée par la Federal Trade Commission (FTC), l'organisme américain responsable de la mise en application de la COPPA. Dans un rapport au Congrès intitulé *Implementing the Children's Online Privacy Protection Act*, la FTC expose son point de vue sur la vérification de l'âge en ligne :

    « Un site dont la page d'inscription permet uniquement d'inscrire une année de naissance à partir de l'âge de 13 ans ou qui signale aux visiteurs que les enfants de moins de 13 ans ne peuvent participer au site risque d'encourager la falsification. Au contraire, un site qui permet aux visiteurs d'inscrire une date de naissance et qui n'indique pas la raison pour laquelle il exige ce renseignement sera plus en mesure de repérer efficacement les enfants de moins de 13 ans » [traduction].

24. La FTC encourage également les sites à utiliser un mécanisme de suivi afin d'éviter que les enfants reviennent en arrière pour modifier leur date de naissance après avoir été bloqués d'un site.

25. Dans sa réponse aux allégations de la CIPPIC, Facebook renvoie à une entente qu'elle a conclue en mai 2008 avec 49 secrétaires à la Justice des États-Unis. L'entente, qui vise à accroître la sécurité de Facebook pour les mineurs, comprend des dispositions relatives à la conception et à la mise en œuvre de technologies et de fonctionnalités qui :

    - empêchent les utilisateurs n'ayant pas l'âge requis d'accéder au site;
    - protègent les mineurs contre les contacts inappropriés;
    - protègent les mineurs contre un contenu inapproprié;
    - offrent des outils de sécurité à tous les utilisateurs de sites de réseautage social.

    Par exemple, Facebook a convenu de mettre en place et d'appliquer le blocage de l'accès en fonction de l'âge ainsi que de surveiller et d'examiner le profil des utilisateurs qui modifient leur âge pour indiquer qu'ils ont plus ou moins de 18 ans.

26. Toujours dans le cadre de cette initiative, Facebook a convenu de participer au groupe de travail Internet Safety Technical Task Force, piloté par le Berkman Center for Internet and Society de l'Université Harvard. Créé à la suite d'un accord entre les secrétaires à la Justice des États-Unis et MySpace, le groupe de travail traite de l'implantation d'un logiciel de vérification de l'âge et de l'identité. Dans son rapport définitif de décembre 2008 intitulé *Enhancing Child Safety and Online Technologies*, le groupe établit, évalue et propose des solutions pour contrer les risques que représente le Web pour les enfants et les jeunes.

27. Dans ses observations au Commissariat, Facebook fait remarquer que le dialogue du groupe de travail s'est tenu en public et fait valoir qu'il est donc fallacieux de la part de la CIPPIC de suggérer que Facebook n'a pas été transparente quant aux raisons pour lesquelles elle exige la date de naissance.

28. En février 2009, Facebook faisait partie des 17 services de réseautage social ayant signé une entente de la Commission européenne visant à améliorer la sécurité des services de réseautage social pour les jeunes Européens. Parallèlement à cette entente, la Commission européenne a publié le document *Safer Social Networking Principles for the EU,* dans lequel elle défend diverses mesures de sécurité prises selon l'âge des utilisateurs.

29. La seconde raison invoquée par Facebook pour justifier la collecte de la date de naissance comme condition de service est de contribuer à vérifier l'identité des adultes. Les comportements interdits dans le site étaient indiqués dans les Conditions d'utilisation et le Code de conduite de Facebook au moment de la plainte. Notamment, en acceptant les Conditions d'utilisation et le Code de conduite, les utilisateurs conviennent de ne pas utiliser le service pour se faire passer pour toute personne physique ou morale, ou faire une fausse déclaration ou représentation au sujet d'eux-mêmes, de leur âge ou de leur affiliation avec une personne physique ou morale. En date du 1er mai 2009, les Conditions d'utilisation avaient été remplacées par une Déclaration des droits et responsabilités, qui remplit en général la même fonction.

30. Facebook encourage les personnes à présenter leur véritable identité, car elle considère que cela favorise un environnement en ligne sécuritaire, en incitant les internautes à assumer la responsabilité de leurs actes. Dans le cadre de la surveillance des comportements anormaux, Facebook tient compte de l'âge de l'utilisateur et de ses activités dans le site, notamment les réseaux dont il est membre et l'âge de ses amis. Tout écart déclenche un signalement.

31. Dans ses observations au Commissariat, Facebook affirme ce qui suit :

« La responsabilité des propos tenus et des activités réalisées sur Facebook est la norme; cette disposition a permis de réduire le risque d'usage abusif, mais non de l'éliminer. » [traduction].

32. Facebook mentionne la limite d'âge minimale de 13 ans à plusieurs reprises dans sa Politique de confidentialité, dans la nouvelle Déclaration des droits et responsabilités et dans la section Aide du site, sous le titre Sécurité. Pour s'inscrire, les utilisateurs doivent reconnaître qu'ils ont lu et accepté la Politique de confidentialité et les Conditions d'utilisation (maintenant remplacée par la Déclaration des droits et responsabilités). Cependant, aucune mention précise de la collecte de la date de naissance n'est faite dans ces documents.

33. En fait, le site Facebook ne contient aucune mention précise de la collecte de la date de naissance, à l'exception de la fenêtre contextuelle mentionnée ci-dessus. Interrogée à ce sujet, Facebook a indiqué ce qui suit :

« L'avis au moment de la collecte constitue une pratique exemplaire de l'industrie. [...] Notre Politique de confidentialité traite des exigences d'âge et il est fait explicitement mention des utilisateurs de moins de 13 ans et de ceux âgés de 13 à 18 ans. Cette section ne serait pas pertinente si nous ne recueillions pas la date de naissance. En outre, les avis réguliers d'anniversaires, par l'entremise de la page d'accueil et du service de courriel, rappellent aux utilisateurs que les dates de naissance ont été demandées et qu'elles peuvent être utilisées pour le fonctionnement du site » [traduction].

34. Facebook a également confirmé que l'âge des utilisateurs servait à des fins publicitaires. Elle signale notamment ceci :

« L'âge de l'utilisateur ne peut être utilisé que sous une forme non nominale à des fins publicitaires, conformément aux dispositions de ciblage des données du profil de la Politique de confidentialité : "Facebook peut utiliser les données de votre profil sans vous identifier en tant qu'individu vis-à-vis des tiers" » [traduction].

35. Selon les observations de Facebook présentées au Commissariat et une revue des documents contenus sur le site, le Commissariat a d'abord cru que, si un utilisateur choisissait de masquer sa date de naissance du profil, celle-ci ne serait pas utilisée à des fins publicitaires. Cependant, il a été porté à notre attention qu'une utilisatrice de Facebook ayant choisi de « masquer », pour

reprendre l'expression de Facebook, sa date de naissance de son profil avait néanmoins reçu une publicité de Facebook destinée aux personnes de son âge.

36. À partir d'autres observations de Facebook à cet égard, nous avons établi ceci :

- En offrant aux utilisateurs la possibilité de « masquer » leurs dates de naissance de leurs profils, Facebook ne permet en fait que de rendre celles-ci « invisibles », et n'empêche pas leur utilisation à des fins publicitaires ou par des applications de tiers.
- Facebook considère donc une date de naissance « masquée » d'un profil comme une information de « profil » qui peut être utilisée à des fins publicitaires.
- Par information de « profil », Facebook n'entend pas nécessairement les renseignements qui apparaissent à l'onglet Profil du compte de l'utilisateur.

37. Ces nouveaux renseignements clarifient un commentaire formulé précédemment par Facebook :

« Nous ne croyons pas qu'il y ait une différence d'ordre juridique entre l'information d'inscription et celle du profil, puisque ces renseignements sont fournis par la même personne à la même entité, aux fins générales mentionnées dans la Politique de confidentialité et indiquées à l'utilisateur par le fonctionnement du service » [traduction].

38. Il est à noter toutefois que Facebook ne mentionne aucunement, dans sa Politique de confidentialité ou ailleurs dans le site, qu'elle ne fait aucune distinction entre l'information d'inscription et celle du profil et que le masquage de la date de naissance du profil n'empêche pas l'utilisation de celle-ci à des fins de publicités ciblées. En fait, Facebook ne définit clairement nulle part ce qu'elle entend par « information du profil ».

Application

39. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.4*d*), 4.2.1, 4.2.3, 4.3, 4.3.2, 4.3.3 et 4.8, ainsi que le paragraphe 5(3).

40. Le principe 4.1.4*d*) stipule notamment que les organisations doivent assurer la mise en œuvre des politiques et pratiques destinées à donner suite aux principes, y compris la rédaction des documents explicatifs concernant leurs politiques et procédures.

41. Le principe 4.2.1 prévoit qu'une organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe 4.8 (transparence) et au principe 4.9 (accès aux renseignements personnels).

42. Le principe 4.2.3 établit notamment qu'il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils sont destinés.

43. Le principe 4.3 précise, entre autres, que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

44. Le principe 4.3.2, s'appuyant sur les notions de connaissance et de consentement énoncées au principe 4.3, stipule que les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. 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.

45. Le principe 4.3.3 prévoit qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

46. Le principe 4.8 précise qu'une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

47. Le paragraphe 5(3) établit qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Constatations

48. Dans la pratique, Facebook exige la date de naissance des utilisateurs aux fins :

1) d'appliquer la politique d'âge minimum requis du site afin de protéger la sécurité des mineurs;
2) d'assurer que les utilisateurs recourent à leur véritable identité sur le site afin de réduire l'incidence de contenu et de comportements inappropriés et de promouvoir un environnement sécuritaire et respectueux à l'endroit de tous les utilisateurs.

49. À mon avis, ces fins sont légitimes et appropriées aux termes du paragraphe 5(3); la collecte de la date de naissance est nécessaire à la réalisation de ces fins. Il est donc raisonnable que la prestation des services de Facebook soit conditionnelle à l'obtention de la date de naissance.

50. Néanmoins, puisque la *Loi* indique clairement que le consentement dépend de l'entendement des fins, et compte tenu du besoin accru de transparence relativement à la collecte et l'utilisation d'un renseignement personnel tant convoité par les voleurs d'identité, je suis préoccupée à l'idée qu'à certains égards, Facebook ne fait pas des efforts raisonnables, conformément au principe 4.3.2, pour documenter, préciser et expliquer les fins de la collecte de la date de naissance des utilisateurs.

51. Je trouve que l'énoncé des fins « assurer l'intégrité du site », tel qu'il apparaît dans la fenêtre contextuelle, est vague. Le principe 4.3.3 stipule que les fins doivent non seulement être légitimes, mais « explicitement indiquées ». Je doute que la phrase en question soit raisonnablement compréhensible pour l'utilisateur moyen de Facebook. Comme je considère que la notification en temps réel est le meilleur moyen d'informer les gens sur l'utilisation de leurs renseignements personnels dans un environnement en ligne, je vois d'un œil favorable que Facebook ait choisi la notification en temps réel par le biais d'une fenêtre contextuelle expliquant la collecte de la date de naissance. Toutefois, il me semble contre-productif de poser une question si claire pour ensuite fournir une réponse si vague. À mon avis, la phrase n'est pas assez claire, ni assez précise pour garantir la compréhension de l'utilisateur afin que ce dernier fasse des choix éclairés relativement au consentement, conformément au principe 4.3.

52. Je remarque que la fenêtre en question traite des fins pour lesquelles Facebook *demande* la date de naissance, mais elle ne donne aucune précision quant à d'autres fins de son utilisation — notamment la publicité ciblée selon l'âge. À mon avis, ayant adopté ce qu'ils qualifient eux-mêmes de « pratique exemplaire » relativement à la notification au moment de la collecte de la date de naissance, Facebook devrait tirer profit au maximum de cette pratique en

avisant les utilisateurs, au moment de l'inscription, de *toutes* les fins auxquelles la date de naissance servira.

53. La fenêtre contextuelle est le seul endroit du site qui fait mention spécifiquement de la date de naissance dans le contexte des fins de la collecte et de l'utilisation. Bien que la Politique de confidentialité aborde de façon générale les fins possibles à l'utilisation de l'information du profil, y compris la publicité ciblée, il n'est pas spécifiquement question de la date de naissance dans ce contexte. Puisque la date de naissance est un renseignement exigé qui sera utilisé à des fins essentielles ainsi qu'à d'autres fins, il serait nécessaire, à mon avis, de faire la distinction et d'expliquer clairement toutes les utilisations dans la Politique de confidentialité.

54. À défaut de documents présentant des définitions et des explications claires, Facebook fait en sorte que les utilisateurs risquent d'avoir l'impression qu'ils peuvent refuser de recevoir de la publicité ciblée selon l'âge. Facebook avise les utilisateurs qu'on pourrait utiliser l'information du profil à des fins de publicité ciblée ou pour des applications tierces, mais indique aussi qu'il est possible de « masquer » la date de naissance dans leur profil. À mon avis, les utilisateurs peuvent raisonnablement présumer que l'information du profil consiste en les renseignements apparaissant dans le profil et qu'en masquant la date de naissance dans le profil, celle-ci ne serait plus considérée comme de l'information de profil et, par conséquent, ne serait pas utilisée à des fins de publicité. Il appert cependant que « masquer » la date de naissance signifie simplement que les autres utilisateurs de Facebook ne le verront pas. Pour Facebook, une date de naissance « masquée » fait tout de même partie de l'information de profil et demeure accessible à des fins de publicité ciblée. Facebook se doit d'expliquer ce que signifie « information de profil » et de préciser que même si une date de naissance est masquée dans le profil, elle pourra tout de même être utilisée à des fins publicitaires. La publicité est abordée plus en détail à la section 3 du présent rapport.

55. En somme, en ce qui a trait à la collecte de la date de naissance, je constate que Facebook contrevient aux principes précités, notamment les principes 4.2.3 et 4.3.2.

Recommandations et réponse

56. Dans mon rapport préliminaire, je recommandais à Facebook :

    1) de revoir la phrase de la fenêtre contextuelle « pour assurer l'intégrité du

site » afin de mieux représenter la véritable fin et de la rendre plus compréhensible pour les utilisateurs;

2) de modifier sa Politique de confidentialité afin d'expliquer les raisons pour lesquelles la date de naissance est précisément exigée et les fins auxquelles elle est utilisée;

3) de revoir les documents du site, au besoin, y compris la fenêtre contextuelle de la page d'inscription, afin de définir clairement ce qu'elle entend par « information du profil » et de dissiper l'impression que masquer la date de naissance de son profil signifie qu'elle ne sera pas utilisée à des fins de publicités ciblées;

4) d'indiquer, dans la fenêtre contextuelle qui précise l'objectif de la collecte de la date de naissance, que celle-ci est également exigée à des fins de publicités ciblées; Facebook devrait également mentionner toute autre fin à laquelle elle prévoit utiliser ou communiquer la date de naissance des utilisateurs.

57. En réponse aux recommandations, Facebook a accepté de modifier le libellé dans la fenêtre contextuelle concernée comme suit :

« Facebook demande à tous les utilisateurs de fournir leur date de naissance réelle pour promouvoir l'authenticité et fournir un accès au contenu approprié selon l'âge. Vous pourrez masquer cette information si vous le souhaitez et son utilisation est régie par la Politique de confidentialité de Facebook » [traduction]

58. Facebook a également accepté d'apporter des modifications à la formulation de sa Politique de confidentialité relativement à l'utilisation des renseignements personnels à des fins publicitaires et a déclaré s'engager à « faire preuve de transparence en ce qui a trait à la collecte et l'utilisation de renseignements à des fins publicitaires » [traduction].

59. Facebook a indiqué que tout changement au libellé de sa Politique de confidentialité serait soumis aux utilisateurs pour une « période de préavis et de réception des commentaires ». Toutefois, indépendamment de l'assentiment des utilisateurs, le Commissariat s'attend à ce que Facebook respecte son engagement à satisfaire à ces recommandations.

Conclusion

60. Je suis confiante qu'une fois mises en œuvre, les mesures correctives que propose Facebook, telles que présentées ci-dessus, sauront satisfaire à nos

recommandations et permettront à Facebook de se conformer à la *Loi*. Aussi, je conclus que les allégations à cet effet sont fondées et résolues.

61. Nous effectuerons un suivi auprès de Facebook au sujet de la mise en œuvre de ces mesures dans les 30 jours suivant la présentation de ce rapport.

Section 2

Paramètres de confidentialité par défaut

Allégations

62. La CIPPIC a allégué que Facebook, en présélectionnant les paramètres de confidentialité par défaut, avait recours au consentement négatif pour utiliser et communiquer des renseignements personnels, et n'en respectait pas les exigences telles qu'établies par le Commissariat dans le cadre de conclusions précédentes. En particulier, la CIPPIC a invoqué que la majorité des renseignements personnels communiqués par les utilisateurs, y compris les photographies, l'état civil, l'âge et les passe-temps, sont de nature délicate et exigent un consentement explicite.

63. La CIPPIC a allégué également que Facebook, dans le contexte des paramètres de confidentialité, ne déployait pas d'efforts raisonnables pour s'assurer que les utilisateurs étaient informés des fins auxquelles les renseignements serviraient et la mesure dans laquelle ils seraient utilisés et communiqués. La CIPPIC a affirmé précisément ce qui suit :

- Facebook n'informe pas les utilisateurs de la mesure dans laquelle leurs renseignements personnels pourraient être communiqués conformément aux paramètres par défaut et, par conséquent, n'obtient pas leur consentement valable.
- Facebook ne dirige pas les utilisateurs vers les paramètres de confidentialité lorsque ces derniers s'inscrivent ou téléchargent des photographies, ou lorsque Facebook modifie les paramètres.
- Facebook n'avise pas les utilisateurs que ne pas modifier les paramètres par défaut signifie l'acceptation de ceux-ci.
- Facebook omet d'informer convenablement les utilisateurs qui publient des albums de photos que les paramètres de confidentialité par défaut de ces albums permettent de les communiquer à tout le monde, ce qui signifie qu'un autre utilisateur qui n'est pas un ami peut regarder les photographies et lire les commentaires qui s'y rapportent, même si le profil de l'utilisateur n'est accessible qu'à ses amis.
- Lorsque les utilisateurs deviennent membres d'un réseau, leurs paramètres de confidentialité par défaut permettent la communication de

renseignements personnels, y compris des renseignements de nature délicate, avec tous les membres du réseau.

Résumé de l'enquête

64. Facebook présélectionne les paramètres de confidentialité qui contrôlent la mesure dans laquelle d'autres personnes peuvent avoir accès aux renseignements d'un utilisateur et déterminent si les renseignements personnels sont accessibles au moyen de moteurs de recherche. Toutefois, les paramètres peuvent être modifiés par les utilisateurs selon leurs préférences. On doit noter que tous les paramètres auxquels on fait référence dans la présente section sont ceux applicables aux utilisateurs de 18 ans et plus.

65. Selon Facebook, la CIPPIC commet une erreur dans son interprétation des réglages de confidentialité en sous-entendant qu'ils se limitent aux paramètres de confidentialité alors qu'en fait, ils comprennent l'architecture d'amis et de réseaux. Dans ses observations au Commissariat, Facebook a présenté sa cause ainsi :

« Contrairement aux rapports généralement faits au grand public, les données du profil complet dans Facebook ne sont pas accessibles à tous les internautes. En fait, ils ne sont même pas accessibles à la plupart des utilisateurs de Facebook. [...] Les paramètres de confidentialité de Facebook jouent un rôle central en permettant aux utilisateurs de choisir qui a accès à leurs renseignements personnels, car ce sont eux qui décident d'accepter ou non des amis et de devenir membres d'un réseau. [...] En plus des restrictions de l'accès par défaut qui font partie de l'architecture de réseaux et d'amis, les utilisateurs disposent d'un pouvoir vaste et précis leur permettant de choisir qui voit quoi, parmi leurs amis et leurs réseaux, et ont à leur disposition des outils pour limiter les renseignements accessibles par les moteurs de recherche et d'autres entités externes » [traduction].

Par exemple, le partage d'information est différent selon le type de réseau. Dans les réseaux régionaux, les coordonnées ne sont pas considérées comme faisant partie du profil; elles ne sont donc pas communiquées aux utilisateurs du réseau. Toutefois, dans les réseaux d'universités, les coordonnées peuvent être échangées entre les utilisateurs qui possèdent une adresse de courriel de l'université. En outre, dans le cadre de l'architecture d'amis, les utilisateurs peuvent créer des listes d'amis qui ont divers degrés d'accès aux renseignements du profil.

66. Facebook estime qu'entre 20 % et 30 % des utilisateurs modifient leurs paramètres de confidentialité. L'entreprise a choisi les paramètres par défaut en fonction de ce qu'elle croyait que les utilisateurs souhaitaient. Dans ses observations au Commissariat, Facebook a déclaré : « Nous croyons que les utilisateurs devraient être encouragés à faire leurs propres choix à l'égard de la communication de leurs renseignements personnels. Nous facilitons ce choix en établissant des paramètres puissants qui reflètent le sens commun à l'égard de l'accessibilité et en permettant aux utilisateurs de les modifier s'ils le souhaitent » [traduction]. Selon Facebook, il ne serait pas pratique d'obliger les utilisateurs à choisir tous leurs paramètres de confidentialité avant l'acceptation de leur inscription. Le nombre élevé d'écrans à parcourir les dissuaderait de s'inscrire au service.

67. En réponse à l'allégation de la CIPPIC voulant que les utilisateurs ne soient pas dirigés vers les paramètres de confidentialité, Facebook précise qu'un lien vers ces derniers apparaît à chaque page du site. Bien que cela fût le cas au moment où la plainte a été déposée, le lien direct a disparu avec le lancement de la nouvelle interface de Facebook, à l'automne 2008. À l'heure actuelle, on retrouve un lien intitulé « Paramètres », que l'on doit faire dérouler pour consulter une série de liens subalternes, y compris un lien vers les paramètres de confidentialité.

68. Facebook fait remarquer ce qui suit :

> *« Une icône de sécurité apparaît un peu partout dans le site pour indiquer la présence de paramètres de confidentialité. Les "listes d'amis", ajoutées aux paramètres de confidentialité, permettent aux utilisateurs de configurer des sous-ensembles d'amis ayant accès à un contenu précis. [...] Les utilisateurs n'ont généralement aucun problème à trouver les paramètres de confidentialité et la CIPPIC n'a pas fourni la preuve du contraire »* [traduction].

69. Cette icône de sécurité est notamment présente lorsque les utilisateurs remplissent l'information du profil. Elle apparaît à droite de tous les champs de la section. Lorsqu'un utilisateur clique sur l'icône, une fenêtre contextuelle « Qui peut voir ces renseignements? » [traduction] s'ouvre; les paramètres par défaut y sont indiqués, et l'utilisateur peut les modifier au besoin à l'aide d'un menu déroulant. Facebook permet également aux utilisateurs de voir leur profil tel qu'il est vu par d'autres utilisateurs et, ainsi, de vérifier en temps réel les renseignements qui sont visibles pour les autres.

70. En ce qui concerne les albums de photos, Facebook présente automatiquement aux utilisateurs qui téléchargent des photos un écran où l'on

répond à la question « Qui peut voir ces renseignements? » [traduction]. Si les paramètres par défaut demeurent inchangés, la réponse est « Tout le monde ». En le faisant dérouler vers le bas, cet écran permet également de modifier facilement les paramètres de confidentialité.

71. Les utilisateurs sont en outre informés des paramètres de confidentialité dans la Politique de confidentialité de Facebook, qui commence ainsi :

« Facebook a été conçu pour faciliter l'échange de renseignements avec vos amis ainsi qu'avec les personnes de votre entourage. Vous ne voulez peut-être pas que le monde entier puisse consulter vos données personnelles; c'est pourquoi Facebook vous permet de contrôler l'accès à vos renseignements. Les paramètres de confidentialité par défaut restreignent l'accès de vos renseignements aux membres de vos réseaux; vos renseignements font également l'objet d'autres limites communautaires que nous jugeons raisonnables et dont nous vous faisons part.

« Facebook respecte deux principes fondamentaux :

a. Vous devez bénéficier du contrôle de vos renseignements personnels. Facebook vous permet de partager des renseignements avec vos amis et les personnes qui vous entourent. C'est vous qui décidez d'afficher ou non de l'information dans votre profil, notamment vos coordonnées et vos renseignements personnels, vos photos, vos intérêts et les groupes dont vous faites partie. En outre, vous pouvez choisir les utilisateurs avec qui vous partagerez ces informations à l'aide des paramètres de confidentialité sur la page Confidentialité.

b. Vous devez avoir accès à l'information que les autres utilisateurs souhaitent partager.
La quantité d'information disponible sur Facebook est en constante augmentation. Vous voulez sûrement savoir en quoi cette information vous concerne, ou concerne vos amis ou votre entourage. Nous souhaitons vous aider à trouver facilement cette information.

« Le partage de l'information devrait se faire facilement. Nous voulons vous fournir les outils de confidentialité nécessaires afin que vous puissiez contrôler comment et avec qui vous partagez cette information. Si vous avez des questions ou des idées, veuillez les faire parvenir à privacy@facebook.com » [traduction].

72. Sous le titre « Utilisation des renseignements obtenus par Facebook » [traduction], on peut lire ce qui suit dans la politique :

« L'information de votre profil est utilisée par Facebook essentiellement pour que vous puissiez y accéder et la modifier, ainsi que pour que les personnes autorisées puissent y accéder, conformément à vos paramètres de confidentialité. Si vos paramètres de confidentialité le permettent, les autres utilisateurs de Facebook pourront ajouter du contenu à votre profil (par exemple, en publiant des messages sur votre Mur).

« Les données de profil que vous transmettez à Facebook seront disponibles aux utilisateurs de Facebook qui sont membres d'au moins un des réseaux auxquels vous avez autorisé l'accès à vos renseignements dans vos paramètres de confidentialité (p. ex., école, emplacement géographique, amis de vos amis, etc.). Votre nom, les noms de vos réseaux et la vignette de votre profil seront disponibles dans les résultats des recherches sur le réseau Facebook. Ces données restreintes pourront également être accessibles à des moteurs de recherche tiers. Ainsi, vos amis pourront vous trouver et vous envoyer une invitation. Les personnes qui voient votre nom au cours d'une recherche ne pourront pas accéder aux renseignements de votre profil à moins d'avoir une relation avec vous (ami, ami d'un ami, membre de vos réseaux, etc.) qui leur donne accès à vos renseignements conformément à vos paramètres de confidentialité » [traduction].

73. Sous « Partage de données avec des tiers » [traduction], la politique indique ceci :

    « Facebook a pour objet le partage de renseignements avec d'autres — amis et personnes appartenant à vos réseaux — tout en vous permettant de définir des paramètres de confidentialité qui empêcheront d'autres utilisateurs d'avoir accès à vos données personnelles. Nous vous donnons l'occasion de choisir quels renseignements vous souhaitez transmettre par l'intermédiaire de Facebook à vos amis et à vos réseaux. Notre système de réseaux et vos paramètres de confidentialité vous permettent de choisir en toute connaissance de cause qui a accès à vos renseignements personnels » [traduction].

74. Au moment où la plainte a été déposée, les utilisateurs devaient indiquer qu'ils avaient lu la Politique de confidentialité et les Conditions d'utilisation et qu'ils les acceptaient. Les Conditions d'utilisation ont maintenant été remplacés par une Déclaration des droits et responsabilités, que les utilisateurs doivent accepter au moment de l'inscription.

