La vie privée sur les sites de réseau social

Analyse comparative de six sites

Préparée pour le Commissariat à la protection de la vie privée du Canada
www.priv.gc.ca | Février 2009
Recherche effectuée par : Jennifer Barrigar

Ce rapport a été préparé pour le Commissariat à la protection de la vie privée par Jennifer Barrigar, consultante et chercheure d'expérience tant en matière de lois sur la protection de la vie privée que de technologie Internet. Il a été commandé à la fin de 2008 et le rapport final a été présenté au Commissariat en février 2009.

Les réseaux sociaux apportent souvent des modifications ou des ajouts à leurs politiques de confidentialité et à leurs mesures de protection. Par conséquent, certaines observations faites dans ce rapport pourraient sembler désuètes, voire erronées. C'est le cas notamment de Facebook, un site de réseautage social qui a connu plusieurs rondes de modifications en matière de confidentialité au cours de l'année 2009.

Or, ce n'est pas de cas de plusieurs autres sites de réseautage social cités par Mme Barrigar. Ces sites sont parmi les plus populaires auprès des Canadiennes et Canadiens, mais sont largement développés et gérés à l'extérieur du Canada. Conséquemment, ils offrent des niveaux de protection de la vie privée largement différents à leurs utilisateurs. Ce rapport indique les secteurs dans lesquels ces sites devraient améliorer leurs politiques et prendre des mesures pour protéger efficacement les renseignements personnels de leurs utilisateurs.

Colin McKay
Directeur, Recherche, sensibilisation et engagement

Commissariat à la protection de la vie privée du Canada
Sans frais : 1-800-282-1376 | Téléphone : 613-995-8210 | Télécopieur : 613-947-6850 | ATS : 613-992-9190
112, rue Kent | Place de Ville | Tour B, 3e étage | Ottawa (Ontario) | K1A 1H3
Numéro de catalogue : IP54-28/2009 | ISBN 978-1-100-50025-6

TABLE DES MATIÈRES

SOMMAIRE

Ce document propose une analyse comparative du traitement des renseignements personnels sur les sites de réseau social (SRS) au Canada. Il présente six (6) SRS populaires au pays en ce moment. Chacun de ces sites est examiné par rapport à son mandat tel qu'énoncé, à ses rouages financiers (selon l'information disponible), à son historique et au profil démographique de ses utilisateurs.

Il va sans dire que la protection de la vie privée est un concept très vaste. Afin de circonscrire l'objet de l'analyse, dix (10) catégories d'activités communes aux SRS ont été déterminées. Pour chaque catégorie, le document décrit en détail la politique adoptée par les sites. Évidemment, cette démarche ne permet pas d'aborder la totalité des questions liées à la protection de la vie privée pour chacun des sites; elle pose néanmoins les bases pour comprendre de manière générale ces questions et les principes établis par les propriétaires des sites à ce sujet.

Par ailleurs, le document fournit quelques pistes de solution pour tenter de réconcilier l'apparente disparité entre le désir de protection de la vie privée exprimé par les utilisateurs et le faible taux d'utilisation des outils prévus à cet effet. En s'appuyant sur la théorie selon laquelle l'intégrité de la vie privée est contextuelle, l'analyse vise à trouver des manières d'approfondir la compréhension qu'a l'utilisateur du contexte dans lequel il interagit sur un SRS. Parallèlement, elle cherche à sensibiliser l'utilisateur aux mesures et aux outils de protection de la vie privée tout en améliorant l'efficacité de ces mesures et outils pour éclairer l'utilisateur dans ses choix en matière de protection de la vie privée.

L'analyse indique aussi que l'utilisateur doit disposer des outils appropriés qui renforceront la protection de ses renseignements personnels sur les SRS. Ces outils lui permettront non seulement de comprendre le contexte dans lequel ses renseignements personnels sont recueillis et de choisir le niveau d'échange de renseignements qui lui convient, mais aussi de mettre en place les mécanismes de protection appropriés selon le niveau choisi et, par le fait même, d'implanter un système de protection de la confidentialité tout aussi valable que convivial.

Suivant cette conception de la protection de la vie privée axée sur l'utilisateur, la dernière partie du document présente l'analyse comparative des SRS selon chacune des catégories définies, de même que des recommandations pour établir le niveau de compréhension et les mesures de protection de la vie privée souhaités, tout cela dans le but de créer des occasions d'améliorer la protection des renseignements personnels.

A : PORTÉE

Ce document propose une analyse comparative du traitement des renseignements personnels sur six (6) SRS choisis.