75. Aux fins de la présente discussion au sujet des paramètres de confidentialité, nous tenons à souligner que les paramètres par défaut en vigueur au moment du dépôt de la plainte ne diffèrent pas de manière significative de ceux en

vigueur à l'heure actuelle. Tous les champs du profil sont réglés à « Mes réseaux et mes amis » pour les utilisateurs qui se sont joints à des réseaux et à « Mes amis seulement » pour les utilisateurs qui ne l'ont pas fait. Tous les champs de coordonnées sont réglés à « Mes amis seulement » (« Tous mes amis » dans version antérieure). Le champ des albums de photos est réglé à « Tout le monde », c'est-à-dire tous les utilisateurs de Facebook. (On doit noter que le 2 juin 2009, Facebook a annoncé sur son blogue qu'elle prenait des mesures afin d'éliminer les réseaux régionaux. Une fois que ce processus sera terminé, les réseaux régionaux n'apparaîtront plus dans les paramètres de confidentialité.)

76. Le réglage du champ « Inscription aux sites de recherche publics » [traduction] est particulièrement notable. Ce champ détermine si une quantité restreinte de renseignements au sujet de l'utilisateur (c.-à-d. nom, réseaux, vignette, amis) sera visible aux moteurs de recherche comme Google. Ce réglage consiste en une case à cocher en regard d'une seule option, soit « Créer pour moi une inscription aux sites de recherche publics et la soumettre à l'indexage des moteurs de recherche » [traduction]. Le paramètre par défaut de Facebook est de cocher cette case. Le champ « Inscription aux sites de recherche publics » et son réglage par défaut ne s'appliquent pas aux mineurs.

77. Au cours de l'inscription, les utilisateurs sont dirigés vers un processus en trois étapes qui leur permet notamment de « Retrouver des amis qui sont déjà sur Facebook ». À la troisième étape du processus, « Rejoignez un réseau », on demande aux utilisateurs d'entrer le nom de leur ville pour trouver un réseau. Sous ce champ, Facebook indique : « Vous pouvez accéder au profil d'autres personnes de votre réseau et elles peuvent voir le vôtre. Cette option peut être modifiée sur la page des paramètres de confidentialité. »

78. Il est à noter que ces étapes ne sont pas obligatoires et qu'un utilisateur n'est pas tenu de devenir membre d'un réseau. Selon Facebook, plus de la moitié des utilisateurs ne sont membres d'aucun réseau.

79. Si un utilisateur n'est membre d'aucun réseau, ses paramètres de confidentialité par défaut sont réglés pour des échanges avec « Seulement mes amis ». Toutefois, s'il se joint plus tard à un réseau pour la première fois, ses paramètres de confidentialité par défaut seront automatiquement modifiés, afin que les renseignements soient échangés avec les autres membres du réseau. Cependant, même si l'échange de renseignements avec les membres du réseau est précisé dans la Politique de confidentialité, l'utilisateur n'est pas avisé en temps réel au moment d'adhérer au réseau après s'être inscrit que les

autres membres du réseau seront en mesure de voir son profil ni que les paramètres de confidentialité d'origine ont été modifiés.

80. Quant à l'allégation relative au consentement, Facebook s'appuie une fois de plus sur la nature volontaire du téléchargement de données :

> *« Les utilisateurs de Facebook ne sont ni tenus ni obligés de fournir d'autres renseignements que leur nom, leur adresse de courriel, leur date de naissance et leur sexe. Lorsqu'ils font le choix de fournir ces données, ils le font dans le but de les communiquer avec d'autres. Ils se sont inscrits explicitement à Facebook et ont décidé de télécharger cette information. En fait, de nombreux utilisateurs ont lu les rapports erronés dans les médias, qui sont repris dans la plainte de la CIPPIC, selon lesquels les renseignements communiqués dans Facebook sont accessibles par tous les internautes, et ils ont néanmoins décidé de fournir ces renseignements »* [traduction].

81. Selon Facebook, les utilisateurs donnent leur consentement explicite en se servant volontairement du site pour partager des renseignements avec les autres. Cet objectif se reflète dans le slogan de Facebook, qui apparaît à la page d'accueil. Au moment du dépôt de la plainte, cette devise était *« Facebook est un utilitaire social qui vous relie à ceux qui comptent pour vous »* [traduction]. Actuellement, ce slogan est *« Facebook vous aide à garder contact avec les personnes de votre entourage »* [traduction], qui sous-tend la même philosophie.

Application

82. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.2.3, 4.3, 4.3.2 et 4.3.5.

83. Le principe 4.2.3 établit notamment qu'il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ces renseignements sont destinés.

84. Le principe 4.3 stipule, entre autres, que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

85. Le principe 4.3.2, s'appuyant sur le principe 4.3, mentionne qu'il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son

consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. 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.

86. Le principe 4.3.5 stipule notamment que, dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes.

Constatations

87. Il est digne de mention que Facebook fournit aux utilisateurs des paramètres de confidentialité très complets. Je considère que ces paramètres donnent suite aux principes de la *Loi* en permettant aux utilisateurs de contrôler l'échange de leurs renseignements. Toutefois, tel que mentionné ci-dessus, Facebook pourrait améliorer certains de ces paramètres.

88. Au sujet de l'allégation principale de la CIPPIC, j'insiste sur le fait que les circonstances en l'espèce sont très différentes de celles de cas passés pour lesquels le Commissariat a élaboré et formulé ses positions sur la question du consentement. Plus particulièrement, et contrairement aux personnes concernées dans des cas précédents, les utilisateurs de Facebook téléchargent leurs renseignements personnels vers le site de leur propre chef et volontairement aux fins expresses d'échange avec d'autres utilisateurs.

89. Dans de telles circonstances, le véritable enjeu n'est pas de faire la distinction entre le consentement actif et négatif au regard des paramètres de confidentialité par défaut. Idéalement, je préférerais qu'au moment de l'inscription, les paramètres ne soient pas présélectionnés et que les utilisateurs aient à les choisir eux-mêmes. Je reconnais tout de même qu'en raison du grand nombre de paramètres en jeu, la tâche de choisir chacun d'entre eux au moment de l'inscription pourrait dissuader d'éventuels utilisateurs d'interagir avec le site. Compte tenu de la nature du site, je ne serais pas opposée à ce que Facebook fasse une présélection des paramètres en autant que les paramètres par défaut soient raisonnables et que les utilisateurs en soient convenablement informés. À mon avis, les enjeux les plus importants dont il est question ici sont de savoir si les paramètres de confidentialité par défaut satisfont aux attentes raisonnables des utilisateurs de Facebook, conformément au principe 4.3.5, et si Facebook fait des efforts raisonnables pour respecter les principes 4.2.3 et 4.3.2 en informant les utilisateurs du mode

selon lequel leurs renseignements seront échangés en fonction des divers paramètres.

90. Pour ce qui est des attentes raisonnables, je remarque que la plupart des paramètres de confidentialité par défaut — notamment ceux associés aux champs du profil — sont réglés pour permettre l'échange de renseignements avec « Mes réseaux et mes amis ». Il est raisonnable que Facebook ait ainsi présélectionné les paramètres. Puisque la structure de Facebook repose sur la notion « d'amis », je trouve raisonnable de supposer que les utilisateurs s'attendent à ce que l'échange de leurs renseignements personnels ait lieu avec les personnes qui sont devenues leurs « amis » ainsi qu'avec les membres des réseaux auxquels ils se sont joints, surtout s'ils en sont avisés de façon adéquate.

91. Dans l'ensemble, je considère donc que Facebook a présélectionné des paramètres de confidentialité qui répondent aux attentes raisonnables des utilisateurs, sauf dans deux circonstances.

92. D'abord, en ce qui concerne les paramètres de l'album photos, Facebook a adopté une pratique louable pour son respect de la protection de la vie privée : les utilisateurs qui téléchargent des photos vers le site reçoivent systématiquement un avis précisant qui peut voir les photos et proposant des moyens faciles de modifier les paramètres de confidentialité s'ils le souhaitent. Cela ne semble toutefois pas concorder avec le réglage des paramètres de confidentialité par défaut à « Tout le monde ».

93. Facebook prétend que plusieurs utilisateurs souhaitent en effet que tout le monde ait accès à leurs photos. Il me semble impossible que les mêmes utilisateurs qui s'attendent à échanger de l'information uniquement avec leurs amis et les membres de leurs réseaux dans la plupart des autres cas aient soudainement des attentes beaucoup plus générales quand il est question de l'album photos. En somme, je trouve que régler les paramètres de l'album photos à « Tout le monde » est incohérent par rapport aux autres paramètres par défaut.

94. Deuxièmement, je remarque que les paramètres de confidentialité par défaut pour le champ « Recherche » font en sorte que tous les utilisateurs (à l'exception des mineurs) sont accessibles via les moteurs de recherche. Cela me paraît tout autant contradictoire aux attentes raisonnables des utilisateurs. Facebook prétend, comme c'était le cas pour les albums photos, que plusieurs utilisateurs souhaitent qu'on puisse les trouver via les moteurs de recherche —

mais n'a fourni aucune preuve à cet effet. Facebook avance que les utilisateurs considèrent qu'ils forment une communauté. Selon moi, chaque utilisateur devrait pouvoir décider si ses renseignements seront accessibles à l'extérieur de cette communauté.

95. En somme, je conclus que les paramètres par défaut de Facebook pour les albums photos et les moteurs de recherche ne répondent pas aux attentes raisonnables des utilisateurs aux termes du principe 4.3.5.

96. Enfin, j'avancerai que Facebook ne prend pas de mesures suffisantes pour informer les utilisateurs, au moment de l'inscription, des paramètres de confidentialité. Les pages relatives à l'inscription ne renferment aucun lien direct aux paramètres de confidentialité, pas de message clair sur ces paramètres ni le fait que Facebook les a présélectionnés par défaut et qu'ils peuvent être modifiés. Il y a un lien direct à la Politique de confidentialité et je considère que l'explication qu'on y fournit est convenable. Il est aussi digne de mention que Facebook utilise des icônes de sécurité et des fenêtres contextuelles « Qui peut voir ces renseignements? » pour l'information du profil. Toutefois, comme Facebook a présélectionné les paramètres de confidentialité, et que plusieurs nouveaux utilisateurs, au moment de l'inscription, risquent de ne pas bien connaître la notion de paramètres de confidentialité et d'ignorer qu'ils peuvent exercer un contrôle sur l'échange de leurs renseignements personnels sur Facebook, je juge que ces mesures seules ne constituent pas un avis adéquat dans les circonstances.

97. Quant à savoir si Facebook fait des efforts raisonnables pour informer les utilisateurs de l'accessibilité de leurs renseignements en fonction des divers paramètres, on note une différence en termes de notification pour les utilisateurs qui se joignent à un réseau dès l'inscription et ceux qui le font ultérieurement. Ceux qui se joignent à un réseau dès l'inscription reçoivent automatiquement un message indiquant que les membres de leur réseau ont accès à l'information de leur profil. En fournissant ce message, Facebook agit avec justesse — c'est exactement le type de notification qu'il faut dans cette situation. Par contre, les utilisateurs qui se joignent à un réseau un certain temps après leur inscription au site ne reçoivent pas un tel message. Selon moi, pour ce qui est de la notification, Facebook devrait agir identiquement envers tous ceux qui se joignent à un réseau, peu importe le moment où ils le font.

98. En somme, je constate dans les circonstances que les efforts de Facebook relativement à la notification au sujet des paramètres de confidentialité ne

satisfont pas au critère raisonnable, tel que le prévoit les principes 4.2.3 et 4.3.2. Plus particulièrement, Facebook doit faire en sorte que les nouveaux utilisateurs puissent prendre des décisions éclairées quant à l'accès à leurs renseignements personnels et ce, dès le moment de l'inscription. Facebook offre aux utilisateurs des outils pour qu'ils puissent exercer un contrôle sur leurs renseignements personnels; Facebook doit maintenant s'assurer que les utilisateurs comprennent ces outils.

Recommandations et réponse

99. Dans mon rapport préliminaire, je recommandais à Facebook :

    1) de rendre les profils des utilisateurs inaccessibles par défaut aux moteurs de recherche;

    2) de remplacer les paramètres par défaut des albums de photos par « Mes réseaux et mes amis »;

    3) de fournir un lien vers les paramètres de confidentialité au moment de l'inscription et des moyens d'informer les utilisateurs de la signification de « paramètres de confidentialité » ainsi que des mécanismes leur permettant de poser des questions à cet égard; en outre, les utilisateurs devraient être avisés que Facebook a réglé ces paramètres par défaut et qu'ils peuvent être modifiés selon les préférences des utilisateurs;

    4) d'aviser les utilisateurs qui adhèrent à un réseau *après* l'inscription de la même façon que ceux qui en deviennent membre *au moment* de l'inscription.

100. En réponse, Facebook a adopté une approche globale face aux préoccupations que le Commissariat entretient par rapport aux paramètres de confidentialité. L'entreprise prévoit mettre en œuvre prochainement deux modifications importantes :

    1) Intégrer un « assistant » pour les questions de protection de la vie privée qui permettra aux utilisateurs de choisir le niveau des paramètres : faible, moyen ou élevé. Cette sélection réglera d'autres paramètres plus détaillés par défaut. Par exemple, les utilisateurs qui choisiront le niveau « élevé » seront exclus des listes de recherche publique. Facebook soutient qu'avec le nouvel « assistant » et en insistant sur le mode de protection de la vie privée par objet (ci-après), elle garantira que les utilisateurs auront fait un choix éclairé quand à l'accessibilité de leurs renseignements via les

moteurs de recherche.

2) Mettre en œuvre un outil de confidentialité par objet qui offrira aux utilisateurs « des paramètres faciles à configurer pour chaque élément de contenu; ils pourront les configurer au moment du téléchargement ou lors de tout échange. En l'espace de quelques semaines, les modifications qui sont présentement mises à l'essai permettront aux utilisateurs de régler les paramètres de confidentialité pour chaque photo et chaque élément de contenu tel que la mise à jour du statut » [traduction]. Le Commissariat en déduit que Facebook prévoit élargir la portée de ses pratiques de notification relatives aux albums photos à d'autres types de renseignements.

101. Facebook a également indiqué qu'elle effectuait des tests préliminaires sur une nouvelle procédure d'inscription qui fournira plus d'information sur les paramètres de confidentialité.

102. Quant à la quatrième recommandation, Facebook a accepté de mettre en œuvre les mesures adéquates.

Conclusion

103. Je suis confiante qu'une fois mises en œuvre, les mesures correctives que propose Facebook, telles que présentées ci-dessus, sauront satisfaire à nos recommandations et permettront à Facebook de se conformer à la *Loi*. Aussi, je conclus que les allégations à cet effet sont fondées et résolues.

104. Nous effectuerons un suivi auprès de Facebook au sujet de la mise en œuvre de ces mesures dans les 30 jours.

Section 3

Publicités de Facebook

Allégations

105. La CIPPIC a allégué que Facebook :

1) ne faisait pas d'efforts raisonnables pour s'assurer que les utilisateurs étaient informés que leurs renseignements personnels serviraient à des fins publicitaires, en dérogation au principe 4.3.2;

2) en ce qui concerne les publicités sociales en particulier, avait recours de façon inappropriée au consentement implicite plutôt qu'au consentement explicite conforme au principe 4.3.6, étant donné la nature délicate des renseignements personnels des utilisateurs;

3) ne permettait pas aux utilisateurs de retirer leur consentement aux publicités Facebook, en dérogation au principe 4.3.8;

4) puisque les utilisateurs n'étaient pas autorisés à retirer leur consentement aux publicités Facebook, demandait sans raison valable de consentir à ces publicités pour obtenir le service, en dérogation au principe 4.3.3.

106. En ce qui concerne la première allégation, la CIPPIC a fait remarquer que, même si la Politique de confidentialité de Facebook mentionnait effectivement que les renseignements personnels pouvaient être utilisés dans les publicités sociales, l'avertissement était insuffisant, car, en raison de leur profil démographique, de nombreux utilisateurs n'étaient pas en mesure de comprendre « le jargon juridique et le libellé complexe de la Politique de confidentialité » [traduction]. Selon la CIPPIC, si le consentement implicite devait s'appliquer, l'avertissement devrait être particulièrement clair.

Résumé de l'enquête

107. Les publicités Facebook ciblent des profils démographiques ou des mots clés du profil des utilisateurs. Par exemple, une femme dans la quarantaine pourrait voir une publicité sur des crèmes de rajeunissement.

108. Les publicités sociales tiennent compte des interactions sociales plutôt que des mots apparaissant dans le profil, par exemple, devenir fan d'une page, joindre un groupe ou faire une activité qui serait publiée dans les Actualités. Par

exemple, si un utilisateur devient fan d'un certain restaurant, cette activité apparaîtra dans les Actualités de ses amis. Si le restaurant achète de la publicité dans Facebook, l'annonce dans les Actualités serait accompagnée d'une publicité comprenant le nom de l'utilisateur et sa vignette (s'il en a publié une).

109. Facebook admet d'emblée que les revenus publicitaires lui permettent d'offrir son service gratuitement. Dans ses observations écrites au Commissariat, elle a déclaré ce qui suit :

« Facebook tient à être transparente quant au fait que la publicité constitue une importante source de revenus et à expliquer entièrement aux utilisateurs le type d'utilisation de leurs renseignements personnels qu'ils autorisent en se servant de Facebook afin d'offrir des publicités pertinentes et personnalisées. [...] La Politique de confidentialité et, surtout, les expériences des utilisateurs, informent ces utilisateurs sur le fonctionnement des publicités, qui permettent à Facebook d'offrir ses services gratuitement et qui ciblent des aspects exprimés dans un profil. Ces publicités sont présentées dans l'espace publicitaire de la page et les annonceurs n'ont pas accès aux profils individuels des utilisateurs » [traduction].

110. Dans la Politique de confidentialité de Facebook, on peut lire ce qui suit :

« Facebook peut utiliser les données de votre profil sans vous identifier personnellement auprès de tiers. Ces données nous permettent notamment d'estimer le nombre de personnes au sein de votre réseau qui aiment telle formation musicale ou tel film, ou encore de personnaliser nos publicités et nos promotions, ce qui nous permet de vous offrir gratuitement Facebook. Nous pensons que c'est à votre avantage. En effet, vous en apprendrez plus sur ceux et celles qui vous entourent et les publicités éventuelles seront ainsi plus ciblées et davantage susceptibles de vous intéresser. À titre d'exemple, si vous indiquez votre film préféré dans votre profil, nous pourrions vous proposer l'affiche ou la bande-annonce d'un film similaire présenté dans votre ville. Cependant, nous ne communiquons pas vos données à la société de distribution » [traduction].

111. Facebook a confirmé que la politique décrite ci-dessus, soit de ne pas communiquer de renseignements personnels aux annonceurs, s'appliquait autant aux publicités sociales qu'aux publicités Facebook. Dans les deux cas, les annonceurs qui achètent des publicités ne reçoivent pas les renseignements personnels des utilisateurs. Ils reçoivent cependant la

confirmation de Facebook du nombre de fois où une publicité a été présentée et du nombre d'utilisateurs qui ont cliqué sur la publicité.

Publicités Facebook

112. Quant aux publicités Facebook en particulier, Facebook résume ainsi sa position :

« Nous ne croyons pas que la diffusion d'une publicité, lorsque l'annonceur n'a accès qu'au nombre de personnes associées à un mot-clé fondé sur des données groupées non liées à des renseignements personnels, peut raisonnablement être interprétée comme un usage de renseignements personnels contraire à la LPRPDE. La Politique de confidentialité indique explicitement aux utilisateurs que leurs renseignements personnels seront utilisés de cette façon et présente des exemples afin de dissiper toute éventuelle confusion. Étant informés, ils continuent d'utiliser le site et de voir des publicités sur chaque page. Un utilisateur peut en tout temps désactiver ou supprimer son compte, mettant ainsi fin à l'utilisation potentielle de ses renseignements » [traduction].

113. Facebook a également confirmé qu'elle n'autorisait pas aux annonceurs l'accès aux renseignements personnels téléchargés par les utilisateurs. Selon l'entreprise, dans le cas des publicités de Facebook, à moins qu'un utilisateur ne décide librement de communiquer ses renseignements à un annonceur (dans le cadre d'un concours, par exemple), « les annonceurs peuvent uniquement cibler des publicités sur des attributs non personnels d'un utilisateur tirés de son profil ». Dans la section Aide du site, Facebook explique ce qui suit, dans le contexte des publicités de Facebook :

« Ces attributs sont basés sur les intérêts, les activités, ainsi que les livres, séries télé, films ou professions préférés que les utilisateurs ont indiqués dans leur profil Facebook. Par exemple, si vous choisissez de cibler les mots-clés "Dave Matthews Band", votre publicité sera alors affichée uniquement sur les comptes des utilisateurs ayant inclus Dave Matthews Band dans la section "Style de musique" de leur profil » [traduction].

114. Tous les utilisateurs reçoivent des publicités de Facebook, et il n'y a aucune façon de les désactiver.

115. Facebook explique que les annonceurs qui achètent des publicités de Facebook précisent les caractéristiques des utilisateurs cibles. Facebook

garantit que les publicités n'apparaîtront qu'aux utilisateurs répondant à ces caractéristiques et offre aux annonceurs des statistiques telles que le nombre de publicités diffusées et le nombre de personnes ayant cliqué sur les publicités.

116. La plupart des publicités sont présentées par Facebook, mais des tiers peuvent également diffuser des publicités dans le cadre de leur réseau publicitaire. Au Canada, Microsoft est l'annonceur tiers exclusif de Facebook. Dans sa Politique de confidentialité, Facebook aborde ainsi le sujet :

« Les publicités qui apparaissent sur Facebook sont souvent diffusées directement aux utilisateurs par des annonceurs tiers. Dans ce cas, ils reçoivent automatiquement votre adresse IP. Ces annonceurs tiers peuvent aussi télécharger des cookies vers votre ordinateur ou utiliser d'autres technologies comme JavaScript et les "balises Web" (aussi connues sous le nom de "1x1 gifs") pour évaluer l'efficacité de leurs publicités et personnaliser leurs contenus » [traduction].

Publicités sociales

117. En ce qui a trait aux publicités sociales, Facebook fait remarquer que les annonceurs paient pour promouvoir certaines interactions des utilisateurs auprès de leurs amis. En outre, elle affirme qu'aucune publicité sociale n'est produite si un utilisateur n'a pas effectué une activité précise, par exemple, soutenir un politicien. Les publicités sociales ne sont diffusées qu'aux amis confirmés. Selon Facebook, les annonceurs n'achètent pas les données personnelles des utilisateurs et n'y ont pas accès. L'entreprise leur dit uniquement le nombre d'utilisateurs ayant fait certaines activités et le nombre de publicités produites par ces activités.

118. Les utilisateurs peuvent choisir, grâce aux paramètres de confidentialité, quelles activités apparaîtront dans les Actualités de leurs amis et, par conséquent, quels renseignements personnels seront utilisés dans les publicités sociales. En outre, ils peuvent refuser de recevoir des publicités sociales en modifiant les paramètres de confidentialité.

119. Au moment de la plainte, les caractéristiques en question s'appelaient « Actualités » et « Mini-actualités », et les paramètres par défaut étaient réglés à « Seulement mes amis ». Dans la dernière version de Facebook, ces caractéristiques s'appellent « Actualités » et « Mur », et les paramètres par défaut sont toujours réglés à « Seulement mes amis ».

120. Dans la section Aide, Facebook explique ainsi les publicités sociales :

« Comment les publicités se retrouvent-elles dans les Actualités?

« Les publicités qui s'affichent dans vos Actualités sont appelées publicités sociales. Les publicités sociales peuvent prendre la forme d'une seule publicité ou combiner une publicité et les actions de vos amis associées à cette publicité. Les publicités sociales descendent progressivement d'un niveau dans vos Actualités comme tout autre type d'actualité. Facebook s'engage à vous offrir un environnement sobre et lisible pour dialoguer et échanger avec vos amis. Notre objectif consiste à ne vous présenter que des publicités utiles et non importunes dont nous nous efforçons continuellement d'accroître la pertinence. Les publicités sociales combinent des informations associées concernant vos amis et des publicités conçues pour vous aider à personnaliser le contenu publicitaire que vous voyez s'afficher en fonction de vos centres d'intérêt et de ceux de vos amis.

« Pourquoi une action que j'ai effectuée apparaît-elle avec une publicité?

« Nous estimons que les publicités peuvent vous procurer divers avantages et qu'elles contribuent à améliorer votre utilisation de Facebook. Les publicités sociales, qui peuvent apparaître dans les Actualités ou dans l'espace publicitaire situé à gauche de l'écran, présentent désormais des publicités ainsi que des informations associées concernant vos amis. Si vous avez effectué une action associée à une Page ou à une application appartenant à un annonceur, cette action est considérée comme une action sociale pouvant apparaître accompagnée d'une publicité. Les publicités sociales n'englobent que les actions dont vous avez autorisé la publication dans vos Actualités par l'intermédiaire des paramètres de confidentialité que vous avez définis pour vos Actualités. En outre, les annonceurs ne peuvent en aucun cas visualiser les actions publiées avec l'une de leurs publicités. Les informations associées sont uniquement destinées à vous permettre de personnaliser le contenu publicitaire en fonction de vos centres d'intérêt et de ceux de vos amis pour que vous n'obteniez que des publicités utiles et instructives » [traduction].

121. Au sujet du consentement, Facebook affirme qu'aucune publicité sociale ne serait produite à moins qu'un utilisateur effectue une activité précise publiée dans les Actualités d'un ami. Selon Facebook, il s'agit d'un consentement en temps réel de la part de l'utilisateur.

122. La nouvelle Déclaration des droits et responsabilités, qui est venue remplacer récemment les Conditions d'utilisation de Facebook, comprend deux sections

au sujet de la publicité — une à l'intention des utilisateurs et une autre à l'intention des annonceurs. La section destinée aux utilisateurs, intitulée « Au sujet des publicités sur Facebook » [traduction], se lit comme suit :

« Notre objectif est de présenter des publicités qui soient utiles tant pour les annonceurs que pour vous. À cette fin, vous acceptez ce qui suit :

« 1. Vous pouvez restreindre la manière dont votre nom et votre photo de profil peuvent être associés à du contenu commercial ou commandité en vous servant des paramètres de confidentialité. Vous nous donnez le droit d'utiliser votre nom et votre photo de profil en regard de ce contenu, selon les limites que vous aurez établies.

« 2. Nous ne partageons pas vos données avec les annonceurs.

« 3. Vous reconnaissez que nous ne désignons pas nécessairement comme tels les services et communications payants » [traduction].

Application

123. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.4*d*), 4.2.1, 4.2.3, 4.3.2, 4.3.3 et 4.8.

124. Le principe 4.1.4*d*) stipule notamment que les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris, notamment, la rédaction des documents explicatifs concernant leurs politiques et procédures.

125. Le principe 4.2.1 prévoit qu'une organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe 4.8 (transparence) et au principe 4.9 (accès aux renseignements personnels).

126. Le principe 4.2.3 établit notamment qu'il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils sont destinés.

127. Le principe 4.3.2, s'appuyant sur le principe 4.3 qui exige l'avis et le consentement, mentionne que les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles

les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

128. Le principe 4.3.3 stipule qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

129. Le principe 4.8 précise qu'une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

Constatations

130. Dans le passé, lorsqu'il était question de marketing, le Commissariat faisait toujours la distinction entre les fins premières et secondaires. Les fins premières sont celles essentielles à la prestation d'un service. Les fins secondaires sont celles qui ne visaient pas les renseignements au moment de leur collecte initiale. Dans les cas étudiés auparavant où il était question de publicité, on considérait souvent que cette dernière constituait une fin secondaire — dans certaines circonstances, les utilisateurs pouvaient choisir d'en être exclus.

131. Le modèle organisationnel de Facebook est différent de ceux des organisations sur lesquelles nous nous sommes penchés jusqu'à maintenant. Si le site est gratuit pour les utilisateurs, il ne l'est pas pour Facebook qui a besoin de revenus publicitaires afin de fournir le service. De ce point de vue, la publicité est essentielle à la prestation de ce service. Ceux et celles qui souhaitent utiliser le service doivent donc accepter de recevoir une certaine quantité de publicité.

132. La plainte actuelle concerne deux types de publicité entraînant l'utilisation de renseignements personnels — l'utilisateur doit consentir à l'un d'eux en vue d'utiliser le site (les publicités Facebook), mais peut refuser l'autre (les publicités sociales). Pour ce qui est de la publicité Facebook, je suis satisfaite que Facebook remet l'information aux publicitaires sous forme agrégée — il n'y a donc pas de *communication* de renseignements personnels aux publicitaires.

Cependant, il ne fait aucun doute que d'accéder aux caractéristiques des utilisateurs via leur profil, agréger les données et envoyer des publicités aux utilisateurs constituent des *utilisations* de renseignements personnels aux termes de la *Loi*.

133. Des deux types de publicité ciblée en cause, la publicité sociale m'apparaît plus problématique parce qu'elle est intrusive par essence. La publicité sociale se sert des actions des personnes, des vignettes et des noms pour promouvoir un produit ou un service particulier. La publicité s'intègre alors aux Actualités et s'entremêle aux interactions normales de l'utilisateur et de ses amis. De fait, la publicité sociale fait en sorte que l'utilisateur semble souscrire au produit. C'est pourquoi les utilisateurs ne s'attendent pas à ce que leurs renseignements soient utilisés ainsi; ils doivent pouvoir, comme c'est actuellement le cas, refuser que leurs renseignements personnels soient utilisés ainsi.

134. En comparaison, la publicité Facebook porte moins atteinte à la vie privée. Seul l'utilisateur peut voir les publicités qu'on lui envoie et il ne souscrit pas à un produit par cooptation. Nous reconnaissons le besoin de Facebook de générer des revenus et la plupart des utilisateurs s'attendent raisonnablement à recevoir de la publicité. Devant la « gratuité » du service de réseautage social qu'offre Facebook, je trouve raisonnable qu'on oblige les utilisateurs à consentir à la publicité Facebook comme condition de service.

135. La question est de déterminer si les fins publicitaires sont « explicitement indiquées » en vertu du principe 4.3.3 et de savoir si Facebook fait des efforts raisonnables, en vertu du principe 4.2.3, pour informer les utilisateurs de ces fins.

136. D'abord, en considération des principes 4.1.4*d)*, 4.2.1, 4.3.2, et 4.8, je suis préoccupée à l'idée que, eu égard au rôle essentiel et prédominant que la publicité joue dans les activités de Facebook, Facebook ne fasse pas d'efforts raisonnables pour documenter et expliquer, dans sa Politique de confidentialité, son usage de la publicité, l'utilisation des renseignements des utilisateurs à des fins de publicité ciblée et la mesure dans laquelle les utilisateurs peuvent refuser de recevoir de la publicité sociale. À l'encontre de la CIPPIC, je ne trouve pas que la Politique de confidentialité de Facebook est marquée par le « jargon juridique et un libellé complexe ». Je constate toutefois que les activités reliées à la publicité ne sont pas expliquées suffisamment en détail. La Politique parle notamment de la publicité ciblée de manière générale et n'explique pas la différence entre la publicité Facebook et la publicité sociale.

Elle ne précise pas non plus que les utilisateurs peuvent refuser la publicité sociale, mais pas la publicité Facebook.

137. Je reconnais que la section Aide de Facebook explique plus en détail et plus utilement les activités reliées à la publicité, et que la nouvelle Déclaration des droits et responsabilités informe les utilisateurs qu'ils peuvent recourir aux paramètres de confidentialité pour limiter l'utilisation de renseignements personnels à des fins de publicité sociale. Je considère cependant que par souci de commodité, l'information relative à la protection de la vie privée, surtout l'information portant sur les fins de la collecte et de l'utilisation des renseignements personnels, devrait être rassemblée et expliquée intégralement dans la politique de confidentialité d'une organisation.

138. En somme, en matière de documentation et d'explication des fins relatives à la publicité, je constate que Facebook ne respecte pas des normes raisonnables en l'espèce, tel que le prévoient les principes 4.1.4*d)*, 4.2.1, 4.3.2 et 4.8.

139. Deuxièmement, en considération des principes 4.2.3 et 4.3.2, je suis préoccupée à l'idée qu'au moment du dépôt de la plainte, Facebook n'avisait pas de façon adéquate les utilisateurs, au moment de la collecte des renseignements, de l'utilisation de ceux-ci à des fins publicitaires. J'indiquais dans mon rapport préliminaire que Facebook devait faire en sorte que les nouveaux utilisateurs — au moment de remplir leur page de profil ou de télécharger de l'information vers le site — comprennent immédiatement les implications de ces gestes de façon à prendre des décisions éclairées. Compte tenu du rôle essentiel et prédominant de la publicité dans les activités de Facebook, et compte tenu que la publicité Facebook constitue une condition de service, je considère que Facebook doit faire preuve de plus de transparence à l'endroit des utilisateurs en ce qui a trait à ses pratiques publicitaires.

Recommandations et réponse

140. Dans mon rapport préliminaire, je recommandais à Facebook :

1) d'étoffer la section de la Politique de confidentialité sur la publicité de façon à :
   i) mieux expliquer le rôle des publicités dans Facebook ainsi que les différences entre les publicités sociales et les publicités Facebook, notamment en ce qui concerne les possibilités de retrait;
   ii) informer les utilisateurs que l'information du profil sert à des fins de

publicités ciblées, de l'impossibilité de refuser les publicités de Facebook et de la façon de se retirer des publicités sociales;

2) dans l'onglet Profil et ailleurs où le téléchargement d'information risque de produire une publicité sociale ou de Facebook,

i) de rappeler aux utilisateurs que les renseignements personnels qu'ils téléchargent sont recueillis, utilisés et communiqués conformément à la Politique de confidentialité de Facebook;

ii) de fournir un lien qui dirigera les utilisateurs vers la section étoffée sur la publicité de la Politique de confidentialité, tel qu'il est recommandé ci-dessus.

141. À la suite de ces recommandations, Facebook a accepté en principe de décrire plus clairement les activités reliées à la publicité dans sa Politique de confidentialité. Plus particulièrement, l'entreprise a déclaré ce qui suit :

« Une description plus détaillée du système global de publicité de Facebook est en cours d'élaboration, puisque le mode de déploiement de la publicité sur Facebook évolue. Nous nous engageons à expliquer la différence entre la publicité sociale et d'autres formes de publicité sur Facebook et à faire preuve de transparence en ce qui a trait à la collecte et à l'utilisation des renseignements à des fins publicitaires » [traduction].

142. Facebook s'est opposé en principe à la recommandation 2 ci-dessus, sous prétexte qu'elle ne voulait pas perturber l'expérience des utilisateurs avec des avis qui créeraient des interruptions. Néanmoins, l'entreprise a accepté de configurer ses systèmes de façon à « permettre aux utilisateurs qui se soucient particulièrement de la protection de la vie privée d'en apprendre facilement davantage sur les opérations du site et de faire part à Facebook de leur rétroaction et de leurs préoccupations » [traduction].

143. Facebook a indiqué que tout changement au libellé de sa Politique de confidentialité serait soumis aux utilisateurs pour une « période de préavis et de réception des commentaires ». Toutefois, indépendamment de l'assentiment des utilisateurs, le Commissariat s'attend à ce que Facebook respecte son engagement à satisfaire à ces recommandations.

Conclusion

144. Je suis confiante qu'une fois mises en œuvre, les mesures correctives que propose Facebook, telles que présentées ci-dessus, sauront satisfaire à nos

recommandations et permettront à Facebook de se conformer à la *Loi*. Aussi, je conclus que les allégations à cet effet sont fondées et résolues.

145. Nous effectuerons un suivi auprès de Facebook au sujet de la mise en œuvre de ces mesures dans les 30 jours.

Section 4

Applications de tiers

Allégations

146. La CIPPIC a allégué que Facebook :

1) n'informait pas les utilisateurs des raisons pour lesquelles elle communiquait leurs renseignements personnels aux tiers développeurs d'applications, en dérogation aux principes 4.2.2 et 4.2.5;

2) permettait aux tiers développeurs d'applications d'accéder à des renseignements personnels au-delà de ce qui est nécessaire pour les besoins de l'application, en dérogation au principe 4.4.1;

3) exigeait que les utilisateurs acceptent de communiquer des renseignements personnels au-delà de ce qui est nécessaire pour le fonctionnement de l'application, en dérogation au principe 4.3.3;

4) n'avisait pas les utilisateurs des conséquences liées au retrait de leur consentement à communiquer des renseignements personnels aux tiers développeurs d'applications, en dérogation au principe 4.3.8;

5) permettait aux tiers développeurs d'applications de conserver les renseignements personnels de l'utilisateur après la suppression de l'application par l'utilisateur, en dérogation au principe 4.5.3;

6) permettait aux tiers développeurs d'accéder aux renseignements personnels d'utilisateurs dont les amis ou les membres de leurs réseaux ajoutaient une application sans les en aviser adéquatement, en dérogation au principe 4.3.2;

7) ne protégeait pas adéquatement les renseignements personnels, car elle ne surveillait ni la qualité ni la légitimité des applications de tiers ni ne prenait les mesures indiquées contre les vulnérabilités inhérentes de nombreuses applications sur la Plateforme Facebook, en dérogation au principe 4.7;

8) n'avisait pas efficacement les utilisateurs de la portée des renseignements personnels communiqués aux tiers développeurs d'applications et fournissait aux utilisateurs de l'information trompeuse ou imprécise sur le partage avec les tiers développeurs d'applications, en dérogation aux principes 4.3 et 4.8;

9) n’assumait aucune responsabilité quant aux renseignements personnels transmis aux tiers développeurs aux fins de traitement, en dérogation au principe 4.1.3;

10) ne permettait pas aux utilisateurs de refuser de communiquer leurs nom, réseaux et listes d’amis lorsque leurs amis ajoutaient une application, en dérogation au principe 4.3 et au paragraphe 5(3).

Résumé de l’enquête

147. Depuis mai 2007, Facebook fournit à des tiers une plateforme (la Plateforme Facebook) qui leur permet de créer au sein de Facebook des applications que les utilisateurs peuvent ajouter à leur compte. Ces applications, parmi lesquelles on retrouve des jeux, des questionnaires, des horoscopes et des petites annonces, ont accès à la base de données de Facebook, mais sont hébergées par les serveurs des développeurs.

148. Selon le blogue de Facebook (entrée du 4 juin 2009) :

> *« La croissance que nous avons observée sur la Plateforme a été formidable. Il y a aujourd’hui plus de 350 000 applications courantes sur la Plateforme, attribuables à plus de 950 000 développeurs provenant de plus de 180 pays. On y retrouve tant des utilisateurs ayant conçu des applications simples qu’ils veulent partager avec leurs amis que des entreprises de grande envergure qui comptent des centaines d’employés, touchent des dizaines de milliers d’utilisateurs chaque mois et ont des revenus dans les dizaines de milliers de dollars. Par exemple, près de 10 000 applications ont 10 000 utilisateurs mensuels actifs et plus, et plus de 100 applications ont plus d’un million d’utilisateurs mensuels actifs »* [traduction].

149. Lorsque les utilisateurs ajoutent une application, ils doivent donner leur consentement pour que les tiers développeurs puissent accéder à leurs renseignements personnels ainsi qu’à ceux de leurs amis. En outre, comme la CIPPIC l’a bien indiqué, à moins que les utilisateurs ne retirent toutes les applications et bloquent des applications précises, ils n’ont pas la possibilité de refuser de communiquer leurs nom, réseaux ou listes d’amis lorsque des amis ajoutent des applications.

150. Depuis que la CIPPIC a déposé sa plainte le 30 mai 2008, Facebook a modifié les écrans qui apparaissent lorsque les utilisateurs ajoutent des applications.

151. Au moment du dépôt de la plainte, les utilisateurs qui ajoutaient une application étaient tenus de permettre aux tiers développeurs d'applications de « savoir qui je suis et accéder à mes informations » [traduction]. La version actuelle de l'écran en question informe les utilisateurs que « le fait d'attribuer un accès à [*nom de l'application*] lui permettra d'accéder aux renseignements de votre profil, à vos photos, aux informations sur vos amis et à tout autre contenu nécessaire à son fonctionnement. […] En continuant, vous autorisez [*nom de l'application*] à accéder à vos renseignements » [traduction]. Dans la version antérieure, on avisait aux utilisateurs qu'ils acceptaient les Conditions de service des utilisateurs de la Plateforme Facebook et on leur fournissait un lien vers celles-ci. Dans la version actuelle, on avise les utilisateurs qu'ils acceptent les Conditions d'utilisation de Facebook en leur fournissant un lien.

152. Les Conditions d'utilisation de Facebook et les Conditions de service de la Plateforme Facebook susmentionnée ont été remplacées par la nouvelle Déclaration des droits et responsabilités (DDR). Bien que la DDR comprenne une section au sujet des applications de tiers, elle ne s'adresse pas aux utilisateurs mais bien précisément aux développeurs d'application et aux exploitants. Contrairement aux anciennes Conditions d'utilisations, et malgré le fait que les utilisateurs doivent y consentir dans le contexte des applications de tiers, la DDR elle-même ne comprend aucune information au sujet des applications adressée explicitement aux utilisateurs qui ne sont pas des développeurs d'applications. À la fin de la DDR, on retrouve des liens vers plusieurs documents, l'un d'entre eux, « Comprendre la Plateforme » [traduction] mène vers le document « Conditions d'utilisation des applications de la Plateforme » [traduction].

153. Des paramètres de confidentialité par défaut sont en place précisément pour la Plateforme Facebook. Les paramètres de confidentialité par défaut de la version actuelle de la Plateforme Facebook et de l'ancienne sont les mêmes. L'option générale préétablie permet la communication du nom de l'utilisateur, de ses réseaux et de sa liste d'amis, de même qu'une série d'éléments facultatifs, notamment sa photo de profil, ses renseignements généraux, ses renseignements personnels (activités, intérêts, etc.), sa ville de résidence, son parcours scolaire et professionnel, son statut, son Mur, ses notes, les groupes auxquels il appartient, les événements auxquels il est invité, les photos qu'il a prises ou que ses amis ont prises de lui, sa situation amoureuse et sa présence en ligne. Parmi les éléments qui ne sont pas présélectionnés, mentionnons le genre de relation que l'utilisateur cherche, son orientation sexuelle, le nom de

la personne avec qui il entretient une relation amoureuse et ses croyances religieuses.

154. L'option générale qui n'est pas présélectionnée se lit comme suit : « Ne partager aucune information me concernant par le biais de l'API Facebook » [traduction]. Les utilisateurs qui cochent cette option ne seront pas en mesure de télécharger des applications. En outre, cette option ne peut être cochée si l'utilisateur a déjà installé des applications.

155. Facebook a également ajouté à la page des paramètres de confidentialité de la Plateforme une section explicative à l'égard de la collecte et de l'utilisation de renseignements personnels par les applications de tiers. La CIPPIC a allégué que le libellé de la page des paramètres et celui de l'aperçu n'indiquaient pas clairement si les paramètres de confidentialité ne renvoient qu'aux applications que l'utilisateur ajoute ou à celles ajoutées par ses amis.

156. Facebook a expliqué que, lorsqu'un utilisateur demande à ajouter une application, il autorise les développeurs à demander ses renseignements à Facebook. Facebook donne alors aux développeurs une clé qui permet d'accéder aux renseignements personnels de l'utilisateur, à l'exception de ses coordonnées, ainsi qu'aux renseignements de ses amis, selon leurs paramètres de confidentialité. Si l'utilisateur est membre d'un réseau, l'application de la Plateforme pourrait également avoir accès aux renseignements personnels des membres du réseau.

157. Concernant l'accès aux renseignements par les applications de la Plateforme, Facebook a affirmé ceci dans ses observations :

« En règle générale, une application de la Plateforme ne peut accéder qu'aux données auxquelles une personne aurait autrement accès sur Facebook. En d'autres mots, le fournisseur de l'application est autorisé à prendre la place de l'utilisateur au nom de qui les données sont demandées. Il n'a pas un accès complet aux données de Facebook seulement parce que son application a été ajoutée » [traduction].

158. Facebook mentionne également les points suivants :

- Une application ne peut accéder aléatoirement à des données, mais il lui est possible de se servir du profil d'un utilisateur si ce dernier met en marche l'application.

- Lorsqu'une application de tiers interagit avec des utilisateurs, elle doit respecter les paramètres de confidentialité de ces derniers. Par exemple, l'application ne peut autoriser d'autres utilisateurs à accéder aux renseignements dont un utilisateur a limité l'accès.

- Le développeur doit accepter les Conditions de service des développeurs (maintenant comprises dans la DDR) et les Lignes directrices des applications de la Plateforme Facebook (maintenant désignées sous le nom de « Lignes directrices de la Plateforme » [traduction], qui stipulent que toutes les données auxquelles accèdent les développeurs doivent être détruites dans les 24 heures et que les données ne peuvent servir à d'autres fins qu'à l'application.

159. Au sujet de ce dernier point, la nouvelle DDR ne contient en fait aucune mention au sujet de la destruction des données après 24 heures. Les Lignes directrices de la Plateforme, qui remplacent les anciennes Lignes directrices des applications de la Plateforme Facebook, mentionnent ce qui suit :

    « Eu égard à la protection des renseignements personnels et à d'autres considérations, vous ne pouvez pas conserver les données que vous recevez de la part de Facebook, mis à part certaines données enregistrables. Toutefois, pour des raisons de performance, vous pouvez conserver en mémoire cache les données que vous recevez de notre part pour au plus 24 heures » [traduction].

    Des précisions supplémentaires sont fournies aux développeurs dans la politique sur les données enregistrables, « Lignes directrices de la Plateforme 11-15 : Données enregistrables » [traduction], qui stipule que les développeurs doivent supprimer la plupart des données au sujet des utilisateurs dans les 24 heures si l'utilisateur a supprimé l'application.

160. Afin de pouvoir développer et offrir des applications sur Facebook, les développeurs doivent être eux-mêmes des membres de Facebook avec des profils déjà établis. Comme on peut le lire au paragraphe 151 ci-dessus, au moment de l'enregistrement, les membres de Facebook doivent accepter les Conditions d'utilisation de Facebook (maintenant remplacées par la DDR), vers lesquelles un lien est fourni. Au moment de créer une nouvelle application, le développeur doit une fois de plus accepter ce que l'écran pertinent désigne comme étant les « Conditions de Facebook », au regard desquelles on fournit un lien vers la DDR.

161. La section 9 de la DDR, intitulée « Clauses spéciales applicables aux développeurs/exploitants d'applications et de sites Web », comprend ce qui suit :

« Si vous êtes un développeur ou un exploitant d'une application de la Plateforme ou d'un site Web qui utilise Connect ("application") ou qui utilise de toute autre manière la Plateforme, vous êtes soumis aux conditions supplémentaires suivantes :

1. *Vous êtes responsable de votre application, de son contenu et de toute utilisation que vous faites de la Plateforme. Vous devez entre autres vous assurer que votre application ou votre utilisation de la Plateforme est conforme à nos* ***Lignes directrices de la Plateforme****.*
2. *Quand des utilisateurs ajoutent votre application ou la relient à leur compte Facebook, ils vous accordent la permission de recevoir certaines données qui les concernent. Votre accès à ces données et l'utilisation que vous en faites sont assujettis aux limites suivantes :*

    1. *Vous utiliserez les données que vous avez reçues seulement dans le cadre de votre application et seulement en lien avec Facebook.*
    2. *Vous indiquerez clairement aux utilisateurs quelles données vous utiliserez et comment vous utiliserez, afficherez ou communiquerez ces données.*
    3. *Vous n'utiliserez pas, n'afficherez pas ou ne communiquerez pas les données d'un utilisateur d'une manière qui irait à l'encontre des paramètres de* ***confidentialité*** *de celui-ci sans son consentement.*
    4. *Vous supprimerez toute donnée que vous auriez reçue de notre part concernant un utilisateur qui supprime ou se débranche de votre application, à moins que ne le permettent les* ***Lignes directrices de la Plateforme****.*
    5. *Vous supprimerez toute donnée que vous auriez reçue de Facebook si nous désactivons votre application ou que nous vous demandons de le faire.*
    6. *Nous pouvons exiger que vous mettiez à jour toute donnée que vous auriez reçue de notre part.*
    7. *Nous pouvons restreindre votre accès aux données.*

> *8. Vous ne transférerez pas les données que vous avez reçues de notre part sans avoir reçu notre consentement au préalable. »* [traduction]

162. Au moment de la plainte, Facebook n'exigeait pas que les développeurs d'applications annoncent clairement aux utilisateurs quelles données précises seraient utilisées ni comment elles seraient utilisées, affichées ou communiquées, comme on le stipule maintenant à la sous-section 9.2.2 de la DDR (voir le paragraphe précédent).

163. En ce qui concerne la sous-section 9.2 de la DDR dans son ensemble, Facebook n'a fourni aucune preuve qu'il existe des contraintes technologiques à l'utilisation, l'affichage ou la communication par les développeurs des données d'un utilisateur d'une manière qui serait interdite aux termes de cette sous-section.

164. Les Lignes directrices de la Plateforme comprennent une section intitulée « Mise à exécution » [traduction], qui se lit comme suit :

> *« Si Facebook détermine (à sa seule discrétion) que vous ou votre application enfreignez les Conditions et Politiques de la Plateforme Facebook, Facebook peut prendre des mesures d'exécution contre l'application délinquante et/ou vos autres applications, en tout ou en partie. Ces mesures d'exécution peuvent comprendre : la désactivation temporaire ou permanente de la ou des applications; la cessation de toute entente entre vous et Facebook; la restriction temporaire ou permanente de votre accès ou de celui de votre application aux fonctions de la Plateforme Facebook, en tout ou en partie; ou toute autre action que Facebook (à sa seule discrétion) juge appropriée »* [traduction].

165. À cet égard, Facebook n'a fourni aucune preuve qu'elle filtrait ou vérifiait de manière systématique les activités des développeurs d'application. Elle compte plutôt sur les utilisateurs eux-mêmes pour repérer les tiers développeurs d'applications qui contreviendraient à la DDR ou aux Lignes directrices de la Plateforme. Selon Facebook, il est dans l'intérêt supérieur des développeurs de respecter les règles, car c'est eux qui ont le plus à perdre : de nombreuses applications sont de nature commerciale et visent à produire de l'achalandage et à diffuser de la publicité.

166. Dans la documentation fournie sur le site, Facebook se présente comme n'étant peu ou pas responsable des activités des tiers développeurs

d’application. Notamment, au moment de la plainte, les Conditions d’utilisation de Facebook stipulaient ce qui suit :

« Nous ne vérifions pas, ne surveillons pas, et ne confirmons pas l’exactitude, la pertinence ou l’exhaustivité des sites, applications, logiciels et contenus de tiers. Nous ne sommes pas responsables des sites de tiers accessibles à partir du Site ou des applications, logiciels et contenus de tiers publiés, installés ou disponibles sur le Site. Nous ne sommes pas non plus responsables du contenu, de l’exactitude, du caractère offensant, des opinions, de la fiabilité, des pratiques relatives au respect de la vie privée et des autres pratiques des sites, applications, logiciels et contenus de tiers. L’inclusion, la création de liens ou l’autorisation d’utilisation ou d’installation d’un site, d’applications, logiciels et contenus de tiers n’est pas soumise à notre acceptation. Si vous quittez le site pour procéder à l’accès à des sites de tiers à partir du Site ou l’utilisation ou l’installation d’applications, logiciels et contenus de tiers se fait à vos risques et périls et sous votre entière responsabilité, et n’est pas régi par nos Conditions d’utilisation ou nos politiques. Vous devez prendre connaissance des conditions et des règlements, y compris des pratiques relatives à la vie privée et à la collecte de données, qui sont en vigueur sur tout site consulté à partir du Site, ou associés aux applications que vous utilisez ou installez à partir du site » [traduction].

167. La nouvelle DDR ne comprend pas l’énoncé cité ci-dessus. Toutefois, on retrouve un passage similaire dans la Politique de confidentialité :

« Avant d’autoriser un développeur de la Plateforme à vous donner accès à toute application de la Plateforme, Facebook demande au développeur de la Plateforme d’accepter un accord qui exige notamment le respect de vos paramètres de confidentialité. La collecte, l’utilisation, et la conservation de vos renseignements sont strictement limitées. Cependant, bien que nous ayons pris des dispositions contractuelles et techniques pour réduire le risque d’une utilisation abusive de ces renseignements par les développeurs de la Plateforme, nous ne pouvons pas garantir que tous les développeurs de la Plateforme respecteront ces accords. Facebook ne présélectionne ni n’approuve les développeurs de la Plateforme et, par conséquent, ne peut pas contrôler leurs pratiques d’utilisation des renseignements personnels qu’ils ont pu obtenir par l’entremise des applications de la Plateforme. Qui plus est, les développeurs de la Plateforme peuvent vous demander d’accepter leurs propres conditions d’utilisation, paramètres de confidentialité ou autres conditions, ce qui peut supposer des droits complémentaires pour eux ou d’autres obligations pour vous. Assurez-vous de lire attentivement ces

conditions avant d'utiliser une application de la Plateforme. Vous pouvez dénoncer n'importe quelle utilisation suspecte de renseignements à même la Plateforme Facebook. Nous ouvrirons une enquête et prendrons les mesures appropriées à l'encontre du développeur de la Plateforme, lesquelles pourraient aller jusqu'à cesser leur utilisation de la Plateforme Facebook ou l'ouverture de poursuites judiciaires formelles » [traduction].

168. Facebook a soutenu que l'architecture de la Plateforme d'applications joue un rôle central dans la sécurité :

« Les applications nécessitent l'établissement de clés d'application qui permettent le suivi des demandes de données et encouragent un comportement plus responsable des applications. Il est bien entendu impossible d'éliminer tous les risques d'utilisation malveillante du système, mais cette décision structurelle visant les demandes individuelles et la responsabilisation permet de faciliter la reddition de comptes » [traduction].

169. En novembre 2008, Facebook a lancé le « Programme de vérification des applications » [traduction], au moyen duquel elle examine et surveille les développeurs pour s'assurer qu'ils satisfont à ses normes et principes directeurs. Contre une somme de 375 $, Facebook examinera une application pour s'assurer qu'elle respecte les principes directeurs de l'entreprise. L'un des éléments examinés par Facebook est la collecte et l'utilisation de renseignements personnels par le développeur d'une application. Dans la description des exigences du programme, Facebook indique ce qui suit :

« Facebook prend la confidentialité des données au sérieux. Nous demanderons une justification pour toutes les données que votre application consulte et des exemples d'utilisation de ces données. Nous vérifions cette information pour assurer aux utilisateurs que vous consultez les données uniquement pour créer la meilleure expérience possible, et rien de plus » [traduction].

Les applications approuvées reçoivent un sceau de vérification de la part de Facebook et ont une visibilité accrue dans le site. La participation des développeurs au programme est purement volontaire.