Aux fins de cette analyse, la définition de SRS retenue est celle donnée par boyd et Ellison, selon laquelle les SRS sont des « services Web qui permettent à une personne (1) de créer un profil public ou partiellement public au sein d'un système délimité, (2) de dresser la liste des autres utilisateurs avec lesquels elle est en relation, et (3) de voir et de parcourir sa liste de relations et celle d'autres utilisateurs du système »[1] [Traduction]. Tous les sites choisis répondent à ces critères, bien que l'organisation de leurs services soit différente.

La distinction faite dans ce document entre un « site de réseau social » et un « site de réseautage social » repose également sur les définitions énoncées par boyd et Ellison. Même si, à première vue, ces deux expressions semblent synonymes, c'est le terme « site de réseau social » qui sera retenu aux fins de l'analyse. Cette décision ne se limite pas à une simple question de style. Il s'agit plutôt de souligner, en considérant le réseau comme un objet et non le résultat de l'action de réseauter, le fait que ces sites ne servent pas principalement à créer des (nouveaux) liens, mais plutôt à structurer et à révéler des réseaux sociaux[2] établis ou en développement.

Voici la liste des six sites Web qui seront examinés (en ordre alphabétique) :
1. Facebook (http://www.facebook.com)
2. Hi5 (http://hi5.com)
3. LinkedIn (http://www.linkedin.com)
4. LiveJournal (http://www.livejournal.com)
5. MySpace (http://www.myspace.com)
6. Skyrock (http://www.Skyrock.com)

Ces sites ont été choisis en raison de leur popularité, mais aussi pour offrir une analyse complète et multivariée. En date du 31 janvier 2009, quatre (4) des six (6) sites figuraient sur la liste des 100 sites les plus populaires au Canada[3], tandis que les deux (2) autres, également bien connus, y étaient répertoriés dernièrement. Par ailleurs, ces SRS ont été choisis car ils reflètent divers intérêts (blogage, réseautage professionnel, musique, etc.) et types d'utilisateurs.

De toute évidence, chaque SRS constitue sa propre plateforme et offre un nombre presque illimité d'interactions avec le site et ses utilisateurs. En conséquence, l'examen complet de chaque site excéderait la portée de la présente analyse. L'analyse a pour but d'examiner les caractéristiques relatives à la protection de la vie privée de chacun des SRS, à l'aide des catégories suivantes :
- Renseignements relatifs à l'inscription
- Identités réelles et pseudonymes
- Mesures de protection de la vie privée
- Marquage de photos
- Accessibilité aux renseignements des membres
- Publicité
- Conservation des données
- Fermeture de compte
- Applications tierces
- Collecte des renseignements personnels des non membres

Une fois ces catégories examinées pour chacun des SRS, l'analyse permettra d'évaluer les décisions prises par les propriétaires de ces sites à l'égard de la protection de la vie privée, pour ensuite cibler les occasions d'améliorer la protection sur ces sites.

Remarque au sujet des limites d'âge

Initialement, une des catégories portait sur l'évaluation de la politique des sites concernant les limites d'âge. Cependant, le 10 février 2009, l'Union européenne (UE) a annoncé la conclusion d'une entente avec 17 SRS pour « améliorer la sécurité des mineurs qui utilisent les sites de socialisation »[4] . Puisque cette entente aura sans doute des répercussions sur la politique de limite d'âge des sites signataires (trois des six sites examinés dans ce document, à savoir Facebook, MySpace et Skyrock, ont signé l'entente), voire des sites non signataires, on a jugé qu'une analyse de la politique mise en place avant la conclusion de l'entente ne servirait en rien la cause de la protection de la vie privée sur les SRS.

Les personnes désireuses d'explorer la question sont invitées à consulter directement l'entente de l'UE[5] ainsi qu'à étudier les travaux déjà publiés sur les jeunes et Internet[6] et sur les difficultés liées à la vérification de l'âge[7].

B : CONTEXTUALISATION DE LA RÉFLEXION

En examinant la façon dont les gens utilisent les SRS et les renseignements qu'ils contiennent, on se rend à l'évidence que ces renseignements sont presque systématiquement considérés comme appartenant au domaine public. En effet, pour l'instant, il semble que « les renseignements personnels que les utilisateurs fournissent sur les sites à accès et aux fonctions de recherche contrôlés relèvent en réalité du domaine public »[8] [Traduction]. Par contre, selon certaines études, il est tout aussi vrai que les utilisateurs de SRS, bien qu'ils n'emploient pas toujours les mesures de protection de la vie privée dans la proportion espérée, manifestent « de grandes inquiétudes à l'égard de la protection de leurs renseignements personnels »[9] [Traduction]. Afin de résoudre cette contradiction apparente, Grimmelmann propose de centrer la réflexion sur l'utilisateur : « plus on réduira l'écart entre le niveau de protection souhaité et le niveau offert, moins l'utilisateur prendra de mauvaises décisions »[10] [Traduction].

C'est ici que la théorie d'Helen Nissenbaum sur le lien entre l'intégrité contextuelle et la protection de la vie privée se révèle d'une certaine utilité. D'emblée, Nissenbaum déclare que « pratiquement tout, que ce soit des gestes, des événements ou des transactions, se produit non seulement dans un contexte situationnel, mais aussi en fonction de principes, de conventions et de coutumes établis »[11] [Traduction]. À la lumière de cette affirmation, elle indique qu'une situation perçue comme portant atteinte à la vie privée découle de la transgression de l'une ou l'autre des normes suivantes : la norme qui dicte les renseignements pouvant être recueillis et la norme qui détermine comment ces renseignements circulent et dans quelle mesure ils peuvent être communiqués. Cette reconnaissance du contexte abonde dans le sens du constat de Grimmelmann voulant que « le principe clé réside dans la compréhension de la dynamique sociale liée à l'utilisation de la technologie, puis dans l'établissement de mesures d'intervention conséquentes »[12] [Traduction]. C'est pourquoi il faut examiner le contexte entourant les SRS (et les attentes des utilisateurs) pour cerner et étudier les questions relatives à la protection de la vie privée.

Penchons nous d'abord sur le « caractère public » des SRS. Certains prétendent que le fait de considérer les SRS comme des sites privés résulte d'une confusion entre « ce qui relève du domaine public et du domaine privé sur Internet »[13] [Traduction]. Toutefois, cette réflexion un peu simpliste ne fait qu'encourager les campagnes d'information sur l'utilisation d'Internet en général, plus particulièrement des SRS, une méthode qui ne semble pas avoir été efficace jusqu'à présent. Une démarche proactive pour l'analyse des questions liées aux SRS doit débuter par un examen de l'opposition binaire des notions du public et du privé.

À ce sujet, danah boyd classe les SRS parmi les « espaces publics médiatisés », c'est à dire les environnements où « les gens peuvent se rassembler publiquement grâce aux technologies des médias » [Traduction]. Elle soutient que les espaces publics médiatisés se distinguent des espaces publics physiques sur quatre plans : (1) la pérennité des données, (2) la facilité de recherche, (3) la reproduisibilité et la transférabilité, et (4) l'invisibilité du public.[14] Comme le souligne Albrechtslund, ces caractéristiques entraînent leur lot de conséquences, puisque « les réseaux sociaux en ligne peuvent comporter une part de communication privée en raison de leur caractère situationnel et anodin, mais les espaces publics médiatisés ne sont certainement pas privés. Cette dichotomie se trouve évidemment au cœur du débat sur la surveillance et la protection de la vie privée; elle devient d'autant plus apparente en raison de l'usage secondaire des renseignements disponibles sur les sites de réseau social »[15] [Traduction]. Sur les SRS, les frontières entre le public et le privé se brouillent; par conséquent, les participants au fonctionnement de ces sites (les utilisateurs, les propriétaires et administrateurs ainsi que les spécialistes du marketing qui cherchent à utiliser les données recueillies dans ces espaces en ligne et, en apparence, publics) n'ont aucune idée claire des pratiques exemplaires à adopter. Cette zone grise résulte peut-être d'un manque de profondeur dans l'étude de la question : il ne s'agit pas de délimiter les frontières entre le domaine public et le domaine privé, ni même de confirmer l'existence d'une telle séparation, mais plutôt d'évaluer les attentes par rapport à ces deux domaines.

En 2006, Acquisti et Gross soulevaient ceci : « certaines preuves semblent indiquer que les comportements à l'égard de la vie privée influencent en partie la décision de participer ou non à un réseau, mais que les renseignements dévoilés par les participants d'un groupe ne varient que très peu, peut-être en raison d'une pression uniformisante ressentie ou par

grégarisme »[16] [Traduction]. Il semble évident que les normes de groupe modifient les comportements sur les SRS, tout comme « les adolescents analysent un contexte à partir des perceptions des autres »[17] [Traduction]. Ainsi, dans les cas où les frontières sont brouillées, on peut présumer que tous les utilisateurs, peu importe leur âge, se fixent des attentes comportementales en fonction des actions des autres sur le site.