170. En ce qui concerne le consentement des utilisateurs à la collecte et à l'utilisation de leurs données de la part des développeurs au moment où des amis ajoutent une application, Facebook a déclaré ceci :

« Les utilisateurs sont libres de choisir s'ils souhaitent ou non interagir avec une application en particulier. Ils disposent également d'un moyen simple de bloquer toute application précise ou de se retirer de toutes les applications » [traduction].

171. Quant au retrait du consentement, la CIPPIC a allégué que, lorsqu'un utilisateur retire son consentement à communiquer ses renseignements aux développeurs, il perd automatiquement toutes les applications sans préavis. Facebook prétend que cette situation ne s'est jamais produite, car, en réalité, les utilisateurs ne peuvent retirer leur consentement s'ils ont ajouté des applications. Dans sa nouvelle version, Facebook explique dans une fenêtre contextuelle que, pour retirer son consentement, un utilisateur doit supprimer toutes les applications qu'il a ajoutées, puis supprimer les autorisations pour toutes les applications externes qu'il a pu utiliser. La CIPPIC n'a fourni aucune impression d'écran pour soutenir ses allégations et a par la suite reconnu que Facebook avait répondu adéquatement à ses préoccupations à cet égard.

172. La CIPPIC a allégué que Facebook n'informait pas efficacement les utilisateurs de la raison pour laquelle les renseignements personnels de ces derniers étaient communiqués aux développeurs tiers d'applications ni de la portée de la communication. En plus de l'information de l'impression d'écran décrite ci-dessus, la Politique de confidentialité de Facebook traite ainsi des applications de tiers :

« Si vous, vos amis, ou les membres de votre réseau utilisez une quelconque application de tiers développée à l'aide de la Plateforme Facebook (les "applications de la Plateforme"), ces applications de la Plateforme peuvent accéder à certains renseignements vous concernant et les partager, conformément à vos paramètres de confidentialité. Vous pouvez retirer votre consentement au partage de vos renseignements, en tout ou en partie, avec les applications de la Plateforme sur la page ***Paramètres de confidentialité****. De plus, les tiers développeurs qui ont mis au point des applications et les exploitent (les "développeurs de la Plateforme") peuvent également avoir accès à vos renseignements personnels (excepté vos coordonnées) si vous donnez aux applications de la Plateforme l'accès à vos données »* [traduction].

173. Dans cet extrait de la Politique de confidentialité, il est fait mention de l'accès par les développeurs aux renseignements des utilisateurs lorsque *les membres de leurs réseaux* utilisent des applications de tiers. Toutefois, dans les écrans des paramètres de confidentialité, les membres des réseaux ne sont pas mentionnés; on ne fait référence qu'aux amis. Tel est également le cas pour l'écran « Autoriser l'accès » qui apparaît lorsqu'un utilisateur ajoute une application. Le Commissariat a demandé à Facebook d'indiquer l'endroit où, hormis la Politique de confidentialité, les utilisateurs étaient informés que leurs renseignements pouvaient être communiqués à des développeurs lorsqu'un membre de leur réseau utilisait une application, et de signaler si les paramètres de confidentialité des applications pouvaient être utilisés pour restreindre la communication d'information lorsqu'un membre du réseau utilisait une application.

174. Facebook a répondu ainsi :

« Les paramètres de confidentialité s'appliquent à toutes les applications de la Plateforme Facebook; si je bloquais une application, ces paramètres empêcheraient l'application d'avoir accès à mes données, même si elle demandait à les consulter au nom d'un ami ou d'un membre du réseau qui serait autrement en mesure de voir ces données » [traduction].

175. Les Conditions d'utilisation des applications de la Plateforme sont plus précises quant au type de renseignements personnels pouvant être fournis aux développeurs :

*« **REMARQUE : La Plateforme Facebook ne permet pas aux développeurs d'accéder à vos adresses de courriel, site Web personnel, pseudonyme de messagerie instantanée, numéros de téléphone ou adresse résidentielle ("coordonnées"). Facebook communiquera uniquement vos coordonnées à des tiers conformément à sa Politique de confidentialité.***
II. Consentement quant à l'utilisation des renseignements du site Facebook
*a) **Information pouvant être transmise aux développeurs.** Afin de vous permettre d'utiliser les applications de la Plateforme créées par des développeurs ("applications de développeurs") et d'y participer, Facebook peut à l'occasion accorder aux développeurs un accès aux renseignements suivants (collectivement les "renseignements du site Facebook") :*
i) tout renseignement que vous avez fourni et qui est visible dans le site Facebook, à l'exclusion de vos coordonnées;
ii) le nom d'utilisateur associé à votre profil Facebook.
*b) **Exemples de renseignements du site Facebook.** Les renseignements du site Facebook comprennent, sans s'y limiter, l'information suivante dans la*

mesure où elle est visible dans le site Facebook : votre nom, votre photo de profil, votre sexe, votre date d'anniversaire, votre pays/État/ville natal, votre pays/État/ville de résidence, vos opinions politiques, vos activités, vos intérêts, vos styles de musique, émissions de télévision, films et livres préférés, vos citations favorites, le texte de la section "À propos de moi", votre situation amoureuse, votre orientation sexuelle, vos projets d'été, vos réseaux Facebook, votre parcours scolaire et professionnel, les renseignements sur vos cours, des copies des photos de vos albums Facebook, les métadonnées liées à vos albums de photos Facebook (p. ex. moment du téléchargement, nom de l'album, commentaires sur les photos, etc.), le nombre de messages que vous avez envoyés ou reçus, le nombre de messages non lus dans votre boîte de réception Facebook, le nombre de "pokes" que vous avez envoyés ou reçus, le nombre de messages sur votre Mur[MC], une liste des noms d'utilisateur associés à vos amis Facebook, votre calendrier social et les événements associés à votre profil Facebook.
c) ***Paramètres de confidentialité*** *: À tout moment, vous pouvez annuler ou modifier l'autorisation que vous avez accordée à Facebook de fournir des renseignements du site Facebook à des développeurs par les moyens offerts dans vos* ***paramètres de sécurité*** *»* [traduction].

176. La CIPPIC a affirmé que l'information des Conditions d'utilisation des applications de la Plateforme Facebook présentée ci-dessus n'était pas facilement accessible, puisque les utilisateurs devaient suivre un lien à partir de la page des Conditions d'utilisation pour la trouver. Dans la plainte qu'elle a déposé, CIPPIC a affirmé également que le document n'était pas accessible de la page principale de Facebook, mais uniquement à partir du site des développeurs. Cependant, la CIPPIC a depuis reconnu que le lien vers les Conditions d'utilisation des applications de la Plateforme se trouvait dans les Conditions d'utilisation sous le titre « Applications de la Plateforme Facebook ». Facebook a fait remarquer qu'en général, les liens vers les Conditions d'utilisation des applications de la Plateforme étaient fournis « aux principaux points d'interaction entre les utilisateurs et le service » [traduction].

177. Le Commissariat n'a pu trouver qu'un seul lien actif vers les Conditions d'utilisation des applications de la Plateforme. Ce lien est présenté parmi d'autres à la fin de la nouvelle DDR. Bien que le lien en question mène vers un document intitulé « Conditions d'utilisation des applications de la Plateforme » [traduction], le lien lui-même est intitulé « Comprendre la Plateforme » [traduction].

178. Au moment où la plainte a été déposée, les Conditions d'utilisation de Facebook stipulaient que les utilisateurs qui installaient des applications de tiers devaient accepter les modalités établies dans les Conditions d'utilisation des applications de la Plateforme. Toutefois, lorsque les utilisateurs ajoutaient une application, ils étaient informés qu'ils approuvent les Conditions de service des utilisateurs de Facebook, et aucune mention n'était faite des Conditions d'utilisation des applications de la Plateforme. À l'heure actuelle, tel qu'il est indiqué ci-dessus, on ne mentionne nulle part que les utilisateurs doivent accepter les Conditions d'utilisation des applications de la Plateforme.

179. En règle générale, les sources d'information au sujet des applications de tiers ne sont ni mentionnées ni identifiées clairement.

180. La CIPPIC a allégué que Facebook n'offrait pas une description complète des fins auxquelles elle permettait aux développeurs d'applications de recueillir, d'utiliser et de communiquer des renseignements personnels au moyen de la Plateforme Facebook. À l'ajout d'une application et dans l'écran d'aperçu d'une application, les utilisateurs sont avisés que l'accès des développeurs à leurs renseignements personnels sera limité au contenu nécessaire à son fonctionnement. Les Conditions de service des développeurs et les Conseils d'utilisation semblent toutefois permettre la collecte, l'utilisation et la communication de renseignements personnels à des fins de commercialisation. La CIPPIC a allégué que les utilisateurs ne sont pas informés de cet usage.

181. La CIPPIC a indiqué que les Conditions d'utilisation des applications de la Plateforme prévoient que « à tout moment, vous pouvez annuler ou modifier l'autorisation que vous avez accordée à Facebook de fournir des renseignements du site Facebook à des développeurs par les moyens offerts dans vos **paramètres de confidentialité** » [traduction]. La CIPPIC estime que cette affirmation donne l'impression que les utilisateurs ont une plus grande maîtrise que ce qu'ils ont en réalité des renseignements fournis aux applications ajoutées par eux-mêmes, par leurs amis ou par les membres de leurs réseaux.

182. Puisque les tiers développeurs d'applications pourraient en théorie avoir accès à une grande quantité de renseignements personnels, on peut se demander si les applications ont généralement besoin de ceux-ci pour fonctionner et, si tel est le cas, dans quelle mesure. En octobre 2007, deux chercheurs de la University of Virginia ont publié une enquête sur les besoins en information des 150 applications les plus populaires sur Facebook. Les chercheurs ont fait état des constatations suivantes :

« Nous avons découvert que 8,7 % d'entre elles n'avaient besoin d'aucun renseignement; 82 % se servaient des données publiques (nom, réseaux, liste d'amis), et seules 9,3 % avaient besoin de renseignements personnels (p. ex. date d'anniversaire). Puisque toutes les applications ont un accès complet aux données personnelles, ces résultats signifient que ***90,7 % des applications ont plus de privilèges que ce dont elles ont besoin*** *»* [traduction; souligné dans l'original].

183. Facebook a émis des réserves quant à la méthodologie utilisée et commenté l'enquête ainsi :

« Nous estimons que les chercheurs, dans le cadre de l'enquête, ont adopté un point de vue indûment limité à l'égard de l'utilisation légitime et sociale des renseignements. Ils ont présenté un accès potentiel aux données en évitant délibérément de mentionner les restrictions importantes que nous avons mises en place et en ignorant les restrictions quant à l'utilisation et à la conservation des données ainsi que les mécanismes d'exécution qui ont fait le succès de la Plateforme Facebook » [traduction].

Application

184. Dans l'analyse des faits, nous avons appliqué les principes 4.2, 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.6, 4.7 et 4.7.1, ainsi que le paragraphe 5(3).

185. Le principe 4.2 prévoit que les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

186. Le principe 4.2.3 établit notamment qu'il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ces renseignements sont destinés.

187. Le principe 4.3 précise, entre autres, que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

188. Le principe 4.3.2, s'appuyant sur l'exigence d'avis et de consentement énoncée au principe 4.3, mentionne qu'il faut faire un effort raisonnable pour informer la personne des fins auxquelles les renseignements seront utilisés. Le principe 4.3.2 précise également 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.

189. Le principe 4.3.4 stipule entre autres que, pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements et que tous les renseignements peuvent devenir sensibles suivant le contexte. Le principe 4.3.5 stipule entre autres que dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Le principe 4.3.6 prévoit notamment que, en général, une organisation devrait chercher à obtenir un consentement explicite si les renseignements sont considérés comme étant sensibles.

190. Le principe 4.7 établit que les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Le principe 4.7.1 prévoit notamment que les mesures de sécurité doivent protéger les renseignements personnels contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Le principe 4.7.3 stipule entre autres que les méthodes de protection devraient comprendre des mesures techniques.

191. Le paragraphe 5(3) établit qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Constatations

192. Dans mon rapport préliminaire, j'ai indiqué ce qui suit :

193. *« Notre* enquête *nous a permis d'identifier les sujets de préoccupation suivants concernant les applications de tiers dans l'environnement Facebook :*

    1) En considération des principes 4.7 et 4.7.1 ainsi que du paragraphe 5(3), j'entretiens des préoccupations à l'effet que Facebook donne à des tiers développeurs d'applications un accès possiblement illimité aux renseignements des utilisateurs, mais n'effectue pas la surveillance des développeurs pour s'assurer :

        i) qu'ils obtiennent uniquement les renseignements nécessaires au fonctionnement de l'application;

        ii) qu'ils ne conservent les renseignements qu'aussi longtemps qu'il est nécessaire pour fournir l'application;

iii) qu'en toutes autres choses, leur traitement des renseignements personnels est conforme aux principes de protection de la vie privée.

Selon moi, rendre tous les renseignements personnels d'un utilisateur accessibles à un tiers équivaut à la communication de ces renseignements à ce tiers. Je doute qu'une personne raisonnable considérerait qu'une telle communication soit appropriée dans les circonstances, en particulier lorsqu'on sait que les tiers n'ont en général besoin que de très peu de renseignements pour réaliser leurs propres fins. De plus, compte tenu du risque important, dans ces circonstances, d'accès, d'utilisation et de communication sans autorisation, je ne suis pas convaincue que les ententes contractuelles avec les développeurs constituent en soi une mesure de sécurité adéquate pour protéger les renseignements personnels des utilisateurs dans l'environnement Facebook.

2) En considération des principes 4.2, 4.2.3, 4.3 et 4.3.2, je suis préoccupée à l'idée que les utilisateurs ne soient pas informés des renseignements personnels auxquels accèdent les développeurs, ni suffisamment informés des fins de l'utilisation et de la communication de leurs renseignements personnels. À cet égard, j'ajouterai que je ne vois pas d'amélioration valable dans le libellé de consentement actuel par apport au libellé original, et je ne le considère pas comme un fondement raisonnable pour donner son consentement.

3) En considération des principes 4.3 et 4.3.4, je suis préoccupée à l'idée que Facebook n'utilise pas la forme de consentement appropriée pour la communication des renseignements personnels des utilisateurs à des tiers développeurs d'applications. À mon avis, compte tenu que les renseignements personnels des utilisateurs sont possiblement sensibles, il y aurait lieu de recourir au consentement actif exprès dans tous les cas.

4) En considération du principe 4.3, je suis préoccupée à l'idée que les utilisateurs ne jouissent pas d'un contrôle suffisant sur leurs renseignements personnels dans la mesure où on ne cherche pas à obtenir leur consentement à la communication de leurs renseignements personnels aux fins des applications quand leurs amis et les membres de leurs réseaux ajoutent des applications.

194. Facebook s'est vigoureusement opposée à notre traitement préliminaire des allégations relatives aux applications de tiers. Cependant, après avoir pris en considération les objections de Facebook, je demeure préoccupée à cet effet.

195. Deux enjeux principaux ont été soulevés dans les allégations : les mesures de sécurité et le consentement.

196. En ce qui a trait au premier, je tiens à souligner qu'en vertu des principes 4.7 et 4.7.1, les organisations doivent instaurer des mesures pour protéger les renseignements personnels contre l'accès, l'utilisation et la communication sans autorisation. De plus, le principe 4.7.3 prévoit que les mesures techniques doivent figurer au nombre des méthodes de protection. C'est avec ces principes à l'esprit que j'ai formulé mes recommandations initiales à l'effet que Facebook devrait « limiter » l'accès des développeurs d'applications aux renseignements des utilisateurs à ce qui est nécessaire au fonctionnement d'une l'application particulière.

197. Dans le rapport préliminaire, j'indiquais que des défenseurs de la protection de la vie privée avaient vivement critiqué le fait que les tiers développeurs d'applications jouissaient d'un accès pratiquement illimité et non surveillé aux renseignements personnels des utilisateurs de Facebook. Voici les objections que Facebook a soulevées :

« Le passage "accès pratiquement illimité et non surveillé" donne l'impression qu'il n'y a aucune limite ni surveillance. Cette affirmation a été complètement démentie lors de présentations, et est démentie par d'autres renseignements qu'on retrouve dans le rapport préliminaire. Il semble régner une certaine confusion dans la description même du problème quand à l'exonération juridique de la responsabilité de surveillance — une clause type dans les contrats Web — et le fait que nous disposons d'une structure bien conçue qui permet l'identification et le retrait d'applications possiblement problématiques » [traduction].

198. Facebook a également élevé des objections contre ma suggestion que l'entreprise donnait aux tiers développeurs d'application un accès possiblement illimité aux renseignements personnels et rendait accessibles aux tiers tous les renseignements personnels des utilisateurs. Facebook soutient plutôt que : « Nous accordons aux développeurs une clé d'application qui leur donne la capacité limitée de présenter une requête pour des données définies dans l'interface de programmation d'applications (API) après qu'un utilisateur a interagi avec cette application, ainsi qu'une licence restreinte pour utiliser ces données conformément aux Lignes directrices de Facebook à l'intention des développeurs » [traduction].

199. En l'absence de preuves de mesures de protection techniques, je ne peux que tenir pour acquis que lorsque Facebook parle d'accès limité aux renseignements des utilisateurs, elle parle de limites contractuelles. En d'autres mots, pour limiter l'accès, Facebook se fie surtout sur certaines interdictions

citées dans les documents de politiques, et fait confiance au développeur d'applications qui, ayant reconnu l'entente, s'engage à respecter les interdictions. Fait notoire, la Déclaration des droits et responsabilités, que tous les utilisateurs de Facebook, y compris les développeurs, sont censés accepter, présente les instructions suivantes aux développeurs :

> *« Quand des utilisateurs ajoutent votre application ou la relient à leur compte Facebook, ils vous accordent la permission de recevoir certaines données qui les concernent. Votre accès à ces données et l'utilisation que vous en faites sont assujettis aux limites suivantes :*
>
> > *1. Vous utiliserez les données que vous avez reçues seulement dans le cadre de votre application et seulement en lien avec Facebook.*
> > *2. Vous indiquerez clairement aux utilisateurs quelles données vous utiliserez et comment vous utiliserez, afficherez ou communiquerez ces données.*
> > *3. Vous n'utiliserez pas, n'afficherez pas ou ne communiquerez pas les données d'un utilisateur d'une manière qui irait à l'encontre des paramètres de confidentialité de celui-ci sans son consentement.»* [traduction].

Facebook semble considérer cet énoncé comme la mesure de protection la plus efficace contre l'accès non autorisé.

200. Quand je parle d'accès limité — surtout quand on prend en considération le très grand nombre de renseignements personnels d'utilisateurs de Facebook potentiellement disponibles à un grand nombre de développeurs d'applications — je pense que des mesures de protection beaucoup plus rigoureuses sont nécessaires. Plus particulièrement, des mesures de protection techniques qui ne feront pas qu'interdire, mais empêcheront réellement les développeurs d'accéder sans autorisation aux renseignements personnels dont ils n'ont pas besoin.

201. Pour en arriver à mes conclusions dans cette affaire, j'ai pris en compte ce qui suit :

- À l'exception des coordonnées, les applications peuvent accéder à pratiquement tous les renseignements personnels dans un compte donné, y compris la liste d'amis, certains renseignements sur les amis et des renseignements qu'on jugerait sensibles à l'extérieur du cercle d'amis.

Même si Facebook oblige les développeurs, par contrat, à respecter les paramètres de confidentialité des utilisateurs, je n'ai vu aucune preuve de barrière technologique empêchant les développeurs d'accéder aux renseignements bloqués par les paramètres.

- J'ai des doutes quant à la quantité de renseignements personnels d'utilisateurs nécessaire au fonctionnement normal d'une application. Il semble donc que sur le plan technique, Facebook donne aux développeurs accès à bien plus de renseignements qu'ils n'en ont besoin.
- La Politique de confidentialité de Facebook précise que « Facebook ne présélectionne ni n'approuve les développeurs de la Plateforme » [traduction].
- Le nouveau Programme de vérification des applications de Facebook est purement volontaire et ne constitue pas un système de surveillance en temps réel. À part ce programme, auquel les développeurs ne sont pas tenus de participer, rien ne porte à croire que Facebook fait des efforts appréciables et soutenus pour garantir que les renseignements auxquels accèdent les développeurs se limitent au strict nécessaire pour le fonctionnement de l'application.
- Puisque les développeurs peuvent copier les renseignements personnels des utilisateurs depuis le site Facebook à leur propres serveurs, il ne semble exister aucun moyen pour que Facebook puisse surveiller efficacement les actions subséquentes des développeurs liées à l'utilisation et au retrait des renseignements. Facebook l'admet dans sa Politique de confidentialité quand elle dit qu'elle « ne peut pas contrôler leurs pratiques en matière d'utilisation des renseignements personnels qu'ils ont pu obtenir via les applications de la plateforme » [traduction]. De plus, dans le même paragraphe, Facebook charge les utilisateurs de la responsabilité de détecter et de signaler les problèmes. Puisqu'on ne peut pas surveiller après coup l'utilisation faite par les développeurs, il importe d'autant plus que Facebook prenne des mesures préventives efficaces.
- Facebook soutient que sa structure est bien conçue et permet l'identification et le retrait d'applications potentiellement problématiques. Toutefois, Facebook n'a fourni aucune preuve à l'effet qu'une telle structure est appliquée de manière rigoureuse et systématique afin de *prévenir* les problèmes — en particulier le problème de l'accès non autorisé. En effet, tout ce que Facebook a démontré laisse entendre le contraire : que toute activité de surveillance de Facebook est en grande partie effectuée en réaction, plutôt que de manière préventive.

202. Je constate que Facebook n'a pas mis en place de mesures de protection adéquates afin de prévenir l'accès non autorisé aux renseignements personnels des utilisateurs par les développeurs d'applications et, par conséquent, qu'elle contrevient aux principes 4.7, 4.7.1, et 4.7.3.

203. En ce qui a trait au consentement, je constate que le moyen par lequel Facebook l'obtient est problématique à deux égards.

204. Premièrement, le libellé qu'emploie Facebook pour obtenir le consentement est trop général. Dans des cas précédents, le Commissariat a souvent fait part de sa désapprobation à l'égard d'un libellé beaucoup moins général et a déterminé qu'un tel libellé ne constituait pas un fondement raisonnable pour obtenir le consentement. Dans le présent cas, le libellé utilisé par Facebook est imprécis. Facebook informe effectivement les utilisateurs que chaque fois qu'ils ajoutent une application, ils doivent accepter de donner accès à pratiquement tout ce que le développeur demande. Selon moi, le consentement ainsi obtenu n'est pas valable. Dans les circonstances, et surtout compte tenu que certains renseignements que les développeurs recherchent peuvent s'avérer sensibles, il faut obtenir le consentement valable de l'utilisateur à la collecte et à l'utilisation de renseignements précis chaque fois qu'un utilisateur ajoute une application.

205. Deuxièmement, en principe, lorsqu'un développeur d'applications reçoit les renseignements personnels des utilisateurs par l'entremise de l'API Facebook, on peut considérer que le développeur procède à la collecte de ces renseignements, mais aussi que Facebook procède à la communication de ces mêmes renseignements. Par conséquent, Facebook est tenu de s'assurer que les utilisateurs consentent à une telle communication. Toutefois, compte tenu de la relation entre la Plateforme Facebook et les applications de tiers, Facebook peut se conformer à cette obligation en prenant des mesures raisonnables pour s'assurer et vérifier que les développeurs d'applications obtiennent le consentement valable des utilisateurs au nom de Facebook.

206. D'après la DDR, Facebook fait d'importantes démarches pour garantir que les utilisateurs sont suffisamment informés pour donner leur consentement valable à la communication et à la collecte de leurs renseignements personnels. La DDR renferme des instructions à l'intention des développeurs d'applications selon lesquelles ces derniers doivent expliquer clairement aux utilisateurs quels renseignements ils utiliseront, et comment il les utiliseront, les afficheront ou les échangeront. Lorsqu'un utilisateur reçoit un avis aussi clair et qu'il ajoute une application, on peut considérer que le développeur a obtenu le

consentement valable de l'utilisateur à la fois à la collecte des renseignements par le développeur et à la communication de ces mêmes renseignements par Facebook.

207. Mais à mon avis, la responsabilité de Facebook ne se limite pas simplement à l'énoncé de cette exigence dans la DDR. Pour pouvoir laisser aux développeurs le soin d'obtenir le consentement des utilisateurs, Facebook devrait faire des démarches supplémentaires pour s'assurer que les développeurs sont parfaitement au courant de cette exigence et qu'ils s'y conforment. En premier lieu, Facebook devrait mettre cette exigence bien en évidence dans les règles spécifiques à la Plateforme, dans toute autre instruction à l'intention des développeurs ainsi que dans la DDR. Ensuite, l'entreprise devrait élaborer un mode de surveillance des applications pour s'assurer que les développeurs agissent conformément à l'exigence d'obtenir le consentement. Facebook pourrait même songer à fournir aux développeurs le moyen d'expliquer aux utilisateurs quels renseignements leur sont nécessaires (possiblement en ajustant la grille-écran actuelle de façon à fournir de l'espace pour cette explication).

208. Une autre préoccupation relative au consentement est le fait qu'on ne cherche pas à obtenir le consentement spécifique des utilisateurs à la communication de leurs renseignements personnels dans le cadre d'applications lorsque leurs amis et les membres de leurs réseaux ajoutent des applications. Facebook soutient que grâce aux paramètres de confidentialité, les utilisateurs sont parfaitement en mesure de choisir s'ils veulent ou non interagir avec une application particulière de Facebook, de bloquer une application particulière ou de refuser toutes les applications de Facebook et ce, de manière simple. Si cette explication est vraie en théorie, je tiens à préciser que les utilisateurs « sont en mesure de choisir » seulement s'ils sont informés des pratiques des développeurs relativement à l'accès et à l'utilisation d'information de tiers lorsque leurs amis ajoutent des applications. J'ajouterai que le seul moyen dont disposent les utilisateurs pour éviter que leurs renseignements personnels soient exposés aux développeurs d'applications lorsque leurs amis et les membres de leurs réseaux ajoutent des applications est soit de refuser toutes les applications ou de bloquer des applications particulières. De plus, la dernière option obligerait les utilisateurs de deviner laquelle ou lesquelles des plus de 350 000 applications leurs amis et les membres de leurs réseaux sont susceptibles d'ajouter.

209. Je trouve inapproprié que Facebook transmette aux utilisateurs le fardeau de s'informer et de refuser de communiquer leurs renseignements personnels

lorsque leurs amis et les membres de leurs réseaux ajoutent des applications. Je doute aussi qu'une telle pratique satisfasse aux attentes raisonnables des utilisateurs.

210. En somme, par rapport aux principes 4.2, 4.2.3, 4.3.2, 4.3.4, 4.3.5, et 4.3.6 ainsi qu'au paragraphe 5(3), je constate que Facebook contrevient au principe 4.3 dans la mesure où elle n'obtient pas le consentement valable des utilisateurs pour la communication de leurs renseignements personnels aux développeurs quand les utilisateurs eux-mêmes, leurs amis ou des membres de leurs réseaux ajoutent des applications.

Recommandations et réponse

211. Dans mon rapport préliminaire, je recommandais que Facebook envisage de mettre en œuvre des mesures

    1) pour limiter l'accès des développeurs d'applications aux renseignements des utilisateurs qui ne sont pas nécessaires au fonctionnement de l'application;
    2) par lesquelles, dans chaque cas, les utilisateurs seraient informés des renseignements qu'une application requiert et des fins y afférentes;
    3) par lesquelles, dans chaque cas, on cherche à obtenir le consentement exprès des utilisateurs à ce que les développeurs aient accès à ces renseignements;
    4) interdisant toute communication de renseignements personnels des utilisateurs qui n'ajoutent pas eux-mêmes une application.

212. En réponse, Facebook a formulé des objections, incluses dans les constatations ci-avant, et a refusé dans les faits de mettre en œuvre les recommandations.

Conclusions

213. Par conséquent, je conclus que les allégations se rapportant au consentement et aux mesures de protection sont fondées.

214. Je demande que Facebook reconsidère mes recommandations à la lumière des constatations présentées ci-dessous. Dans le cadre du suivi que nous effectuerons dans les 30 jours concernant d'autres enjeux, nous chercherons à savoir si ces recommandations ont été acceptées et mises en œuvre ou si des

solutions de rechange acceptables ont été trouvées. Si nous ne disposons d’aucune preuve à cet effet, nous déterminerons le meilleur moyen de traiter ces problèmes et toute autre question non résolue conformément à nos pouvoirs.

Section 5

Nouveaux usages des renseignements personnels

Allégation

215. La CIPPIC a allégué que Facebook n'avisait pas les utilisateurs des nouvelles fins auxquelles leurs renseignements personnels étaient recueillis, utilisés ou communiqués, en dérogation au principe 4.2.4.

216. Selon la CIPPIC, Facebook doit informer les utilisateurs de toute nouvelle fin et obtenir leur consentement avant d'utiliser ou de communiquer leurs renseignements personnels à ces nouvelles fins. La CIPPIC n'a toutefois pas précisé de cas dans lesquels Facebook avait instauré une nouvelle fin sans en aviser les utilisateurs et obtenir leur consentement.

Résumé de l'enquête

217. Toute modification aux fins pour lesquelles les renseignements personnels sont recueillis, utilisés ou communiqués par Facebook devrait être indiquée dans sa Politique de confidentialité. En réponse aux allégations de la CIPPIC présentées ci-dessus, Facebook cite la section suivante de sa Politique de confidentialité :

    « Nous nous réservons le droit de modifier notre Politique de confidentialité et nos Conditions d'utilisation à tout moment. Les modifications non substantielles et les précisions apportées prendront effet immédiatement. Quant aux mises à jour importantes, elles prendront effet dans les 30 jours qui suivent leur affichage sur le site. Si nous apportons des modifications, nous les publierons et nous indiquerons en haut de cette page la nouvelle date d'effet de cette politique. Si nous apportons des changements substantiels à cette politique, nous vous en informerons sur cette page, par courriel ou par un avis sur notre page d'accueil. Nous vous invitons à consulter cette Politique de confidentialité régulièrement afin de bien comprendre la politique en vigueur » [traduction].

218. Facebook affirme qu'elle n'a apporté aucune modification substantielle depuis l'entrée en vigueur de cette politique et que toutes les nouvelles fonctionnalités sont conformes à l'infrastructure de confidentialité existante.

219. Au moment du dépôt de la plainte, les Conditions d'utilisation de Facebook mentionnaient également ce qui suit :

« Nous nous réservons le droit, à notre entière discrétion et sans notification préalable, de mettre à jour, modifier, ajouter ou supprimer des dispositions aux présentes Conditions d'utilisation. Dans ce cas, nous publierons sur cette page les modifications apportées aux Conditions d'utilisation en faisant figurer au haut de la page les dates de mise à jour de ces conditions. En continuant d'utiliser le Service ou le Site après de telles modifications, vous acceptez les nouvelles Conditions d'utilisation. Si vous ne souhaitez pas vous conformer aux Conditions d'utilisation, présentes ou futures, veuillez ne pas ou ne plus utiliser ou accéder au Service ou au Site. Il est de votre responsabilité de visiter régulièrement le Site afin de prendre connaissance des éventuelles modifications apportées aux Conditions d'utilisation. »

220. Il est à noter que les Conditions d'utilisation ont été remplacées récemment par la nouvelle Déclaration des droits et responsabilités (DDR). La DDR comprend une section intitulée « Modifications » [traduction], dans laquelle on peut lire ce qui suit :

1. *Nous pouvons modifier la présente Déclaration pourvu que nous vous avisions par l'entremise de Facebook (à moins que vous n'ayez indiqué votre refus de recevoir de tels avis) et que nous vous ayons donné l'occasion de formuler vos commentaires.*

2. *Pour les modifications aux sections 7, 8, 9 et 11 (soit les sections relatives aux paiements, aux développeurs d'applications, aux exploitants de sites Web et aux annonceurs), nous vous aviserons au moins trois jours à l'avance. Pour tout autre changement, nous vous aviserons sept jours à l'avance.*

3. *Si plus de 7 000 utilisateurs émettent un commentaire au sujet des modifications proposées, nous vous donnerons également l'occasion de prendre part à un vote ou vous pourrez choisir parmi plusieurs options. Le vote sera contraignant si plus de 30 % des utilisateurs actifs enregistrés en date de l'avis participent au vote.*

4. *Nous pouvons effectuer des changements pour des motifs juridiques ou administratifs sur avis mais sans donner l'occasion de commenter.*

Constatations

221. En l’absence de preuves que Facebook aurait omis d’informer les utilisateurs de nouvelles utilisations de leurs renseignements personnels, il m’est présentement impossible d’affirmer que Facebook contrevient à la *Loi* à cet égard.

Conclusions

222. Par conséquent, je conclus que l’allégation se rapportant à de nouvelles utilisations des renseignements personnels n’est pas fondée.

Section 6

Collecte de renseignements personnels de sources externes à Facebook

Allégations

223. La CIPPIC a allégué que Facebook :

    1) ne fournissait pas aux utilisateurs de renseignements précis sur les fins et les modes de collecte de renseignements personnels de sources externes à Facebook, sur les sources d'information, et sur l'usage et la communication des renseignements;

    2) n'ayant pas fourni cette information, n'obtenait pas le consentement valable des utilisateurs.

Résumé de l'enquête

224. Dans sa Politique de confidentialité, Facebook indique ce qui suit :

    « Facebook peut également recueillir des renseignements à votre sujet à partir d'autres sources, comme les journaux, les blogues, les services de messagerie instantanée ou par l'utilisation du service par d'autres utilisateurs de Facebook (p. ex. une étiquette sur une photo) afin de vous proposer des renseignements plus utiles et une expérience Facebook personnalisée » [traduction].

225. Dans ses observations au Commissariat, Facebook a affirmé qu'elle ne recueillait pas de renseignements personnels de sources externes, mais qu'elle avait inclus le passage ci-dessus dans sa Politique de confidentialité puisqu'il n'était pas exclu qu'elle le fasse à l'avenir.

Constatations

226. En l'absence de preuves que Facebook recueillait des renseignements personnels de sources externes au moment du dépôt de la plainte, il m'est présentement impossible d'affirmer que Facebook contrevient à la *Loi* à cet égard.

Conclusions

227. Par conséquent, je conclus que les allégations se rapportant à la collecte de renseignements personnels de sources externes à Facebook ne sont pas fondées.

Section 7a)

Désactivation et suppression du compte

Allégations

228. La CIPPIC a allégué que Facebook n'offrait que l'option de désactivation du compte, ce qui est différent de la suppression du compte. Ce faisant, elle privait indûment les utilisateurs d'une façon de supprimer tous leurs renseignements personnels du site.

229. La CIPPIC a formulé ainsi ses allégations générales :

« Nous craignons que la pratique actuelle de Facebook visant à n'offrir que la désactivation du compte crée de la confusion quant à la nature de cette option et à l'option distincte de supprimer le compte. [...] L'option de suppression n'est pas offerte et les utilisateurs n'en sont pas avisés lorsqu'ils désactivent leur compte. Facebook devrait offrir clairement aux utilisateurs le choix entre la désactivation [temporaire] et la suppression [permanente] du compte » [traduction].

230. CIPPIC a précisé ainsi ses préoccupations :

- Facebook devrait offrir aux utilisateurs de manière équitable la possibilité de supprimer leur compte en entier afin que Facebook ne conserve aucun renseignement.
- L'option de désactivation du compte devrait être clairement distinguée de l'option de suppression et les utilisateurs devraient être informés des deux options.
- L'option de désactivation du compte devrait clairement indiquer que les profils des utilisateurs seront conservés par Facebook en vue d'une réactivation future.
- L'option de désactivation du compte devrait prévoir une période de conservation précise, préférablement établie par l'utilisateur, après quoi Facebook détruira les renseignements de ses dossiers, conformément aux principes 4.5.2 et 4.5.3.
- Les renseignements figurant à des comptes désactivés conservés par Facebook devraient être conservés de manière sécuritaire.

Résumé de l'enquête

231. Depuis que Facebook est offerte au public, les utilisateurs peuvent désactiver leur compte. Auparavant, ils étaient en mesure de supprimer manuellement l'information de leur profil, mais non de tout éliminer en même temps. En février 2008, à la suite de critiques publiques et d'une enquête du Privacy Commissioner du Royaume-Uni, Facebook a commencé à permettre aux utilisateurs de supprimer leur compte de façon permanente.

232. En cherchant « supprimer un compte » dans la section Aide de Facebook, l'utilisateur sera dirigé vers une page où la distinction entre suppression et désactivation du compte est expliquée. Une demande de suppression du compte peut être envoyée à partir de l'écran en question, mais une demande de désactivation doit être présentée dans la page Paramètres de la section Compte (« Mon compte »), à laquelle les utilisateurs peuvent accéder par le lien Paramètres. La page Paramètres de la section Compte comprend l'option de désactivation, mais non l'option de suppression. Les deux options sont donc offertes effectivement à des écrans différents.

233. La suppression d'un compte signifie que toutes les données personnelles d'un utilisateur seront éliminées des bases de données actives, y compris des étiquettes sur les photos. Dans la section Aide, sous le titre « Je souhaite supprimer mon compte définitivement » [traduction], Facebook explique ainsi la suppression d'un compte :

    « Si vous désactivez votre compte dans la section "Désactiver le compte" sur la page Compte, votre profil et tous les renseignements qui lui sont associés sont immédiatement rendus inaccessibles aux autres utilisateurs de Facebook. Cela signifie que vous disparaissez réellement du site Facebook. Toutefois, nous sauvegardons les renseignements de votre profil (amis, photos, intérêts, etc.). Ainsi, si vous souhaitez le réactiver ultérieurement, votre compte aura exactement le même aspect et les mêmes contenus que lorsque vous l'avez désactivé. De nombreux utilisateurs désactivent temporairement leur compte et souhaitent retrouver leurs renseignements quand ils reviennent sur Facebook.

    « Si vous pensez ne plus jamais utiliser Facebook et que vous souhaitez supprimer définitivement votre compte, nous nous en chargerons. Gardez à l'esprit que vous ne serez pas en mesure de réactiver votre compte ou de récupérer tout contenu ou renseignement que vous avez ajoutés. Si vous souhaitez supprimer définitivement votre compte sans la possibilité de le récupérer, veuillez soumettre votre demande ici même » [traduction].

234. Toutefois, Facebook a souligné au Commissariat que la suppression des données était difficile sur le plan technique et qu'il était impossible de supprimer entièrement tous les renseignements du site. À la réunion de l'International Working Group on Data Protection in Telecommunications en septembre 2007, Facebook a affirmé que la période de conservation moyenne de données supprimées était de 10 à 15 jours, mais qu'elle pouvait être plus longue dans certaines parties du système.

235. La désactivation du compte signifie que le profil de l'utilisateur et tout le contenu connexe « disparaissent » du site même, mais que le compte demeure dans les serveurs de Facebook jusqu'à ce que l'utilisateur demande sa suppression ou le réactive. Dans la section Aide, sous la rubrique « Comment désactiver mon compte? » [traduction], Facebook explique ainsi la désactivation d'un compte :

    « Si vous vous inquiétez de savoir qui peut vous voir et ce qu'ils peuvent voir, n'oubliez pas que vous disposez d'un contrôle complet sur ces paramètres et que vous pouvez les modifier comme bon vous semble sur la page Confidentialité. Si vous souhaitez tout de même quitter Facebook, vous pouvez désactiver votre compte dans l'onglet "Paramètres" sur la page Compte. La désactivation éliminera complètement votre profil et tous les contenus associés à votre compte Facebook. De plus, les utilisateurs ne seront pas en mesure de vous rechercher ou de consulter vos renseignements. Si vous réactivez votre compte, votre profil sera rétabli dans son intégralité (amis, photos, intérêts, etc.) » [traduction].

236. Dans ses observations au Commissariat, Facebook a affirmé :

    « Nous offrons la désactivation aux utilisateurs qui souhaitent disparaître pour un moment; environ 50 % des utilisateurs qui désactivent leur compte reviennent dans le mois suivant la désactivation, et un petit nombre réactive son compte après cette période. L'information du compte de ces utilisateurs est conservée pour leur permettre de vivre une continuité s'ils souhaitent revenir. Lorsque le compte est désactivé, l'utilisateur n'est plus présent dans le site. [...] De nombreux utilisateurs ne savent pas s'ils reviendront et ils doivent avoir la possibilité de réactiver facilement leur compte » [traduction].

237. Au sujet de la conservation, Facebook a reconnu que les téléchargements des utilisateurs demeuraient dans le site jusqu'à ce qu'ils soient retirés par l'utilisateur ou à la demande de celui-ci. Selon Facebook, cette pratique reflète les attentes des utilisateurs puisqu'ils traitent leur compte Facebook comme un dépôt d'information. Par exemple, en octobre 2008, 10 milliards de photos

étaient affichées dans Facebook. L'entreprise estime qu'il serait inapproprié de limiter la durée du stockage d'information et qu'il ne serait pas dans le meilleur intérêt des utilisateurs de le faire.

238. La seule référence à la conservation de renseignements dans le site a été trouvée dans la Politique de confidentialité, et se lit comme suit :

« Quand vous utilisez Facebook, vous pouvez créer votre profil personnel, établir des liens, envoyer des messages, effectuer des recherches et envoyer des invitations, créer des groupes, organiser des événements, ajouter des applications, ainsi que transmettre de l'information par divers moyens. Nous recueillons ces renseignements afin de vous offrir un service et des fonctions personnalisés. Dans la plupart des cas, nous les conservons de façon à ce que, par exemple, vous puissiez retrouver les messages que vous avez envoyés ou consulter votre liste d'amis. Lorsque vous mettez à jour des données, nous conservons généralement une copie de sauvegarde des versions antérieures pendant un certain temps, afin de pouvoir les récupérer si nécessaire. [...]

« Vous comprenez et reconnaissez que, même après élimination, des copies de votre contenu d'utilisateur peuvent rester visibles dans les pages d'archives et les pages en cache, ou encore si d'autres utilisateurs ont enregistré ou copié votre contenu d'utilisateur. [...]

« Les renseignements éliminés seront conservés pendant une période raisonnable, mais ne seront généralement pas accessibles aux membres de Facebook.

« En revanche, quand vous utilisez les fonctions de communication du Site pour partager de l'information avec d'autres individus sur Facebook (p. ex., envoyer un message personnel à un autre utilisateur de Facebook), vous ne pouvez généralement pas éliminer ce type de communications » [traduction].

Application

239. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.4*d*), 4.5, 4.5.2, 4.5.3, 4.3.8 et 4.8.

240. Le principe 4.1.4*d*) stipule notamment que les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris, notamment, la rédaction des documents explicatifs concernant leurs politiques et procédures.

241. Le principe 4.5 prévoit entre autres qu'on ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins auxquelles ils ont été recueillis. Le principe 4.5.2 stipule notamment que les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels, et que ces lignes directrices devraient préciser les durées minimales et maximales de conservation. Le principe 4.5.3 établit entre autres qu'on devrait détruire, effacer ou dépersonnaliser les renseignements personnels qui ne sont plus nécessaires aux fins précisées.

242. Le principe 4.3.8 prévoit qu'une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable, et que l'organisation doit informer la personne des conséquences d'un tel retrait.

243. Le principe 4.8 précise qu'une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

Constatations

244. Dans l'ensemble, il m'apparaît que Facebook se conforme au principe 4.3.8 en offrant aux utilisateurs une option de suppression du compte, laquelle constitue en fait un mécanisme de retrait du consentement. Il m'apparaît également que la section Aide de Facebook explique adéquatement cette option par rapport à l'option de désactivation du compte. J'entretiens toutefois certaines préoccupations relativement à ces deux options.

245. Pour dire clairement, je ne propose pas que Facebook élabore une politique de rétention pour les comptes actifs. Mes préoccupations concernent plutôt les comptes désactivés. En vertu de la politique actuelle de désactivation des comptes de Facebook, les renseignements personnels des utilisateurs qui ont désactivé leur compte sont conservés indéfiniment. La conservation indéfinie contrevient aux principes 4.5 et 4.5.3. Selon moi, une personne raisonnable ne trouverait pas approprié que Facebook conserve indéfiniment les renseignements personnels d'un utilisateur qui a désactivé son compte depuis un bon moment et qui ne l'a jamais réactivé. Si je suis consciente qu'en désactivant leur compte, les utilisateurs choisissent en fait que Facebook

conserve temporairement les renseignements personnels inutilisés, je tiens à souligner que plus longue est la période pendant laquelle un compte est désactivé et les renseignements qu'il contient demeurent inutilisés, plus il est difficile d'argumenter que la conservation des renseignements personnels des utilisateurs est raisonnable aux mêmes fins de réseautage social pour lesquelles ils ont été recueillis. Je ne propose pas non plus de période de conservation précise pour les comptes désactivés. Facebook devrait plutôt établir une interruption de la conservation, qu'une personne raisonnable jugerait appropriée dans les circonstances, en se fondant sur ses expériences relatives à la réactivation des comptes. Facebook devrait également informer les utilisateurs de la durée de conservation au moment de la désactivation du compte.

246. En somme, concernant la conservation indéfinie des renseignements personnels des utilisateurs après la désactivation d'un compte, je constate que Facebook contrevient aux principes 4.5 et 4.5.3.

247. Deuxièmement, bien que je reconnaisse en gros que la section Aide de Facebook explique suffisamment bien les deux options, je trouve préoccupant, à l'instar de ce qu'avançait la CIPPIC, que d'offrir l'option de désactivation du compte uniquement à la page « Mon compte » risque de faire en sorte que certains utilisateurs croiront que la désactivation du compte est la seule option disponible. Je ne vois aucune raison qui empêcherait Facebook de présenter tout simplement une option de suppression du compte de même qu'une option de désactivation du compte à la page « Mon compte » de façon à représenter équitablement les deux options et qu'il soit clair aux yeux des utilisateurs qu'ils peuvent choisir entre les deux.

248. Enfin, je suis aussi préoccupée à l'idée qu'il n'y a aucune explication des options de suppression du compte et de désactivation du compte dans la Politique de confidentialité de Facebook. Je mentionne ailleurs dans le présent rapport que selon moi, par souci de commodité pour les utilisateurs intéressés, la politique de confidentialité d'une organisation doit expliquer les questions de protection de la vie privée, peu importe si elles sont expliquées ailleurs.

Recommandations et réponse

249. Dans mon rapport préliminaire, je recommandais à Facebook d'élaborer et de mettre en place une politique en matière de conservation de l'information en vertu de laquelle les renseignements personnels des utilisateurs qui ont

désactivé leur compte seraient supprimés des serveurs de Facebook après une période raisonnable, et d'en informer les utilisateurs.

250. J'ai suggéré également, à titre de pratique exemplaire dans l'intérêt de la clarté pour les utilisateurs, que Facebook :

    1) inclue une option de suppression du compte et une explication de sa différence avec la désactivation, dans les pages Paramètres du Compte de l'utilisateur;

    2) explique, dans sa Politique de confidentialité, la différence entre la suppression et la désactivation d'un compte.

251. En réponse à mes recommandations, Facebook a soulevé des objections pour les motifs suivants :

    « La plupart des utilisateurs qui désactivent leur compte le réactivent au cours des semaines qui suivent, et ceux qui le réactivent à une période ultérieure à quelques semaines s'attendent généralement à ce que leurs contacts sociaux soient intacts à leur retour. Puisque les utilisateurs ont accès à l'option de suppression des données, et parce que certaines données sont interdépendantes, il serait inapproprié, dans ce contexte, de fixer une date pour effacer les renseignements des utilisateurs sans tenir compte de leurs instructions à cet effet » [traduction].

252. La *Loi* est claire : une organisation ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées; une organisation devrait élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels et ces lignes directrices devraient préciser les durées minimales et maximales de conservation. Je reconnais que la période de conservation des renseignements personnels peut varier d'une organisation à l'autre selon les circonstances, mais je juge qu'il n'est ni nécessaire, ni raisonnable en l'espèce que Facebook conserve indéfiniment les renseignements personnels des comptes désactivés.

253. Je suis déçue que Facebook ait refusé d'adopter la première pratique exemplaire que j'ai proposée. Je continue de croire que l'ajout de l'option de suppression du compte sur la page « Mon compte » constitue une façon simple et efficace de promouvoir une transparence accrue à l'intention des utilisateurs.

254. Sur une note plus positive, je vois d'un œil favorable que Facebook ait accepté de mettre en œuvre la seconde pratique exemplaire que j'ai proposée. L'organisation a en effet suggéré d'ajouter le libellé suivant à la Politique de confidentialité :

> *« Les personnes désirant désactiver leur compte Facebook peuvent le faire sur la page "Mon compte". Les traces des renseignements éliminés pourraient être conservées sur des copies de sauvegarde pendant une durée raisonnable, mais ne seront généralement consultables par aucun des membres de Facebook. Les personnes désirant supprimer leur compte peuvent le faire en utilisant le formulaire ci-joint pour soumettre leur compte au processus de suppression, la complétion duquel peut prendre jusqu'à plusieurs semaines. »*

Conclusions

255. Par conséquent, je conclus que l'allégation est fondée pour autant qu'elle se rapporte aux principes 4.5 et 4.5.3.

256. Je demanderais à Facebook de reconsidérer mes recommandations. Dans le cadre du suivi que nous effectuerons dans les 30 jours, nous chercherons à savoir si ces recommandations ont été acceptées et mises en œuvre ou si des solutions de rechange acceptables ont été trouvées. Si nous ne disposons d'aucune preuve à cet effet, nous déterminerons le meilleur moyen de traiter ces problèmes et toute autre question non résolue conformément à nos pouvoirs.

Section 7b)

Comptes des utilisateurs décédés

Allégations

257. La CIPPIC a allégué que Facebook :

1) en ne mentionnant son intention de conserver le profil des utilisateurs décédés à des fins commémoratives que dans ses Conditions d'utilisation et non dans sa Politique de confidentialité, n'obtenait pas le consentement valable des utilisateurs pour cette utilisation de leurs renseignements personnels;

2) obligeait les utilisateurs, en dérogation au principe 4.3.3, à consentir à cette fin comme condition de service, même si la commémoration d'un profil n'est pas nécessaire à l'objectif principal de Facebook, soit le réseautage social.

258. La CIPPIC a précisé ainsi ses préoccupations :

- Facebook devrait, dans sa Politique de confidentialité et ses Conditions d'utilisation, informer les utilisateurs que le profil des utilisateurs décédés demeure actif à des fins commémoratives, conformément au principe 4.8.1.
- Facebook devrait offrir aux utilisateurs la possibilité de refuser l'affichage posthume de leur profil, conformément au principe 4.3.8.
- Facebook devrait mettre en place une procédure permettant aux proches d'un utilisateur décédé de demander le retrait du profil de l'utilisateur, conformément au paragraphe 5(3). La CIPPIC a suggéré « qu'une personne raisonnable ne s'attendrait pas à ce que Facebook continue à afficher le profil d'un utilisateur décédé si sa famille souhaite le contraire » [traduction].

Résumé de l'enquête

259. Au moment du dépôt de la plainte, Facebook indiquait dans ses Conditions d'utilisation, que les utilisateurs étaient tenus d'accepter lorsqu'ils s'inscrivaient, qu'elle se réservait le droit de garder ouvert le profil d'un utilisateur décédé à des fins commémoratives :

« Quand nous apprenons le décès d'un utilisateur, nous laissons généralement mais non systématiquement son compte ouvert à des fins commémoratives spéciales pour une durée déterminée par nous afin que les autres utilisateurs puissent afficher et lire des commentaires » [traduction].

260. À l'heure actuelle, la nouvelle Déclaration des droits et responsabilités (DDR), qui remplace les Conditions d'utilisation, ne mentionne pas la pratique de laisser les comptes Facebook ouverts à des fins commémoratives. Toutefois, la pratique elle-même se poursuit, comme on le constate à la lecture de cet extrait tiré des pages d'aide :

« J'aimerais signaler le décès d'un utilisateur ou demander la commémoration d'un compte.
« Veuillez ***entrer cette information ici*** *afin que nous puissions mettre le compte de cette personne en mode commémoration. Mettre un compte en mode commémoration retire certains renseignements de nature sensible, comme les mises à jour, et limite l'accès au profil aux amis confirmés seulement. Veuillez noter qu'afin de protéger la confidentialité de l'utilisateur décédé, nous ne pouvons pas donner le mot de passe d'accès au compte à qui que ce soit. Nous accédons aux demandes de fermeture complète d'un compte faites par des proches »* [traduction].

261. Le lien « entrer cette information ici » mène vers un formulaire qui exige le nom, la date de naissance, les adresses de courriel associées au compte et les réseaux de la personne décédée, ainsi que son lien de parenté avec le demandeur. Ce formulaire débute par la déclaration suivante :

« IMPORTANT : Ce formulaire sert strictement à rapporter le décès d'une personne aux fins de la commémoration d'un compte. Veuillez noter que les autres types de demandes faites par l'entremise de ce formulaire pourraient demeurer sans suite » [traduction].

262. Facebook n'estime pas que la commémoration d'un profil constitue une nouvelle fin au titre de la *Loi.* Dans ses observations au Commissariat, Facebook affirme :

« Notre politique permet aux proches de choisir si le profil sera conservé temporairement à des fins commémoratives ou gardé indéfiniment. [...] Les amis d'utilisateurs qui ont été tués [...] ont été heureux d'utiliser les pages Facebook à des fins commémoratives et [...] nous en avons conclu qu'un

proche parent était la personne appropriée pour décider si le défunt aurait voulu que sa page reste ouverte pour ses amis » [traduction].

Application

263. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.4*d*), 4.2.1, 4.2.3, 4.3.2, 4.3.3, 4.3.5, 4.3.6, 4.3.8 et 4.8.

264. Le principe 4.1.4*d)* stipule que les organisations doivent assurer la mise en œuvre de politiques et de pratiques destinées à donner suite aux principes, y compris la rédaction de documents explicatifs concernant leurs principes et procédures.

265. Le principe 4.2.1 prévoit qu'une organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe 4.8 (transparence) et au principe 4.9 (accès aux renseignements personnels).

266. Le principe 4.2.3 établit notamment qu'il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles les renseignements sont destinés.

267. Le principe 4.3.2 mentionne entre autres que les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés.

268. Le principe 4.3.3 prévoit qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

269. Le principe 4.3.5 stipule notamment que dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes.

270. Le principe 4.3.6 stipule entre autres que la façon dont une organisation obtient le consentement (explicite ou implicite) peut varier selon les circonstances et la nature des renseignements recueillis.

271. Le principe 4.3.8 prévoit qu'une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un

préavis raisonnable, et que l'organisation doit informer la personne des conséquences d'un tel retrait.