Sur les SRS, la communication et l'échange de renseignements sont des processus ouverts et, jusqu'à un certain point, continus. Peu importe la portée réelle des renseignements transmis sur ces sites, « (…) les adolescents ne réfléchissent pas dans une perspective élargie. Bien que leur public potentiel soit mondial, ils le perçoivent comme un public très local, constitué principalement de personnes qu'ils connaissent »[18] [Traduction]. L'utilisateur pense en fonction de ses « amis », puis dresse son profil et interagit selon ce public. Ensemble, le public perçu et les normes de groupe peuvent créer une « illusion de vie privée protégée »[19] [Traduction]. Cependant, la notion d'intégrité contextuelle permet de dissiper cette illusion au profit d'une réflexion plus productive sur les attentes à l'égard de la protection de la vie privée au sein d'un espace. Ainsi, si l'utilisateur se concentre sur un public en particulier et tient compte des normes de groupe pour nourrir ses attentes en matière de protection de la vie privée, le meilleur moyen d'améliorer la confidentialité sur les SRS n'est peut-être pas d'aller à l'encontre de ces attentes. Il faut plutôt mettre en place des mesures de protection de la vie privée qui combleront les attentes de l'utilisateur ou les clarifieront en augmentant sa compréhension du contexte dans lequel se déroule ses interactions sur les SRS.

L'ouverture constitue, dans une certaine mesure, un « aspect conçu du système (…); pour atteindre l'objectif fixé, il faut souvent être plus permissif par rapport à la confidentialité des profils »[20] [Traduction]. Par ailleurs, l'utilisateur n'a pas l'habitude d'avoir recours à des mécanismes de protection de la vie privée au cours d'interactions sociales. Comme le soulignent Dwyer et coll., « hors ligne, la plupart des interactions sociales ne laissent aucune trace. Cette éphémérité joue un rôle passif dans l'établissement de paramètres de confidentialité sur le plan social. En conséquence, ces sites doivent se munir d'une politique et de mécanismes de protection de données explicites pour offrir le même niveau de confidentialité dont on jouit hors ligne »[21] [Traduction]. Toutefois, ce besoin de protection provoque des tensions particulières parmi les exploitants de sites Web, puisque « d'emblée, l'exploitant d'un site Web poursuit simultanément des objectifs divergents à l'égard de la confidentialité. D'une part, il doit s'assurer qu'une quantité suffisante de renseignements personnels est diffusée pour attirer de nouveaux membres; d'autre part, il doit voir à ce que certains renseignements restent exclusifs aux membres de la communauté en ligne pour justifier l'adhésion à cette communauté »[22] [Traduction]. Ainsi, si le but de la réflexion consiste à déterminer ce que la vie privée représente aux yeux de l'utilisateur et comment il peut la protéger le mieux possible, la prise de décisions ne peut pas incomber uniquement aux exploitants de sites Web[23].

La clé pour sensibiliser l'utilisateur à l'importance de la confidentialité sur les SRS ne se résume pas à la création de politiques et de mesures de protection de la vie privée. En effet, il faut aussi voir à ce que la prise de décisions en matière de protection de la vie privée sur les SRS devienne pratique courante, non seulement chez les utilisateurs déjà inscrits, mais aussi chez les nouveaux membres.


adaptable
communication
efficace
applications
affichable
connaissances
commentaires
social
photos
mur
marquage
collège
emplacement
cadeaux virtuels
actuel
efficient
amélioré
clavardage
divertissant
accessible
entreprise
jeune
réseau
billets
dynamique
statut
rapide
groupe
international
système
paramètres
amis
applications
mises à jour
messages
communiquer
actualités
développement
échange
gratuit
simple
sécurité
école secondaire
generational
pokes
complet
pratique
jeux
données
témoins
commode
populaire
affichable
innovateur
débrouillard
professionnel
significatif
albums
utile
communauté

Facebook

Facebook

www.facebook.com

Mandat

Facebook se définit comme « un utilitaire social qui facilite la communication entre amis, parents et collègues de travail »[24] [Traduction].

Historique

Le site Facebook a été fondé le 4 février 2004 par Mark Zuckerberg, l'actuel PDG. Le site en soi est exploité par Facebook Inc., une entreprise privée. Le siège social est situé à Palo Alto, en Californie, tandis que le siège social international (qui dessert l'Europe, l'Afrique et le Moyen Orient) se trouve à Dublin, en Irlande[25].