272. Le principe 4.8 précise qu'une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

Constatations

273. Dans mon rapport préliminaire, j'ai indiqué ce qui suit :

274. *« Notre enquête nous a permis d'identifier les sujets de préoccupation suivants concernant la pratique de Facebook visant à conserver les comptes des utilisateurs décédés à des fins commémoratives :*

    1) *En considération des principes 4.2.1, 4.2.3, 4.3.2 et 4.8, je suis préoccupée à l'idée qu'en limitant la description de cette pratique uniquement dans les Conditions d'utilisation, Facebook ne fait pas les efforts raisonnables pour s'assurer que les utilisateurs sont avisés de cet usage prévu des renseignements personnels. Je considère que la description dans les Conditions d'utilisation est adéquate. Toutefois, par égard pour ses utilisateurs et par souci de commodité, Facebook devrait également inclure une explication de cette pratique dans sa Politique de confidentialité.*

    2) *En considération des principes 4.3.3 et 4.3.8, je suis préoccupée à l'idée qu'en omettant de permettre à ses utilisateurs de refuser l'utilisation future de leurs renseignements personnels à des fins commémoratives, Facebook les oblige dans les faits à consentir à une fin non nécessaire comme condition de service.*

275. Concernant la première de mes préoccupations, je tiens à faire remarquer qu'en plus de ses Conditions d'utilisation, Facebook semble aussi avoir discontinué toute description adéquate de sa pratique de commémoration des comptes. La nouvelle DDR ne mentionne pas la pratique et je ne considère pas que la documentation de la rubrique Aide sur le signalement « des comptes à commémorer » constitue une description adéquate de la pratique, ni un avis adéquat aux utilisateurs. À mon avis, accorder un statut particulier, à des fins commémoratives, au compte d'un utilisateur décédé constitue une utilisation prévue des renseignements personnels de l'utilisateur. Aussi, cette pratique devrait-elle être bien documentée et les utilisateurs doivent en être avisés de façon appropriée. Que Facebook n'offre même plus de description claire de

cette pratique dans les Conditions d'utilisation ne fait qu'ajouter à mes préoccupations et me convainc d'autant plus que la description de cette pratique doit figurer dans la Politique de confidentialité.

276. Par conséquent, concernant la question d'aviser les utilisateurs de la pratique de commémoration des comptes, je constate que Facebook contrevient aux principes 4.2.1, 4.2.3, 4.3.2 et 4.8.

277. Quant à ma deuxième préoccupation, après avoir réexaminé la position que j'adoptais dans le rapport préliminaire, je prends position autrement en ce qui a trait au consentement de l'utilisateur à la commémoration des comptes.

278. En partant du principe que la pratique de conservation des comptes des utilisateurs décédés sous un statut commémoratif particulier constitue une utilisation de renseignements personnels à des fins non nécessaires, j'étais portée au départ à conclure que les allégations de la CIPPIC à cet effet étaient fondées en vertu des principes 4.3.3 et 4.3.8. Depuis, cependant, j'ai réexaminé la question à la lumière du principe 4.3.5.

279. Ce principe met l'accent sur la pertinence des attentes raisonnables d'une personne en matière de consentement. À mon avis, l'utilisateur moyen de Facebook verrait d'un œil favorable la possibilité d'être honoré à titre posthume par ses amis sur le site. De même, je suis persuadée que pour la plupart des utilisateurs, la possibilité de rendre un dernier hommage à des amis décédés et des confrères Facebook constitue une part importante de l'expérience du site de réseautage social. Je tiens aussi compte que dans le cadre du processus de commémoration du compte, Facebook prend soin de retirer les renseignements comme la mise à jour du profil et à limiter l'accès aux amis confirmés.

280. Il m'apparaît donc que la pratique de commémoration des comptes satisfait aux attentes raisonnables des utilisateurs et que Facebook peut donc continuer à invoquer le consentement implicite pour cette pratique. Je ne crois pas qu'un mécanisme de consentement négatif soit nécessaire dans les circonstances. Il faut toutefois aviser les utilisateurs de la pratique. Toutefois, comme je l'indique ci-dessus, Facebook devrait fournir au moins un fondement au consentement valable des utilisateurs à cette pratique en décrivant cette dernière dans la Politique de confidentialité

Recommandations et réponse

281. Dans mon rapport préliminaire, je recommandais à Facebook :

1) d’expliquer dans sa Politique de confidentialité, dans le contexte de tous les usages des renseignements personnels prévus, l’usage des renseignements personnels du compte des utilisateurs décédés prévu à des fins commémoratives;

2) d’offrir aux utilisateurs une façon de refuser l’usage par Facebook de leurs renseignements personnels à des fins commémoratives et les en aviser.

282. En réponse, Facebook a refusé de mettre en œuvre l’une ou l’autre des recommandations pour les raisons suivantes :

> *« Nous ne considérons toujours pas que la conservation des données en vue de permettre aux utilisateurs de rendre un dernier hommage à leurs amis constitue un nouvel usage aux termes de la LPRPDE. De toute façon, les utilisateurs sont parfaitement en mesure d’employer d’autres moyens pour exprimer leurs souhaits sur cette question. Nous croyons aussi qu’il serait inapproprié de créer dans de tels cas des normes de traitement des renseignements qui divergeraient des normes juridiques existantes en matière de disposition des biens d’une succession »* [traduction].
>
> Facebook a également précisé que les services relatifs à l’accès aux biens numériques en cas de décès étaient assurés par des fournisseurs privés.

Conclusions

283. Je conclus que les allégations sont fondées par rapport à l’exigence de consentement, et bien fondées par rapport à la documentation et à la notification.

284. Je n’insisterai pas sur la mise en œuvre de ma deuxième recommandation. Toutefois, je maintiens ma première recommandation; j’exhorte Facebook de la reconsidérer.

285. Dans le cadre du suivi que nous effectuerons dans les 30 jours concernant d’autres enjeux, nous chercherons à savoir si ma première recommandation a été acceptée et mise en œuvre. Si nous ne disposons d’aucune preuve à cet effet, nous déterminerons le meilleur moyen de traiter ce problème et toute autre question non résolue conformément à nos pouvoirs.

Section 8

Renseignements personnels des non-utilisateurs

Allégations

286. La CIPPIC a allégué que Facebook n'obtenait pas le consentement des non-utilisateurs au téléchargement de leurs renseignements personnels vers le site, en dérogation au principe 4.3.

287. À cet égard, la plainte de la CIPPIC porte sur la collecte et l'usage par Facebook des renseignements personnels de non-utilisateurs dans les situations suivantes :

1) Des utilisateurs peuvent publier des renseignements personnels de non-utilisateurs dans leur profil et celui d'autres utilisateurs par des fonctionnalités comme les « Actualités » et le « Mur ». En outre, les utilisateurs peuvent étiqueter des non-utilisateurs sur des photos ou dans des vidéos.

2) Les utilisateurs peuvent fournir l'adresse de courriel de non-utilisateurs pour les inviter à s'inscrire au site.

288. La CIPPIC a précisé ses préoccupations ainsi :

- Dans le cas des étiquettes associées à des photos et des vidéos, les renseignements personnels sont diffusés dans le site Facebook. Les non-utilisateurs ne sont pas avisés que leurs renseignements personnels ont été fournis à Facebook ni qu'ils peuvent être vus. Les non-utilisateurs ne peuvent retirer l'étiquette à moins de s'inscrire à Facebook. Certains renseignements personnels sur des photographies ou dans des vidéos peuvent être délicats, car il n'est pas exclu qu'elles représentent le non-utilisateur dans des situations qui risquent de ternir sa réputation et l'empêcher d'obtenir un emploi potentiel; Facebook devrait donc obtenir le consentement explicite des non-utilisateurs, conformément au principe 4.3.5.
- Afin d'envoyer à des non-utilisateurs des invitations à se joindre au site, Facebook recueille auprès d'utilisateurs les adresses de courriel de non-utilisateurs et conserve ces adresses indéfiniment à moins que les non-utilisateurs fassent une demande de suppression. En outre, elle n'informe pas les non-utilisateurs que leurs adresses de courriel sont

conservées ni qu'il peuvent en demander la suppression. Facebook peut, selon la CIPPIC, produire une invitation sans conserver l'adresse du non-utilisateur. La conservation par Facebook des adresses de courriel des non-utilisateurs pour toute période prolongée à leur insu et sans leur consentement contrevient au principe 4.3.

- Facebook devrait interdire aux utilisateurs de publier de l'information sur des non-utilisateurs sans leur consentement et imposer le retrait unilatéral de matériel non autorisé. Dans certaines circonstances, comme la publication persistante d'information de non-utilisateurs, Facebook devrait imposer une sanction plus sévère, comme la résiliation du compte.
- Facebook devrait fournir aux non-utilisateurs une façon efficace de trouver leurs renseignements personnels et de les retirer du site. La CIPPIC est d'avis qu'il est inacceptable que Facebook néglige de fournir une telle possibilité aux non-utilisateurs et que cette omission contrevient au paragraphe 5(3) de la *Loi*.

289. CIPPIC a allégué également que les non-utilisateurs qui sont étiquetés sur des photos ou dans des vidéos peuvent faire l'objet d'une recherche dans le site, ce que Facebook nie. Le Commissariat n'a trouvé aucune preuve au soutien de l'allégation.

Résumé de l'enquête

290. La Politique de confidentialité de Facebook aborde les renseignements personnels de non-utilisateurs seulement dans le contexte du service d'invitation :

« Si vous utilisez notre service d'invitation pour informer un ami au sujet de notre site, nous vous demanderons de fournir l'information dont nous aurons besoin pour envoyer l'invitation, comme l'adresse de courriel de votre ami. Nous enverrons à votre ami un seul courriel ou message instantané pour l'inviter à visiter le site. Facebook conserve cette information pour envoyer l'invitation unique, pour établir un lien entre vous deux si votre invitation est acceptée et pour mesurer le succès obtenu par notre programme d'invitation. Votre ami peut nous joindre à info@facebook.com pour nous demander de retirer cette information de notre base de données » [traduction].

La Politique de confidentialité ne traite pas de la question du consentement des non-utilisateurs.

291. Au moment du dépôt de la plainte, les Conditions d'utilisation et le Code de conduite interdisaient tous deux la publication de renseignements qui contreviendraient au droit à la vie privée de tiers, y compris les coordonnées, le numéro d'assurance sociale et les numéros de carte de crédit. Toutefois, le libellé utilisé ne mentionne pas expressément l'obtention du consentement de non-utilisateurs avant la publication de leurs renseignements personnels.
292. La nouvelle Déclaration des droits et responsabilités (DDR), qui remplace les Conditions d'utilisation et le Code de conduite, comprend la section suivante, intitulée « Protéger les droits d'autrui » [traduction] :

    « Nous respectons les droits d'autrui et nous nous attendons à ce que vous fassiez de même.
    1. Vous n'afficherez pas de contenu et ne ferez aucune action sur Facebook qui violerait les droits d'une autre personne ou contreviendrait à la loi de toute autre manière.
    2. Nous pouvons retirer tout contenu que vous affichez sur Facebook si nous jugeons qu'il va à l'encontre de la présente Déclaration.
    3. Nous vous fournirons les outils dont vous avez besoin pour protéger vos droits de propriété intellectuelle. Pour en savoir davantage, visitez notre page intitulée ***Comment alléguer une violation de vos droits de propriété intellectuelle****.*
    4. Si nous avons retiré votre contenu parce qu'il allait à l'encontre des droits de propriété intellectuelle d'une autre personne mais que vous croyez qu'il y a erreur, nous vous donnerons ***l'occasion de faire appel****.*
    5. Si vous violez de manière répétée les droits de propriété intellectuelle d'autres personnes, nous fermerons votre compte le cas échéant.
    6. Vous n'utiliserez pas notre contenu protégé par le droit d'auteur ou nos marques de commerce (y compris Facebook, les logos Facebook et F, FB, Face, Poke, Mur et 32665) sans notre permission écrite.
    7. Si vous recueillez de l'information de la part d'autres utilisateurs, vous obtiendrez leur consentement, direz clairement que c'est bien vous (et non Facebook) qui recueille ces renseignements et afficherez une politique de confidentialité expliquant quels renseignements vous recueillez et comment vous utiliserez ces renseignements.
    8. Vous n'afficherez pas des documents d'identification ou des renseignements financiers de nature délicate sur Facebook » [traduction].

293. La DDR n'aborde pas précisément l'obtention du consentement pour télécharger les renseignements personnels de tiers. De plus, contrairement aux Conditions d'utilisation et au Code de conduite antérieurs, elle ne précise pas

que le droit à la vie privée de tiers fait partie des droits auxquels les utilisateurs ne doivent pas contrevenir.

294. À l'égard des photographies, Facebook a déclaré dans ses observations au Commissariat que « les utilisateurs décidaient eux-mêmes ce qu'ils voulaient publier » et que, en vertu des lois sur le droit d'auteur, « les droits de reproduction d'une photographie ou d'une vidéo appartiennent généralement à celui qui l'a prise ou filmée » [traduction]. Le Commissariat en a déduit que Facebook croit que la responsabilité de l'obtention du consentement d'un non-utilisateur ne lui incombe pas, mais repose sur les utilisateurs qui téléchargent des renseignements personnels de non-utilisateurs.

295. Dans Facebook, les utilisateurs peuvent étiqueter — identifier sur une photographie — toute personne apparaissant sur une photo affichée sur le site. Quand un utilisateur affiche une photo, Facebook lui demande s'il désire ajouter une étiquette à la photo. Facebook permet l'étiquetage de non-utilisateurs, mais permet seulement aux utilisateurs de faire retirer l'étiquette. Facebook offre une fonction qui permet à l'utilisateur d'entrer l'adresse de courriel de la personne étiquetée sur une photo. À partir de l'adresse de courriel, Facebook peut déterminer si la personne étiquetée est un non-utilisateur. Facebook envoie alors un message au non-utilisateur l'informant qu'il a été étiqueté sur une photo, lui fournissant un lien vers cette photo et l'invitant à se joindre à Facebook. Les non-utilisateurs qui souhaitent retirer une étiquette à leur sujet sur une photo ne peuvent le faire à moins de se joindre à Facebook.

296. Indépendamment des étiquettes associées aux photos, Facebook mène un programme d'invitations, dans le cadre duquel elle demande aux utilisateurs de fournir l'adresse de courriel de non-utilisateurs pour les inviter à s'inscrire au site. Sur la page « Invitez vos amis », les utilisateurs peuvent fournir des adresses une à une ou permettre à Facebook d'accéder au carnet d'adresses de leurs comptes de courriel Web ou applications de courriel. La page ne fait aucune mention d'exiger le consentement des non-utilisateurs.

297. L'invitation envoyée par Facebook aux non-utilisateurs permet à l'invité de se retirer de toute liste d'envoi commercial de Facebook. Si un invité décline l'invitation de se joindre à Facebook, le prochain utilisateur qui tentera d'envoyer une invitation au même non-utilisateur recevra un message indiquant que la personne en question ne peut pas être invitée. Le non-utilisateur n'est pas informé que Facebook conserve l'adresse de courriel même si l'invitation est refusée.

298. Dans ses observations au Commissariat, Facebook a affirmé ainsi sa position :

> *« Facebook conserve une adresse de courriel à laquelle une invitation est envoyée ainsi que l'information précisant le compte qui a envoyé l'invitation afin d'établir un lien entre les deux personnes si l'invitation est acceptée. Les invitations sont également conservées afin que les utilisateurs puissent établir des liens avec tous ceux qui les ont invités, principalement dans l'intérêt des utilisateurs ayant téléchargé les coordonnées, pour leur permettre de savoir si leur ami (soit une personne dont ils avaient déjà l'adresse de courriel) s'inscrit au service »* [traduction].

299. Facebook a confirmé également que les adresses de courriel ne servent qu'au service d'invitation et ne sont accessibles par aucun utilisateur du service, à l'exception de celui qui les a fournies. Facebook reconnaît qu'elle conserve les adresses indéfiniment, à moins de recevoir une demande de retrait de la part d'un non-utilisateur.

300. À la page « Inviter des amis », la fonction « Historique des invitations » permet aux utilisateurs de voir toutes leurs invitations, y compris les membres qui se sont inscrits grâce à eux. Lorsque des non-utilisateurs s'inscrivent à Facebook, toutes les demandes d'ajout d'amis qu'ils ont reçues apparaîtront à leur page d'accueil.

Application

301. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.3 et 4.5.

302. Le principe 4.3 précise que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

303. Le principe 4.5 prévoit entre autres qu'on ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

Constatations

304. Dans mon rapport préliminaire, j'ai indiqué ce qui suit :

305. *« Notre enquête nous a permis d'identifier les sujets de préoccupation suivants concernant le traitement des renseignements des non-utilisateurs par Facebook :*

    1) *En considération du principe 4.3, je suis préoccupée à l'idée que Facebook n'obtient pas le consentement éclairé des non-utilisateurs pour les étiqueter sur des photos. À mon avis, puisque l'entreprise a rendu l'étiquetage possible et utilise les photos étiquetées pour inviter les non-utilisateurs à devenir membres, il incombe à Facebook d'obtenir le consentement des non-utilisateurs.*

    2) *Toujours en considération du principe 4.3, je suis préoccupée à l'idée que Facebook n'obtient pas le consentement des non-utilisateurs au regard de son service d'invitation, par lequel il encourage activement les utilisateurs à fournir les adresses de courriel de non-utilisateurs, utilise ces adresses pour envoyer des invitations aux non-utilisateurs, conserve les adresses indéfiniment et utilise à nouveau ces adresses pour fournir aux utilisateurs un bilan des invitations et un suivi du succès du programme d'invitations.*

    3) *En considération du principe 4.5, je suis préoccupée à l'idée que dans l'éventualité où un non-utilisateur refuserait l'invitation de se joindre à Facebook, l'entreprise conserve néanmoins indéfiniment l'adresse de courriel du non-utilisateur aux fins de fournir à l'utilisateur un bilan des invitations et un suivi du succès du programme d'invitations. »*

306. En présentant mes préoccupations, j'ai pris soin de faire une distinction claire entre les activités d'un utilisateur de Facebook à des fins purement personnelles et les activités auxquelles Facebook prend part. Lorsque les utilisateurs affichent de l'information au sujet de non-utilisateurs sur leur page de profil, leur Mur ou dans les Actualités, ces affichages sont réalisés à des fins personnelles et ne sont pas du ressort de la *Loi*. La *Loi* s'appliquerait seulement quand Facebook utilise les renseignements personnels des non-utilisateurs à ses propres fins.

307. Aviser les non-utilisateurs par courriel qu'ils ont été étiquetés sur des photos est l'une de ces activités. Lorsqu'un utilisateur identifie un non-utilisateur, on offre à l'utilisateur la possibilité de télécharger l'adresse de courriel du non-utilisateur. Facebook se sert ensuite de cette adresse pour aviser le non-utilisateur de la photo étiquetée et pour l'inviter à se joindre à Facebook. Il ne fait pas de doute que les non-utilisateurs ont avantage à être informés qu'ils ont été étiquetés. Toutefois, Facebook en tire aussi profit puisqu'il a la chance

d’inviter un nouveau membre potentiel et que sa capacité de générer des revenus est étroitement liée au nombre de membres.

308. Le service d’invitation par courriel est une autre activité menée par Facebook. Facebook soutient que ce service est offert pour le bénéfice des utilisateurs, mais il est clair qu’il permet aussi à Facebook d’attirer de nouveaux membres et, par conséquent, d’augmenter sa capacité de générer des revenus.

309. Selon moi, Facebook devrait assumer une part de la responsabilité d’obtenir le consentement des personnes dans ce contexte. Mais la responsabilité sous quelle forme?

310. Au départ, j’étais d’avis que Facebook devait avoir la responsabilité *d’obtenir*, directement auprès des non-utilisateurs, le consentement à l’étiquetage des photos et à la collecte et à l’utilisation de leur adresse de courriel aux fins d’invitation. J’affirmais en effet qu’il « incombe à Facebook d’obtenir le consentement des non-utilisateurs ». Cependant, après mûre réflexion, je perçois la question de la responsabilité sous un éclairage nouveau.

311. À mon avis, l’étiquetage représente une utilisation personnelle des utilisateurs de Facebook. Que Facebook fasse en sorte que l’étiquetage de photos est possible ne suffit pas à ce que l’entreprise soit responsable du consentement, pas plus que le fait qu’elle rend d’autres caractéristiques possibles, comme le Mur et les Actualités. Je continue tout de même de croire que la responsabilité du consentement doit être assumée au moment du processus d’étiquetage où Facebook entreprend de solliciter l’adresse de courriel des non-utilisateurs auprès des utilisateurs dans l’intention de s’en servir à ses propres fins.

312. De plus, le principe 4.3 stipule que la personne doit être informée de l’utilisation et y consentir. Dans les cas où une des parties recueille auprès d’une deuxième partie les renseignements personnels d’un tiers, le Commissariat a déterminé, dans des affaires précédentes, que dans certaines circonstances, il pourrait incomber à la deuxième partie (dans le présent cas, l’utilisateur Facebook) d’obtenir le consentement directement auprès du tiers (dans le présent cas, le non-utilisateur). Nous avons également déterminé que dans de tels cas, la première partie (Facebook, dans ce cas-ci) bien qu’elle n’ait pas la responsabilité d’obtenir directement le consentement, doit néanmoins instaurer des mesures raisonnables pour s’assurer que la deuxième partie obtiendra le consentement. En d’autres mots, la première partie doit faire preuve de diligence raisonnable pour garantir que l’exigence de consentement soit satisfaite.

313. Par conséquent, il m’apparaît satisfaisant que Facebook s’en remette aux utilisateurs pour obtenir le consentement des non-utilisateurs, pour autant que

l'entreprise elle-même fasse preuve de diligence raisonnable. De plus, il me semble que la diligence raisonnable dans de pareilles circonstances consisterait à faire les démarches appropriées pour s'assurer que les utilisateurs sont bien informés qu'ils doivent obtenir le consentement des non-utilisateurs avant de communiquer l'adresse de courriel à Facebook. Cela signifie qu'il faut non seulement informer les utilisateurs de l'exigence de consentement dans la Politique de confidentialité, mais aussi les aviser de cette exigence chaque fois qu'ils communiquent l'adresse de courriel d'un non-utilisateur à Facebook. Cela signifie aussi qu'il faudra prévoir l'exécution de mesures punitives à l'endroit des utilisateurs qui contreviennent à l'exigence de consentement.

314. Malheureusement, ni à l'heure actuelle ni par le passé, Facebook ne fait preuve de diligence raisonnable en ce qui a trait au consentement des non-utilisateurs. Aussi, je constate que Facebook contrevient au principe 4.3 à cet égard.

315. Que Facebook *conserve* l'adresse de courriel des non-utilisateurs après l'usage initial représente un autre problème; à cet effet, l'entreprise est responsable dans une bien plus grande mesure. Lorsqu'elle invite directement les non-utilisateurs, Facebook a, mais ne profite pas de, l'occasion d'informer les personnes concernées de ses intentions futures, ni ne leur offre-t-elle la chance de refuser que leur adresse de courriel soit conservée afin qu'on leur fasse parvenir un bilan des invitations et le suivi du succès du programme d'invitations. Facebook conserve et utilise donc à ces fins les renseignements personnels des non-utilisateurs à leur insu et sans leur consentement. Par conséquent, je constate que l'entreprise contrevient une fois de plus au principe 4.3 à cet égard.

316. Je constate également qu'en conservant l'adresse de courriel des non-utilisateurs indéfiniment, au-delà des fins initiales de la collecte, Facebook contrevient au principe 4.5.

Recommandations et réponse

317. Dans mon rapport préliminaire, je recommandais à Facebook :

    1) d'examiner et de mettre en place des mesures afin d'aborder les préoccupations quant au fait que les non-utilisateurs ignorent qu'ils ont été étiquetés sur une photo et qu'ils n'ont pas l'occasion d'y consentir;

    2) d'examiner et de mettre en place des mesures pour améliorer le service d'invitation afin d'aborder la préoccupation du Commissariat quant au fait que les non-utilisateurs ignorent que Facebook recueille, utilise et conserve leur adresse de courriel, et qu'ils n'y consentent pas;

3) d’établir une limite raisonnable de conservation des adresses de courriel de non-utilisateurs pour les besoins du suivi de l’historique des invitations et du succès du programme d’invitations.

318. En réponse à mes deux premières recommandations, Facebook a refusé de les mettre en œuvre pour les motifs suivants :

« Facebook croit continuer d’informer les non-utilisateurs, dans une mesure toujours plus grande, que notre site Web renferme des renseignements sur eux — nous le faisons dans une plus grande mesure que n’importe quel autre site Web. Si les non-utilisateurs souhaitent bloquer tous les avis futurs, nous accédons à leur demande et les données sont conservées sous la conduite de l’utilisateur qui les a téléchargées au départ; il serait inapproprié que Facebook prenne des mesures pour supprimer les données sans l’intervention de la personne qui les a téléchargées au départ » [traduction].

319. En ce qui a trait à la pratique d’étiquetage des non-utilisateurs, Facebook a fait les commentaires suivants :

« En ce qui concerne les photographies, l’infrastructure d’étiquetage de Facebook offre aux utilisateurs davantage d’information que n’importe quel autre site Web par rapport à une photo qui nécessite potentiellement l’attention de la personne concernée. Sur la plupart des sites Web, il est possible de télécharger la photo d’une personne à l’insu de celle-ci. Facebook prévoit un moyen de les en aviser et de communiquer avec la personne qui a téléchargé la photo, au besoin. Pour un non-utilisateur, il peut s’agir d’ajouter une adresse de courriel à une étiquette. De plus, l’infrastructure d’étiquetage est conçue de façon à ce que la personne étiquetée puisse retirer l’étiquette et bloquer tout courriel futur si c’est ce qu’elle souhaite » [traduction].

320. Dans l’ensemble, Facebook avance que les données des non-utilisateurs sont sous la responsabilité des utilisateurs qui les ont téléchargées, que l’étiquetage de photos et le service d’invitation constituent des utilisations personnelles des utilisateurs et que Facebook donne plus d’information aux non-utilisateurs que n’importe quel autre site Web au sujet de la présence de leurs données sur le site.

321. À l’instar de toutes mes autres recommandations relatives à la conservation, Facebook n’a fourni aucune réponse directe à la troisième recommandation ci-dessus.

Conclusions

322. Je conclus que les allégations par rapport au consentement et à la conservation dans le contexte des invitations sont fondées. Je demanderais à Facebook de reconsidérer les recommandations 2 et 3 à la lumière des constatations présentées ci-dessus. Dans le cadre du suivi que nous effectuerons dans les 30 jours, nous chercherons à savoir si ces recommandations ont été acceptées et mises en œuvre ou si des solutions de rechange acceptables ont été trouvées. Si nous ne disposons d'aucune preuve à cet effet, nous déterminerons le meilleur moyen de traiter ces problèmes et toute autre question non résolue conformément à nos pouvoirs.

Section 9

Facebook Mobile et mesures de sécurité

Allégations

323. En ce qui concerne les utilisateurs de la version mobile du site Facebook (Facebook Mobile), la CIPPIC a allégué que, en fournissant aux utilisateurs un témoin persistant sans date de péremption apparente, Facebook ne protégeait pas adéquatement les renseignements personnels des utilisateurs, en dérogation aux principes 4.7, 4.7.1 et 4.7.3.

324. Plus précisément, la CIPPIC a émis les préoccupations suivantes au sujet de la sécurité :

    (1) Si un utilisateur se sert de l'appareil sans fil d'un autre personne pour ouvrir une session sur Facebook puis oublie de fermer la session, l'autre personne aura accès indéfiniment au compte Facebook de l'utilisateur, même si ce dernier change son mot de passe.

    (2) Si un utilisateur donne son mot de passe de compte Facebook à une autre personne, cette dernière peut ouvrir une session sur un appareil sans fil et obtenir accès indéfiniment, même si l'utilisateur change son mot de passe.

325. Selon la CIPPIC, le témoin de connexion laissé par Facebook devrait être périmé après une période raisonnable et chaque fois qu'un utilisateur modifie son mot de passe en ligne.

326. En raison du travail de recherche nécessaire, le Commissariat a mené une enquête distincte au sujet de cette allégation, portant un numéro de dossier différent des autres allégations faites par la CIPPIC dans sa plainte contre Facebook. Cette allégation n'a pas été incluse dans notre rapport préliminaire.

Résumé de l'enquête

327. Les témoins de connexion sont de petits fichiers textes incorporés aux requêtes et réponses HTTP, et échangés entre un navigateur et un serveur Web. Ils sont émis par le serveur Web la première fois qu'un utilisateur visite un site. Ils sont conservés dans le navigateur Web qui se trouve sur l'ordinateur ou l'appareil de

l'utilisateur. Un témoin persistant demeure sur l'ordinateur ou l'appareil de l'utilisateur même après la fin de la session, jusqu'à une date de péremption préétablie.

328. Dans le cas particulier de Facebook Mobile, le témoin persistant sert à éviter aux utilisateurs d'ouvrir une nouvelle session chaque fois qu'ils se servent d'un appareil sans fil pour accéder à Facebook.

329. Le site Facebook est accessible de plusieurs manières à partir d'un appareil sans fil comme un BlackBerry ou un iPhone. La méthode citée explicitement dans l'allégation de la CIPPIC est d'entrer http://m.facebook.com dans le navigateur de l'appareil sans fil. Cette option de rechange à l'adresse www.facebook.com offre une présentation visuelle mieux adaptée aux écrans restreints des appareils sans fil et est recommandée pour le navigateur du BlackBerry et pour Internet Explorer Mobile.

330. Le Commissariat a retenu les services d'une société d'ingénierie informatique pour tester la manière dont différents appareils sans fil interagissent avec m.facebook.com.

Aperçu des tests

331. Nous avons testé la gestion de session sur m.facebook.com à partir de quatre plateformes :

    1) BlackBerry;
    2) iPhone;
    3) Windows Mobile;
    4) ordinateur de bureau.

    Les appareils sans fil retenus représentent la majorité des appareils sans fil comprenant des navigateurs Web.

332. Les tests suivants ont été effectués sur chaque plateforme :

    1) Charger le site Web m.facebook.com à partir du navigateur de l'appareil sans fil en fournissant un nom d'utilisateur et un mot de passe.
    2) Vérifier la péremption du témoin en laissant s'écouler la période de temps indiquée dans le témoin puis en tentant d'effectuer une action sur le message d'état dans Facebook.

3) Modifier des données personnelles sur m.facebook.com avant de modifier le mot de passe à partir d'un ordinateur de bureau.
4) Modifier des données personnelles sur m.facebook.com après avoir modifié le mot de passe à partir d'un ordinateur de bureau.

333. Les résultats des tests ont été essentiellement les mêmes pour chaque plateforme. Ce résultat était prévisible, puisque le fonctionnement de m.facebook.com est déterminé par le serveur et non par l'appareil sans fil.

Date de péremption du témoin (tests 1 et 2)

334. La première fois qu'un utilisateur ouvre une session sur le site m.facebook.com, un message HTTP POST comprenant le nom d'utilisateur et le mot de passe est envoyé à l'hôte m.facebook.com. Facebook envoie alors une réponse 302 HTTP acceptant la demande et redirigeant essentiellement le navigateur vers la page d'accueil de Facebook.

335. Sont compris dans la réponse de nombreux en-têtes « Set-Cookie » demandant au navigateur de sauvegarder des témoins précis afin d'identifier la session. Cinq témoins sont envoyés au navigateur par Facebook dans sa réponse.

336. Les tests ont permis de déterminer que l'un de ces témoins est le témoin persistant que m.facebook.com utilise pour identifier et enregistrer la session d'un utilisateur pour une période pouvant aller jusqu'à 14 jours. Des tests ultérieurs ont permis de confirmer qu'après la période de 14 jours, on demande à l'utilisateur de confirmer son identité. On doit noter, toutefois, que chaque fois qu'un utilisateur accède au site m.facebook.com, la date de péremption du témoin est prolongée de 14 jours.

337. Facebook a admis utiliser un témoin persistant de 14 jours sur m.facebook.com. Selon Facebook, « un témoin persistant sert à offrir aux utilisateurs un accès pratique à leurs renseignements » [traduction].

338. Dans ses observations au Commissariat, Facebook a répondu ainsi aux allégations de la CIPPIC :

« Les pratiques de Facebook relatives à l'accès mobile ne diffèrent pas des pratiques dominantes de tout service auquel on peut se brancher à partir d'appareils sans fil. Permettre des ouvertures de session à répétition une fois que l'appareil a été authentifié est une pratique courante. Par exemple, le

réglage par défaut du service BlackBerry n'est pas d'exiger une authentification complexe à chaque utilisation. Certains utilisateurs choisissent d'utiliser un mot de passe sur leur BlackBerry comme mesure de sécurité additionnelle, tout comme certains pourraient choisir de fermer la session sur Facebook sur leur appareil sans fil de manière à devoir la rouvrir explicitement la prochaine fois. Il ne s'agit pas d'une obligation selon toute interprétation raisonnable de la LPRPDE, avec raison » [traduction].

339. Les utilisateurs peuvent fermer leur session sur Facebook en faisant défiler l'écran jusqu'au bouton LOGOUT. Tant sur m.facebook.com que sur www.facebook.com, un témoin persistant distinct est utilisé pour conserver le nom d'utilisateur, mais pas le mot de passe. En d'autres mots, quand les utilisateurs ouvrent une nouvelle session sur Facebook, leurs adresses de courriel sont déjà en mémoire, mais ils doivent entrer à nouveau leurs mots de passe.

340. Dans sa Politique de confidentialité, Facebook aborde son utilisation de témoins en ces termes :

« Quand vous entrez sur Facebook, nous enregistrons votre type de navigateur et votre adresse IP. Ces renseignements sont recueillis pour chaque visiteur du site Facebook. Nous enregistrons également certains renseignements à partir de votre navigateur en nous servant de témoins. Un témoin est un élément de données enregistré sur l'ordinateur d'un utilisateur et lié à de l'information au sujet de ce dernier. Nous utilisons des témoins identificateurs de session pour confirmer qu'un utilisateur a une session en cours. Ces témoins disparaissent une fois que l'utilisateur ferme le navigateur. Par défaut, nous utilisons un témoin persistant qui comprend votre nom d'utilisateur (mais pas votre mot de passe) afin de faciliter l'ouverture de session quand vous revenez sur Facebook. Si vous voulez désactiver cette fonction de commodité, vous pouvez supprimer ou bloquer le témoin en question à partir des paramètres de votre navigateur » [traduction].

341. La Politique de confidentialité ne fait aucune référence précise au témoin persistant de 14 jours utilisé sur m.facebook.com. Lorsqu'on leur a demandé si l'utilisation de témoins persistants était abordée ailleurs sur le site Facebook, les représentants du site ont répondu ainsi :

« On fait référence aux témoins dans la Politique de confidentialité au niveau de détail approprié, et toute précision sémantique sera effectuée dans la révision prochaine de la Politique de confidentialité » [traduction].

Résultats après un changement de mot de passe (tests 3 et 4)

342. Après avoir ouvert une session sur m.facebook.com à partir d'un appareil sans fil, nous avons utilisé une plateforme différente pour modifier le mot de passe du compte Facebook en question. Nous avons ensuite tenté de faire une action sur le compte Facebook à partir de l'appareil sans fil. Notre tentative s'est soldée par un échec; nous avons plutôt été redirigés vers l'écran d'ouverture de session et obligés à nous identifier de nouveau.

Résumé des tests menés sur m.facebook.com

343. Les tests ont révélé ce qui suit au sujet des quatre plateformes :

- Quand les utilisateurs ouvrent une session sur m.facebook.com, que ce soit à partir d'un appareil sans fil ou d'un ordinateur de bureau, le site Facebook renvoie un témoin persistant dont la date de péremption valide est de 14 jours.

- Une fois que le témoin est périmé, toute action entreprise sur le site Web nécessite une réauthentification.

- Contrairement à l'allégation faite par la CIPPIC, si le mot de passe est modifié sur une autre plateforme, toute demande subséquente effectuée à partir d'un appareil sans fil ayant une session en cours sur m.facebook.com est refusée par Facebook et l'on demande à l'utilisateur de s'identifier de nouveau.

Examen de l'industrie

344. À la suite d'un examen, le Commissariat a déterminé qu'il n'existe au sein de l'industrie aucune spécification ou norme officielle de gestion de session à laquelle les sites Web doivent se conformer. Toutefois, nous avons appris qu'une organisation connue sous le nom d'Open Web Application Security Project (OWASP) préconise le développement d'applications sécurisées et a élaboré de nombreuses lignes directrices portant sur la gestion de session. Entre autres, l'OWASP recommande aux concepteurs de sites Web que les sessions devraient avoir un délai d'attente de 5 minutes pour les applications à valeur supérieure, de 10 minutes pour celles à valeur moyenne et de 20 minutes pour celles à valeur inférieure. Bien que l'OWASP n'ait pas fourni de définitions concrètes pour les données à valeur supérieure, moyenne et inférieure, il cite les systèmes comptables, bancaires et de bourse en ligne et

les dossiers de santé et du gouvernement comme exemples de valeur supérieure, et les blogues et forums de discussion comme exemples de valeur inférieure.

345. Toutefois, l'examen fait par le Commissariat de la manière dont divers sites Web gèrent les sessions laisse entendre que les lignes directrices de l'OWASP ne sont pas utilisées à grande échelle au sein de l'industrie. La plupart des sites Web semblent réfractaires à demander aux utilisateurs de s'identifier de nouveau après une période d'inactivité relativement courte, puisque cela pourrait miner la convivialité du site. Certains sites bancaires offrant des services en ligne exigent une réauthentification après une période d'inactivité relativement courte (p. ex., 30 minutes dans un cas et 10 minutes dans un autre).

346. Dans l'ensemble, tout porte à croire qu'au sein de l'industrie, la commodité de l'utilisateur a préséance sur les enjeux de sécurité dans le contexte de la gestion de session pour les applications lancées à partir d'appareils sans fil. Toutefois, on doit noter que les utilisateurs peuvent toujours protéger l'ensemble de leur appareil à l'aide d'un mot de passe, tout comme ils peuvent le faire sur un ordinateur de bureau ou portable.

Application

347. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.4, 4.7, 4.7.1, 4.7.3 et 4.8.

348. Le principe 4.1.4 stipule notamment que les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris la rédaction des documents explicatifs concernant leurs politiques et procédures. Le principe 4.8 stipule qu'une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

349. Le principe 4.7 stipule que les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Le principe 4.7.1 stipule notamment que les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Le principe 4.7.3 stipule entre autres que les méthodes de protection devraient comprendre des mesures techniques.

Constatations

350. La CIPPIC a signalé qu'elle était préoccupée par deux scénarios potentiels d'accès non autorisé des renseignements personnels d'utilisateurs de Facebook et d'utilisation non autorisée de ces derniers, par l'entremise d'appareils sans fil. Facebook fournit à ma satisfaction aux utilisateurs un moyen simple de fermer des sessions sur m.facebook.com ainsi que, contrairement aux allégations de la CIPPIC, la mesure de sécurité supplémentaire permettant de fermer effectivement des sessions Facebook ouvertes à partir d'appareils sans fil en modifiant leurs mots de passe sur d'autres plateformes. Les utilisateurs devraient assumer eux-mêmes la responsabilité de protéger leurs renseignements personnels contenus dans leurs comptes Facebook en s'assurant que leurs appareils sans fil sont protégés à l'aide d'un mot de passe, en ne communiquant pas leurs mots de passe de Facebook et en ne laissant pas d'autres personnes utiliser leurs appareils sans fil. (Je tiens à noter que dans sa nouvelle Déclaration des droits et responsabilités, Facebook interdit de communiquer son mot de passe et de donner accès à son compte à autrui.)

351. En résumé, je constate que Facebook ne contrevient pas aux principes 4.7, 4.7.1 et 4.7.3 dans les circonstances.

Conclusions

352. Conséquemment, je conclus que l'allégation n'est pas fondée.

353. Néanmoins, en ce qui concerne les principes 4.1.4 et 4.8, je recommande fortement à titre de pratique exemplaire que Facebook élabore davantage au sujet de son utilisation des témoins dans sa Politique de confidentialité, afin d'expliquer clairement l'utilisation de tous les témoins sur le site et l'incidence de cette utilisation sur les sessions, y compris les sessions ouvertes sur Facebook Mobile.

Section 10

Suivi des activités irrégulières

Allégation

354. La CIPPIC a allégué que Facebook n'informait pas les utilisateurs que cette dernière surveillait le site pour détecter des comportements irréguliers et omettait notamment de mentionner cette pratique dans sa Politique de confidentialité, en dérogation au principe 4.8.

Résumé de l'enquête

355. Comme preuve de cette surveillance, la CIPPIC a cité une entrevue avec un cadre de Facebook qui reconnaissait que le site avait recours à la technologie pour chercher activement tout comportement irrégulier.

356. Dans son argument voulant que les utilisateurs savent que leurs activités sont surveillées, Facebook a indiqué que les Mini-actualités et les Actualités se fondent sur la surveillance des activités des utilisateurs (les Mini-actualités ne sont plus une fonctionnalité de Facebook).

357. En outre, dans ses observations au Commissariat, Facebook a reconnu ainsi qu'elle surveillait les activités :

> « *Nous utilisons certains algorithmes pour protéger les utilisateurs de Facebook en surveillant les comportements irréguliers et [...] nous sommes plutôt ouverts quant à leur fonctionnement, en particulier avec ceux qui sont directement affectés. Si un utilisateur franchit les fils-pièges établis par les algorithmes, il est avisé en temps réel qu'il vient de dépasser les limites permises. Par exemple, l'envoi d'un trop grand nombre de demandes d'ajout d'ami (en particulier si ces demandes ont été rapportées comme étant importunes par d'autres utilisateurs) entraînera la suspension de la possibilité d'envoyer des demandes d'ajout d'ami pour cet utilisateur. Nous utilisons cette infrastructure en grande partie pour éviter que le site serve à des polluposteurs et à des fraudeurs, et pour protéger les utilisateurs en montrant rapidement à ceux qui tentent d'abuser de jeunes utilisateurs que leur conduite entraînera des conséquences* » [traduction].

358. Au moment du dépôt de la plainte, les Conditions d'utilisation de Facebook comportaient une section intitulée « Code de bonne conduite des utilisateurs »

[traduction], qui dressait une liste de 15 types d'activités interdites sur le site, notamment recueillir les adresses de courriel ou les coordonnées d'autres utilisateurs par des moyens électroniques ou autres dans le but d'envoyer des messages non sollicités. Plus loin, sous « Contenu utilisateur publié sur le Site » [traduction], les Conditions d'utilisation prévoyaient :

« Vous reconnaissez et acceptez que la Société peut, sans y être tenue, modifier le Site, ou supprimer ou retirer (sans préavis) tout Contenu du site ou tout Contenu utilisateur, à son entière discrétion, avec ou sans motif quelconque, y compris tout Contenu utilisateur que la Société estime enfreindre les conditions du présent Contrat ou le Code de bonne conduite Facebook, ainsi que tout Contenu utilisateur pouvant présenter un caractère offensant ou illégal ou susceptible d'enfreindre les droits des utilisateurs ou de tiers, ou encore de menacer la sécurité des utilisateurs ou de tiers ou de leur porter atteinte » [traduction].

359. La nouvelle Déclaration des droits et responsabilités (DDR), qui remplace les Conditions d'utilisation, énumère plusieurs types d'activités interdites et signale ce qui suit dans une section intitulée « Résiliation » :

« Si vous contrevenez à la lettre ou à l'esprit de la présente déclaration, ou que vous nous exposez de toute autre manière à des actions en justice, nous pouvons cesser de vous permettre d'utiliser Facebook, en tout ou en partie. En général, nous tenterons de vous en aviser, mais nous ne sommes pas tenus de le faire » [traduction].

Toutefois, la nouvelle DDR ne mentionne pas explicitement si Facebook mène des examens ou une surveillance pour déceler les activités irrégulières.

360. Le premier paragraphe de la section sur la sécurité sur Facebook se lit comme suit :

« Nous améliorons constamment nos systèmes pour reconnaître et éliminer les contenus et les personnes inappropriés » [traduction].

361. Facebook fait également remarquer que son suivi des activités irrégulières a été décrit publiquement dans son entente de mai 2008 avec les secrétaires d'État américains à la Justice, qui visait à accroître la sécurité dans Facebook pour les mineurs. Facebook a notamment convenu de « continuer à utiliser des outils technologiques pour détecter toute conduite inappropriée auprès d'un mineur » et de « prendre des mesures appropriées pour limiter ou interdire l'accès au site à des utilisateurs en fonction de leurs activités inappropriées » [traduction].

Application

362. Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.4, 4.2.1, 4.3.2 et 4.8.

363. Le principe 4.1.4 stipule notamment que les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris, notamment, la rédaction des documents explicatifs concernant leurs politiques et procédures.

364. Le principe 4.2.1 prévoit qu'une organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe 4.8 (transparence) et au principe 4.9 (accès aux renseignements personnels).

365. Le principe 4.3.2 mentionne entre autres que les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés.

366. Le principe 4.8 précise qu'une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

Constatations

367. Facebook reconnaît ouvertement qu'elle effectue la surveillance du site pour détecter toute activité irrégulière. Toutefois, alors que les anciennes Conditions d'utilisation présentaient les types d'activités interdites et informaient les utilisateurs qu'on surveillait le site pour détecter la manifestation de ces activités, la nouvelle DDR ne mentionne pas la pratique de surveillance. La Politique de confidentialité non plus. En fait, à l'heure actuelle, seule la section Sécurité du site contient une phrase à cet effet, mais n'indique pas de manière explicite que Facebook surveille les activités des utilisateurs.

368. Si cette pratique ne m'apparaît ni déraisonnable ni inappropriée en soi, en considération des principes mentionnés ci-dessus, je suis préoccupée à l'idée que Facebook ne fait pas des efforts raisonnables pour documenter cette pratique et en informer les utilisateurs. Je réaffirme mon point de vue : lorsqu'une organisation affiche une politique de confidentialité officielle à titre de référence, le document lui-même doit être compréhensible dans une mesure

raisonnable. En d'autres mots, il doit viser à expliquer toutes les pratiques relatives à la protection de la vie privée de l'organisation, même si elles sont expliquées en tout ou en partie ailleurs.

369. En somme, en ce qui concerne la notification des utilisateurs relativement à la surveillance du site pour détecter les activités irrégulières, je constate que Facebook contrevient aux principes 4.1.4, 4.2.1, 4.3.2, et 4.8.

Recommandations et réponse

370. Dans mon rapport préliminaire, je recommandais à Facebook de décrire dans sa Politique de confidentialité sa pratique de surveillance du site pour déceler des activités irrégulières.

371. En réponse, Facebook a proposé d'inclure le libellé suivant à sa Politique de confidentialité :

« Afin d'améliorer la sécurité du site, Facebook a recours à plusieurs systèmes de technologie visant à détecter et à régler toute activité irrégulière entreprise par un utilisateur. Il pourrait en résulter, à l'occasion, un arrêt temporaire ou permanent de certaines fonctions du service Facebook pour certains utilisateurs » [traduction].

372. Facebook a indiqué que tout changement au libellé de sa Politique de confidentialité serait soumis aux utilisateurs pour une « période de préavis et de réception des commentaires ». Toutefois, indépendamment de l'assentiment des utilisateurs, le Commissariat s'attend à ce que Facebook respecte son engagement à satisfaire à ces recommandations.

Conclusions

373. Je suis confiante qu'une fois mises en œuvre, les mesures correctives que propose Facebook, telles que présentées ci-dessus, sauront satisfaire à nos recommandations et permettront à l'organisation de se conformer à la *Loi*. Aussi, je conclus que les allégations à cet effet sont fondées et résolues.

374. Nous effectuerons un suivi de Facebook et de la mise en œuvre de ces mesures dans les 30 jours.

Section 11

Tromperie et fausse représentation

Allégations

375. La CIPPIC a allégué que Facebook :

1) se représentait faussement en affirmant qu'elle est purement un site de réseautage social alors qu'elle participait à d'autres activités qui n'étaient pas clairement expliquées, telles que la publicité et les applications de tiers, en dérogation aux principes 4.3.2 et 4.4.2;

2) présentait de façon inexacte le niveau de contrôle que les utilisateurs avaient sur leurs renseignements personnels, en dérogation aux principes 4.3.2 et 4.4.2.

Résumé de l'enquête

376. Nous n'avons trouvé aucune preuve que Facebook trompait ou induisait en erreur volontairement les utilisateurs quant aux fins pour lesquelles elle recueillait des renseignements, ou qu'elle obtenait leur consentement de façon trompeuse.

Constatations

377. Je considère comme sérieuses les allégations de tromperie; elles exigent à tout le moins quelques preuves d'intention de tromper. À défaut de tels éléments de preuve, il m'est impossible d'affirmer que Facebook contrevient à la *Loi*.

Conclusion

378. Par conséquent, je conclus que les allégations de fausse représentation ne sont pas fondées.

Résumé des conclusions

Allégations non fondées

379. En ce qui a trait aux nouveaux usages des renseignements personnels, à la collecte de renseignements personnels de sources externes à Facebook, à Facebook Mobile et aux mesures de sécurité, et à la tromperie et la fausse représentation, je conclus que les allégations de la CIPPIC ne sont pas fondées.

Allégations fondées et résolues

380. En ce qui a trait à la collecte de la date de naissance, aux paramètres de confidentialité par défaut, à la publicité et au suivi des activités irrégulières, je conclus que les allégations de la CIPPIC sont fondées et résolues à la lumière des mesures correctives que Facebook propose en réponse à mes recommandations.

381. J'ai avisé Facebook que le Commissariat effectuera un suivi après 30 jours pour vérifier si les mesures proposées ont été mises en œuvre.

Allégations fondées comportant des questions non résolues

382. En ce qui a trait aux applications de tiers, à la désactivation et la suppression du compte, aux comptes des utilisateurs décédés, et aux renseignements personnels des non-utilisateurs, je conclus que les allégations de la CIPPIC sont fondées. Toutefois, en ces cas, des questions demeurent irrésolues dans la mesure où Facebook n'a pas encore accepté d'adopter certaines de mes recommandations, ni des solutions de rechange acceptables.

383. Les recommandations qui demeurent en suspens sont les suivantes :

(Applications de tiers)

- Que Facebook prenne en considération et mette en œuvre des mesures :

1) pour limiter l'accès des développeurs d'applications aux renseignements des utilisateurs qui ne sont pas nécessaires au fonctionnement d'une application particulière;

2) par lesquelles, dans chaque cas, les utilisateurs seraient informés des renseignements qu'une application requiert et des fins y afférentes;

3) par lesquelles, dans chaque cas, on cherche à obtenir le consentement exprès des utilisateurs à ce que les développeurs aient accès à ces renseignements;

4) interdisant toute communication de renseignements personnels des utilisateurs qui n'ajoutent pas eux-mêmes une application.

(Désactivation et suppression du compte)

- Que Facebook élabore et mette en place une politique en matière de conservation des renseignements en vertu de laquelle les renseignements personnels des utilisateurs qui ont désactivé leur compte seraient éliminés des serveurs de Facebook après une période raisonnable, et que Facebook en informe les utilisateurs.

(Comptes des utilisateurs décédés)

- Que Facebook explique dans sa Politique de confidentialité, dans le contexte de tous les usages des renseignements personnels prévus, l'usage des renseignements personnels du compte des utilisateurs décédés prévu à des fins commémoratives.

(Renseignements personnels des non-utilisateurs)

- Que Facebook examine et mette en place des mesures pour améliorer le service d'invitation afin de répondre à la préoccupation du Commissariat quant au fait que les non-utilisateurs ignorent que Facebook recueille, utilise et conserve leur adresse de courriel et qu'ils n'y consentent pas;

- Que Facebook établisse une limite raisonnable de conservation des adresses de courriel de non-utilisateurs aux fins du suivi de l'historique des invitations et du succès du programme d'invitation.

384. J'ai demandé que Facebook reconsidère ces recommandations en suspens à la lumière de mes constatations. J'ai également précisé que dans le cadre du suivi d'autres affaires que le Commissariat effectuera 30 jours après la présentation du rapport, on chercherait également des preuves que les recommandations en suspens, ou des solutions de rechange acceptables, ont été acceptées et mises en œuvre. À défaut de telles preuves, nous déterminerons le meilleur moyen de traiter toute autre question non résolue conformément à nos pouvoirs.

385. Il me tarde de procéder à l'examen des progrès de Facebook relativement à la mise en œuvre de mes recommandations et j'anticipe favorablement la

coopération soutenue de l'organisation à résoudre les questions soulevées dans cette plainte.

ANNEXE A

Allégations	Conclusions
Section 1 – Collecte de la date de naissance 1) Facebook exigerait des utilisateurs qu'ils fournissent leur date de naissance comme condition d'inscription sans raison valable, en dérogation au principe 4.3.3. 2) Facebook n'expliquerait pas correctement aux utilisateurs la raison pour laquelle ils doivent fournir leur date de naissance et la façon dont celle-ci serait utilisée, en dérogation au principe 4.3.2.	Constatations : 1) Il est acceptable d'exiger la date de naissance comme condition de service puisque les fins de son utilisation sont appropriées. 2) Toutefois, Facebook n'expliquait pas clairement ces fins. Recommandation : • On a demandé à Facebook d'indiquer clairement aux utilisateurs, au moment de l'inscription, pourquoi leur date de naissance était requise. • On a également demandé à Facebook de préciser dans la documentation offerte sur le site les raisons pour lesquelles on recueille la date de naissance et la manière dont cette dernière sera utilisée.

Réponse :

- Facebook a accepté toutes les recommandations.

Conclusion : fondée et résolue

Section 2 – Paramètres de confidentialité par défaut

1) Facebook, en présélectionnant les paramètres de confidentialité par défaut, aurait recours au consentement négatif pour utiliser et communiquer des renseignements personnels, et n'en respecterait pas les exigences telles qu'établies par le Commissariat dans le cadre de conclusions précédentes. En particulier, on a invoqué que la majorité des renseignements personnels communiqués par les utilisateurs, y compris les photographies, l'état civil, l'âge et les passe-temps, sont de nature délicate et exigent un consentement explicite.

2) Facebook, dans le contexte des paramètres de confidentialité, ne déploierait pas d'efforts raisonnables pour s'assurer que les utilisateurs sont informés des fins auxquelles les renseignements serviraient et la mesure dans laquelle ils seraient utilisés et communiqués. Précisément :

   - Facebook n'informerait pas les

Constatations :

1) Les utilisateurs téléchargent volontairement leurs renseignements personnels dans le but de les partager avec d'autres.

2) Les paramètres de confidentialité par défaut sont acceptables pour autant qu'ils correspondent aux attentes raisonnables des utilisateurs. Ils n'y correspondent pas dans deux cas : les albums de photos (réglés à « Tout le monde ») et les moteurs de recherche (être accessible via les moteurs de recherche).

3) On n'a pas fourni aux utilisateurs suffisamment d'information quant aux paramètres de confidentialité par défaut et aux conséquences découlant de la non-modification des paramètres par défaut.

utilisateurs de la mesure dans laquelle leurs renseignements personnels pourraient être communiqués conformément aux paramètres par défaut et, par conséquent, n'obtiendrait pas leur consentement valable.

- Facebook ne dirigerait pas les utilisateurs vers les paramètres de confidentialité lorsque ces derniers s'inscrivent ou téléchargent des photographies, ou lorsque Facebook modifie les paramètres.
- Facebook n'aviserait pas les utilisateurs que ne pas modifier les paramètres par défaut signifie l'acceptation de ceux-ci.
- Facebook omettrait d'informer convenablement les utilisateurs qui publient des albums de photos que les paramètres de confidentialité par défaut de ces albums permettent de les communiquer à tout le monde, ce qui signifie qu'un autre utilisateur qui n'est pas un ami peut regarder les photographies et lire les commentaires qui s'y rapportent, même si le profil de l'utilisateur n'est accessible qu'aux amis.
- Lorsque les utilisateurs deviennent membres d'un réseau, leurs paramètres de confidentialité par défaut permettent la communication de renseignements personnels, y compris des renseignements de nature délicate, avec tous les membres du réseau.

Recommandations :

On a demandé à Facebook :

- de rendre les profils des utilisateurs inaccessibles par défaut aux moteurs de recherche;
- de remplacer les paramètres par défaut des albums de photos par « Mes réseaux et mes amis »;
- de fournir un lien vers les paramètres de confidentialité au moment de l'inscription, un énoncé sur l'objet des paramètres, et un avis que Facebook a présélectionné les paramètres et que ces derniers peuvent être modifiés au gré des préférences.

Réponse :

Facebook modifie ses réglages de confidentialité (a) en permettant aux utilisateurs de choisir le niveau des paramètres, soit faible, moyen ou élevé, et (b) en mettant en œuvre un outil de confidentialité par objet qui permettra aux utilisateurs de régler les paramètres individuels de chaque photo et de chaque élément de contenu telles les mises à jour.

Conclusion : fondée et résolue

Section 3 – Publicités de Facebook

1) Facebook ne ferait pas d'efforts raisonnables pour s'assurer que les utilisateurs soient informés que leurs renseignements personnels serviraient à des fins publicitaires, en dérogation au principe 4.3.2.

2) Facebook, en ce qui concerne les publicités sociales en particulier, aurait recours de façon inappropriée au consentement implicite plutôt qu'au consentement explicite conforme au principe 4.3.6, étant donné la nature délicate des renseignements personnels des utilisateurs.

3) Facebook ne permettrait pas aux utilisateurs de retirer leur consentement aux publicités Facebook, en dérogation au principe 4.3.8.

4) Puisque les utilisateurs ne sont pas autorisés à retirer leur consentement aux publicités Facebook, cette dernière demanderait sans raison valable de consentir à ces publicités pour obtenir le service, en dérogation au principe 4.3.3.

Constatations :

1) Les utilisateurs ne peuvent pas retirer leur consentement à toute forme de publicité puisque les revenus publicitaires sont nécessaires au maintien du site (qui est gratuit pour les utilisateurs).

2) Les utilisateurs peuvent retirer leur consentement aux publicités sociales — cette forme de publicité est plus envahissante (on se sert des personnes pour faire la promotion de produits, services, etc.) et, par conséquent, les utilisateurs ne devraient pas être obligés de consentir aux publicités sociales.

3) Exiger des utilisateurs qu'ils consentent aux publicités Facebook est acceptable, puisqu'on ne tient pas pour acquis qu'ils endossent un produit.

4) Toutefois, Facebook n'informe pas les utilisateurs des fins de la publicité.

Recommandations :

- On a demandé à Facebook d'étoffer la section de la Politique de confidentialité portant sur la

publicité afin de mieux expliquer le rôle des publicités et informer les utilisateurs que leur information de profil sert à la publicité ciblée.

Réponse :

Facebook a accepté de décrire la publicité de manière plus claire et de configurer ses systèmes afin de permettre aux utilisateurs de trouver plus facilement l'information au sujet de la publicité.

Conclusion : fondée et résolue

Section 4 – Applications de tiers

1) Facebook n'informerait pas les utilisateurs des raisons pour lesquelles elle communique leurs renseignements personnels aux tiers développeurs d'applications, en dérogation aux principes 4.2.2 et 4.2.5.

2) Facebook permettrait aux tiers développeurs d'applications d'accéder à des renseignements personnels au-delà de ce qui est nécessaire pour les besoins de l'application, en dérogation au principe 4.4.1.

3) Facebook exigerait que les utilisateurs acceptent de communiquer des

Constatations :

1) Facebook disposait de mesures inadéquates qui ne permettaient pas de restreindre de manière effective l'accès de ces développeurs externes à l'information de profil des utilisateurs et à l'information des amis en ligne de ces utilisateurs.

2) Facebook n'obtenait pas le consentement valable des utilisateurs à la communication de leurs renseignements personnels aux développeurs d'applications quand les utilisateurs eux-mêmes ou leurs amis ajoutaient des applications.

renseignements personnels au-delà de ce qui est nécessaire pour le fonctionnement de l'application, en dérogation au principe 4.3.3.

4) Facebook n'aviserait pas les utilisateurs des conséquences liées au retrait de leur consentement à communiquer des renseignements personnels aux tiers développeurs d'applications, en dérogation au principe 4.3.8.

5) Facebook permettrait aux tiers développeurs d'applications de conserver les renseignements personnels de l'utilisateur après la suppression de l'application par l'utilisateur, en dérogation au principe 4.5.3.

6) Facebook permettrait aux tiers développeurs d'accéder aux renseignements personnels d'utilisateurs dont les amis ou les membres de leurs réseaux ajoutent une application sans les en aviser adéquatement, en dérogation au principe 4.3.2.

7) Facebook ne protégerait pas adéquatement les renseignements personnels, car elle ne surveillerait ni la qualité ni la légitimité des applications de tiers ni ne prendrait les mesures indiquées contre les vulnérabilités inhérentes de nombreuses applications sur la Plateforme

Recommandations :

- On a demandé à Facebook de mettre en œuvre des mesures technologiques pour limiter l'accès des développeurs d'applications aux renseignements des utilisateurs qui ne sont pas nécessaires au fonctionnement de l'application.
- Le site devrait également faire en sorte que les utilisateurs sont informés des renseignements spécifiques qu'une application requiert et des fins y afférentes. En outre, le consentement exprès des utilisateurs à ce que les développeurs aient accès à ces renseignements spécifiques devrait être obtenu chaque fois qu'une personne s'inscrit à une application.
- Finalement, des mesures sont nécessaires afin d'interdire toute communication de renseignements personnels des utilisateurs qui n'ajoutent pas eux-mêmes une application.

Réponse :

Facebook n'a pas accepté de mettre en œuvre les recommandations.

Conclusion : fondée

Facebook, en dérogation au principe 4.7.

8) Facebook n’aviserait pas efficacement les utilisateurs de la portée des renseignements personnels communiqués aux tiers développeurs d’applications et fournirait aux utilisateurs de l’information trompeuse ou imprécise sur le partage avec les tiers développeurs d’applications, en dérogation aux principes 4.3 et 4.8.

9) Facebook n’assumerait aucune responsabilité quant aux renseignements personnels transmis aux tiers développeurs aux fins de traitement, en dérogation au principe 4.1.3.

10) Facebook ne permettrait pas aux utilisateurs de refuser de communiquer leurs nom, réseaux et listes d’amis lorsque leurs amis ajoutaient une application, en dérogation au principe 4.3 et au paragraphe 5(3).

Section 5 – Nouveaux usages des renseignements personnels

1) Facebook n’aviserait pas les utilisateurs des nouvelles fins auxquelles leurs renseignements seraient recueillis, utilisés ou communiqués, en dérogation au principe 4.2.4.

Constatations :

Il n’y a aucune preuve à l’effet que Facebook aurait manqué d’informer ses utilisateurs de nouvelles fins.

	Conclusion : non fondée
Section 6 – Collecte de renseignements personnels de sources externes à Facebook	
1) Facebook ne fournirait pas aux utilisateurs de renseignements précis sur les fins et les modes de collecte de renseignements personnels de sources externes à Facebook, sur les sources d'information, et sur l'usage et la communication des renseignements. 2) N'ayant pas fourni cette information, Facebook n'obtiendrait pas le consentement valable des utilisateurs.	Constatations : Bien que la politique de confidentialité de Facebook comprenne un libellé concernant la collecte de renseignements de sources externes, dans les faits, Facebook ne recueille pas de tels renseignements à l'heure actuelle. Conclusion : non fondée
Section 7a) – Désactivation et suppression du compte	
1) Facebook n'offrirait que l'option de désactivation du compte, ce qui est différent de la suppression du compte. Ce faisant, elle priverait indûment les utilisateurs d'une façon de supprimer tous leurs renseignements personnels du site.	Constatations : 1) La désactivation et la suppression du compte sont décrites sur le site, mais pas au même endroit. Cela pourrait porter certains utilisateurs à croire que la désactivation est la seule option qui leur est disponible. 2) Les renseignements personnels faisant partie de comptes désactivés sont conservés

	indéfiniment. Recommandations : • On a demandé à Facebook d'élaborer et de mettre en place une politique en matière de conservation de l'information en vertu de laquelle les renseignements personnels des utilisateurs qui ont désactivé leur compte seraient supprimés des serveurs de Facebook après une période raisonnable, et d'en informer les utilisateurs. • La commissaire adjointe a également suggéré à titre de pratique exemplaire que l'option de suppression du compte soit plus apparente pour les utilisateurs. Réponse : Facebook a accepté d'ajouter de l'information au sujet de la suppression du compte dans sa politique de confidentialité, mais a refusé d'élaborer une politique de conservation au sujet des comptes désactivés. Conclusion : fondée
Section 7b) – Comptes des utilisateurs décédés	
1) En ne mentionnant son intention de conserver le profil des utilisateurs	Constatations :

décédés à des fins commémoratives que dans ses Conditions d'utilisation et non dans sa Politique de confidentialité, Facebook n'obtiendrait pas le consentement valable des utilisateurs pour cette utilisation de leurs renseignements personnels.

2) Facebook obligerait les utilisateurs, en dérogation au principe 4.3.3, à consentir à cette fin comme condition de service, même si la commémoration d'un profil n'est pas nécessaire à l'objectif principal de Facebook, soit le réseautage social.

1) On pourrait considérer que la commémoration est une utilisation primaire, puisque la plupart des utilisateurs auraient des attentes raisonnables à cet égard.

2) Toutefois, les utilisateurs ne sont pas avisés de cette pratique et par conséquent ne peuvent pas effectivement y consentir.

Recommandation :

- On a demandé à Facebook d'expliquer dans sa politique de confidentialité la pratique d'utiliser à des fins commémoratives des renseignements personnels des comptes d'utilisateurs décédés.

Réponse :

Facebook a refusé de mettre en œuvre la recommandation parce qu'elle considérait qu'elle n'était pas nécessaire aux termes de la loi.

Conclusion : fondée

Section 8 – Renseignements personnels des non-utilisateurs

1) Facebook n'obtiendrait pas le consentement des non-utilisateurs au téléchargement de leurs renseignements personnels vers le site, en dérogation au principe 4.3,

Constatations :

1) Lorsque les utilisateurs affichent des renseignements personnels au sujet de non-utilisateurs sur

dans les situations suivantes :

- Des utilisateurs peuvent publier des renseignements personnels de non-utilisateurs dans leur profil et celui d'autres utilisateurs par des fonctionnalités comme les « Actualités » et le « Mur ». En outre, les utilisateurs peuvent étiqueter des non-utilisateurs sur des photos ou dans des vidéos.
- Les utilisateurs peuvent fournir l'adresse de courriel de non-utilisateurs pour les inviter à s'inscrire au site.

les murs, dans les profils ou dans les Actualités, ces affichages sont faits à des fins purement personnelles et ne sont pas assujettis à la *Loi*.

2) Pour ce qui est de l'étiquetage et des invitations envoyées aux non-utilisateurs, la *Loi* s'applique seulement là où Facebook se sert des renseignements de non-utilisateurs à ses propres fins, nommément, informer les non-utilisateurs qu'ils ont été étiquetés sur une photo ou les inviter à se joindre à Facebook.

3) Facebook peut laisser aux utilisateurs le soin d'obtenir le consentement de non-utilisateurs à ces deux fins, pourvu que l'entreprise fasse preuve de diligence raisonnable. Cela pourrait se faire simplement en adoptant des mesures pour s'assurer que les utilisateurs savent qu'ils doivent obtenir le consentement de non-utilisateurs avant de communiquer l'adresse de courriel de ces derniers à Facebook et punir les utilisateurs qui ne respectent pas l'exigence d'obtenir le consentement.

4) Toutefois, on ne retrouve aucune information à ce sujet dans la Politique de confidentialité.

Recommandations :

- On a demandé à Facebook de mettre en place des mesures pour améliorer le service d'invitation afin d'aborder nos préoccupations quant au fait que les non-utilisateurs ignorent que Facebook recueille, utilise et conserve leur adresse de courriel, et qu'ils n'y consentent pas.
- On a demandé à Facebook d'établir une limite raisonnable de conservation des adresses de courriel de non-utilisateurs une fois que ces derniers ont été invités à se joindre à Facebook.

Réponse :

Facebook a refusé de mettre en œuvre les première et deuxième recommandations ci-dessus en invoquant que le site « continue d'informer les non-utilisateurs, dans une mesure toujours plus grande, que notre site Web renferme des renseignements sur eux — nous le faisons dans une plus grande mesure que n'importe quel autre site Web. »

Facebook a également souligné qu'elle ne pourrait pas de manière réaliste supprimer les renseignements personnels de non-utilisateurs téléchargés par des utilisateurs, puisque ces renseignements appartiennent aux utilisateurs et sont sous le contrôle de ces derniers. Par conséquent, l'utilisateur qui télécharge les renseignements d'un non-utilisateur est

responsable de ces renseignements.

Facebook n’a fourni aucune réponse directe à la troisième recommandation.

Conclusion : fondée

Section 9 – Facebook Mobile et mesures de sécurité

1) En ce qui concerne les utilisateurs de la version mobile du site Facebook (Facebook Mobile), la CIPPIC a allégué que, en fournissant aux utilisateurs un témoin persistant sans date de péremption apparente, Facebook ne protégeait pas adéquatement les renseignements personnels des utilisateurs, en dérogation aux principes 4.7, 4.7.1 et 4.7.3.

2) Plus précisément, la CIPPIC a émis les préoccupations suivantes au sujet

Constatations :

1) Facebook utilise un témoin persistant de 14 jours. Un changement de mot de passe sur une autre plateforme ferme une session ouverte sur Facebook Mobile; l’utilisateur devra s’identifier de nouveau afin d’ouvrir une nouvelle session.

2) Par conséquent, Facebook offre aux utilisateurs un moyen simple de fermer des sessions sur Facebook Mobile ainsi que la possibilité de

de la sécurité :

(1) Si un utilisateur se sert de l'appareil sans fil d'un autre personne pour ouvrir une session sur Facebook puis oublie de fermer la session, l'autre personne aura accès indéfiniment au compte Facebook de l'utilisateur, même si ce dernier change son mot de passe.

(2) Si un utilisateur donne son mot de passe de compte Facebook à une autre personne, cette dernière peut ouvrir une session sur un appareil sans fil et obtenir accès indéfiniment, même si l'utilisateur change son mot de passe.

3) Selon la CIPPIC, le témoin de connexion laissé par Facebook devrait être périmé après une période raisonnable et chaque fois qu'un utilisateur modifie son mot de passe en ligne.

fermer effectivement des sessions ouvertes sur des appareils sans fil, en modifiant leur mot de passe sur d'autres plateformes.

3) Par conséquent, Facebook offre aux utilisateurs de Facebook Mobile des mesures de protection adéquates contre l'accès non autorisé à leurs sessions.

Conclusion : non fondée

Section 10 – Suivi des activités irrégulières

1) Facebook n'informerait pas les utilisateurs qu'elle surveille le site pour détecter des comportements irréguliers et omettrait notamment de mentionner cette pratique dans sa Politique de confidentialité, en

Constatations :

1) La pratique de surveillance du site pour détecter des comportements irréguliers est

dérogation au principe 4.8.	appropriée, mais Facebook ne déploie pas d'efforts raisonnables pour en informer les utilisateurs. Recommandation : • On a demandé à Facebook d'expliquer cette pratique dans sa Politique de confidentialité. Réponse : Facebook a accepté la recommandation. Conclusion : fondée et résolue
Section 11 – Tromperie et fausse représentation	
1) Facebook se représenterait faussement en affirmant qu'elle est purement un site de réseautage social alors qu'elle participerait à d'autres activités qui n'étaient pas clairement expliquées, telles que la publicité et les applications de tiers, en dérogation aux principes 4.3.2 et 4.4.2.	Constatations : Il n'y a aucune preuve que Facebook tromperait ou induirait en erreur volontairement. Conclusion : non fondée
2) Facebook présenterait de façon inexacte le niveau de contrôle que les utilisateurs avaient sur leurs renseignements personnels, en dérogation aux principes 4.3.2 et 4.4.2.	

ANNEXE B

Loi sur la protection des renseignements personnels et les documents électroniques

Section 1

5. (1) Sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1.

(2) L'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit d'une recommandation et non d'une obligation.

(3) L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.
Le paragraphe 5(3) établit qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Annexe 1 - Principes Énoncés dans la Norme Nationale du Canada intitulée *Code Type sur la Protection des Renseignements Personnels,* CAN/CSA-Q830-96

4.1 Premier principe — Responsabilité
Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

4.1.1
Il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidiens des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées.

4.1.2
Il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

4.1.3
Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.1.4
Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris :
a) la mise en œuvre des procédures pour protéger les renseignements personnels;
b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;
c) la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation; et
d) la rédaction des documents explicatifs concernant leurs politiques et procédures.

4.2 Deuxième principe — Détermination des fins de la collecte des renseignements
Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

4.2.1
L'organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe de la transparence (article 4.8) et au principe de l'accès aux renseignements personnels (article 4.9).

4.2.2
Le fait de préciser les fins de la collecte de renseignements personnels avant celle-ci ou au moment de celle-ci permet à l'organisation de déterminer les renseignements dont elle a besoin pour réaliser les fins mentionnées. Suivant le principe de la limitation en matière de collecte (article 4.4), l'organisation ne doit recueillir que les renseignements nécessaires aux fins mentionnées.

4.2.3
Il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils

sont destinés. Selon la façon dont se fait la collecte, cette précision peut être communiquée de vive voix ou par écrit. Par exemple, on peut indiquer ces fins sur un formulaire de demande de renseignements.

4.2.4
Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées avant l'utilisation. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements à cette nouvelle fin. Pour obtenir plus de précisions sur le consentement, se reporter au principe du consentement (article 4.3).

4.2.5
Les personnes qui recueillent des renseignements personnels devraient être en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements.

4.2.6
Ce principe est étroitement lié au principe de la limitation de la collecte (article 4.4) et à celui de la limitation de l'utilisation, de la communication et de la conservation (article 4.5).

4.3 Troisième principe — Consentement
Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
Note : Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d'obtenir le consentement de la personne concernée. Lorsqu'on recueille des renseignements aux fins du contrôle d'application de la loi, de la détection d'une fraude ou de sa prévention, on peut aller à l'encontre du but visé si l'on cherche à obtenir le consentement de la personne concernée. Il peut être impossible ou inopportun de chercher à obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale. De plus, les organisations qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui

fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels.

4.3.1
Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, une organisation peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand elle veut les utiliser à des fins non précisées antérieurement.

4.3.2
Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

4.3.3
Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

4.3.4
La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

4.3.5
Dans l'obtention du consentement, les attentes raisonnables de la personne sont

aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge.

4.3.6
La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).

4.3.7
Le consentement peut revêtir différentes formes, par exemple :
a) on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;
b) on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organisations. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;
c) le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou
d) le consentement peut être donné au moment où le produit ou le service est utilisé.

4.3.8
Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait.

4.4 Quatrième principe — Limitation de la collecte
L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

4.4.1
Les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Conformément au principe de la transparence (article 4.8), les organisations doivent préciser la nature des renseignements recueillis comme partie intégrante de leurs politiques et pratiques concernant le traitement des renseignements.

4.4.2
L'exigence selon laquelle les organisations sont tenues de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. Cette obligation suppose que le consentement à la collecte de renseignements ne doit pas être obtenu par un subterfuge.

4.4.3
Ce principe est étroitement lié au principe de détermination des fins auxquelles la collecte est destinée (article 4.2) et à celui du consentement (article 4.3).

4.5 Cinquième principe — Limitation de l'utilisation, de la communication et de la conservation
Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

4.5.1
Les organisations qui se servent de renseignements personnels à des fins nouvelles doivent documenter ces fins (voir article 4.2.1).

4.5.2
Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation. On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne

concernée d’exercer son droit d’accès à l’information après que la décision a été prise. Une organisation peut être assujettie à des exigences prévues par la loi en ce qui concerne les périodes de conservation.

4.5.3
On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n’a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

4.5.4
Ce principe est étroitement lié au principe du consentement (article 4.3), à celui de la détermination des fins auxquelles la collecte est destinée (article 4.2), ainsi qu’à celui de l’accès individuel (article 4.9).

4.6 Sixième principe — Exactitude
Les renseignements personnels doivent être aussi exacts, complets et à jour que l’exigent les fins auxquelles ils sont destinés.

4.6.1
Le degré d’exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l’usage auquel ils sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision à son sujet.

4.6.2
Une organisation ne doit pas systématiquement mettre à jour les renseignements personnels à moins que cela ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis.

4.6.3
Les renseignements personnels qui servent en permanence, y compris les renseignements qui sont communiqués à des tiers, devraient normalement être exacts et à jour à moins que des limites se rapportant à l’exactitude de ces renseignements ne soient clairement établies.

4.7 Septième principe — Mesures de sécurité
Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1
Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

4.7.2
La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

4.7.3
Les méthodes de protection devraient comprendre :
a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et
c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

4.7.4
Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

4.7.5
Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3).

4.8 Huitième principe — Transparence
Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

4.8.1
Les organisations doivent faire preuve de transparence au sujet de leurs politiques et pratiques concernant la gestion des renseignements personnels. Une personne doit pouvoir obtenir sans efforts déraisonnables de l'information au sujet des politiques et des pratiques d'une organisation. Ces renseignements doivent être fournis sous une forme généralement compréhensible.

4.8.2
Les renseignements fournis doivent comprendre :
a) le nom ou la fonction de même que l'adresse de la personne responsable de la politique et des pratiques de l'organisation et à qui il faut acheminer les plaintes et les demandes de renseignements;
b) la description du moyen d'accès aux renseignements personnels que possède l'organisation;
c) la description du genre de renseignements personnels que possède l'organisation, y compris une explication générale de l'usage auquel ils sont destinés;
d) une copie de toute brochure ou autre document d'information expliquant la politique, les normes ou les codes de l'organisation; et
e) la définition de la nature des renseignements personnels communiqués aux organisations connexes (par exemple, les filiales).

4.8.3
Une organisation peut rendre l'information concernant sa politique et ses pratiques accessibles de diverses façons. La méthode choisie est fonction de la nature des activités de l'organisation et d'autres considérations. Par exemple, une organisation peut offrir des brochures à son établissement, poster des renseignements à ses clients, offrir un accès en ligne ou établir un numéro de téléphone sans frais.

4.9 Neuvième principe — Accès aux renseignements personnels
Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.
Note : Dans certains cas, il peut être impossible à une organisation de communiquer tous les renseignements personnels qu'elle possède au sujet d'une personne. Les exceptions aux exigences en matière d'accès aux renseignements personnels devraient être restreintes et précises. On devrait informer la personne, sur demande, des raisons pour lesquelles on lui refuse l'accès aux renseignements. Ces raisons peuvent comprendre le coût exorbitant de la fourniture de l'information, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons d'ordre commercial exclusives et le fait que les renseignements sont protégés par le secret professionnel ou dans le cours d'une procédure de nature judiciaire.

4.9.1
Une organisation doit informer la personne qui en fait la demande du fait qu'elle

possède des renseignements personnels à son sujet, le cas échéant. Les organisations sont invitées à indiquer la source des renseignements. L'organisation doit permettre à la personne concernée de consulter ces renseignements. Dans le cas de renseignements médicaux sensibles, l'organisation peut préférer que ces renseignements soient communiqués par un médecin. En outre, l'organisation doit informer la personne concernée de l'usage qu'elle fait ou a fait des renseignements et des tiers à qui ils ont été communiqués.

4.9.2
Une organisation peut exiger que la personne concernée lui fournisse suffisamment de renseignements pour qu'il lui soit possible de la renseigner sur l'existence, l'utilisation et la communication de renseignements personnels. L'information ainsi fournie doit servir à cette seule fin.

4.9.3
L'organisation qui fournit le relevé des tiers à qui elle a communiqué des renseignements personnels au sujet d'une personne devrait être la plus précise possible. S'il lui est impossible de fournir une liste des organisations à qui elle a effectivement communiqué des renseignements au sujet d'une personne, l'organisation doit fournir une liste des organisations à qui elle pourrait avoir communiqué de tels renseignements.

4.9.4
Une organisation qui reçoit une demande de communication de renseignements doit répondre dans un délai raisonnable et ne peut exiger, pour ce faire, que des droits minimes. Les renseignements demandés doivent être fournis sous une forme généralement compréhensible. Par exemple, l'organisation qui se sert d'abréviations ou de codes pour l'enregistrement des renseignements doit fournir les explications nécessaires.

4.9.5
Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisation doit apporter les modifications nécessaires à ces renseignements. Selon la nature des renseignements qui font l'objet de la contestation, l'organisation doit corriger, supprimer ou ajouter des renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

4.9.6
Lorsqu'une contestation n'est pas réglée à la satisfaction de la personne concernée, l'organisation prend note de l'objet de la contestation. S'il y a lieu, les tierces parties

ayant accès à l'information en question doivent être informées du fait que la contestation n'a pas été réglée.

4.10 Dixième principe — Possibilité de porter plainte à l'égard du non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les personnes responsables de les faire respecter au sein de l'organisation concernée.

4.10.1

La question de la désignation de la personne responsable du respect des principes dans l'organisation fait l'objet de l'article 4.1.1.

4.10.2

Les organisations doivent établir des procédures pour recevoir les plaintes et les demandes de renseignements concernant leurs politiques et pratiques de gestion des renseignements personnels et y donner suite. Les procédures relatives aux plaintes devraient être facilement accessibles et simples à utiliser.

4.10.3

Les organisations doivent informer les personnes qui présentent une demande de renseignements ou déposent une plainte de l'existence des procédures pertinentes. Il peut exister un éventail de ces procédures. Par exemple, certaines autorités réglementaires acceptent les plaintes concernant les pratiques de gestion des renseignements personnels des entreprises relevant de leur compétence.

4.10.4

Une organisation doit faire enquête sur toutes les plaintes. Si une plainte est jugée fondée, l'organisation doit prendre les mesures appropriées, y compris la modification de ses politiques et de ses pratiques au besoin.