À l'origine, l'utilisation de Facebook, une application créée à l'Université Harvard, était restreinte à cette institution, puisque seulement les personnes possédant un courriel à l'adresse Harvard.edu pouvaient s'y inscrire. En mars 2004, le réseau s'est étendu à d'autres universités de l'Ivy League, soit Stanford, Columbia et Yale, puis à tous les étudiants de niveau collégial et universitaire aux États Unis. En septembre 2005, Facebook comptait également parmi ses membres des étudiants de niveau secondaire. En octobre 2005, il a ouvert ses portes aux écoles à l'échelle internationale. Enfin, en septembre 2006, le site permettait à toutes les personnes âgées de plus de 13 ans de devenir membre.

Information financière

L'utilisation du site Facebook est gratuite.

À l'été 2004, Peter Thiel, cofondateur de PayPal, a investi un montant initial de 500 000 $ dans Facebook. En avril 2005, Accel Partners a versé une somme de 12,7 millions de dollars. Depuis, un montant supplémentaire de 25 millions de dollars a été investi par Greylock Partners, Meritech Capital Partners, Accel Partners et Peter Thiel[26].

En octobre 2007, Microsoft a acheté 1,6 % des parts de Facebook pour la somme de 240 millions de dollars, une transaction qui a élevé la valeur totale du site à 15 milliards de dollars. Malgré cette évaluation, à l'automne 2008, l'entreprise Facebook Inc. a obligé ses employés à ne vendre leurs actions qu'à des prix fixés selon une valeur n'excédant pas 3,75 milliards de dollars[27].

En ce qui a trait à d'autres formes de revenus, Facebook permet à ses utilisateurs d'acheter des cadeaux virtuels au prix unitaire de 1 $US.

Lors d'une entrevue accordée récemment, Mark Zuckerberg a refusé de se prononcer sur les revenus générés par l'application Cadeaux et par la publicité intéressée, mais il a laissé entendre qu'à elle seule, ce type de publicité produisait un revenu annuel de plus de 50 millions de dollars[28].

Profil démographique des utilisateurs

En janvier 2009, Facebook comptait plus de 150 millions d'utilisateurs actifs (c'est à dire qui ont accédé au site dans les 30 derniers jours)[29]. Selon un rapport comScore, en décembre 2008, Facebook a accueilli 222 millions de visiteurs uniques et affichait un taux de croissance de 127 % cette année-là[30].

Aujourd'hui, plus de 50 % des utilisateurs de Facebook ne proviennent pas du milieu universitaire, malgré le fait que le site détient encore 85 % du marché des universités américaines offrant des programmes d'études de 4 ans. En fait, la catégorie d'utilisateurs qui connaît la plus forte croissance est celle des 30 ans et plus[31].

Actuellement, plus de 70 % des utilisateurs de Facebook sont à l'extérieur des États Unis. Le Canada compte le plus grand nombre d'utilisateurs non américains, soit plus de 7 millions d'utilisateurs actifs. Le Royaume Uni occupe le troisième rang avec, lui aussi, plus de 7 millions d'utilisateurs actifs. Parmi les 10 pays ayant le plus grand nombre d'utilisateurs non américains, citons également l'Australie, la Turquie, la Suède, la Norvège, l'Afrique du Sud, la France ainsi que la région administrative spéciale de Hong Kong[32].

Renseignements relatifs à l'inscription

Une fois sur le site Facebook.com, l'utilisateur est invité à inscrire son nom au complet, son adresse de courriel, son mot de passe, son sexe et sa date de naissance. Une fenêtre contextuelle indique que la date de naissance est requise « comme mesure de sécurité et comme protection pour l'intégrité du site », et que l'utilisateur pourra cacher cette information de son profil s'il le souhaite. En s'inscrivant, l'utilisateur

indique qu'il a lu et accepté les conditions d'utilisation et la politique de confidentialité. Après avoir cliqué sur « Inscription », l'utilisateur accède à une page de test captcha. S'il entre correctement le code captcha, il recevra un courriel de confirmation à l'adresse qu'il a fournie en s'inscrivant. L'utilisateur doit cliquer sur un lien indiqué dans le courriel pour confirmer qu'il désire ouvrir un compte Facebook et que l'adresse de courriel fournie est valide.

Après avoir cliqué sur le lien de confirmation, l'utilisateur entame un processus en quatre étapes. D'abord, il est invité à accepter ou à rejeter une invitation à devenir l'ami d'une de ses connaissances. Cette étape peut être sautée.

Ensuite, l'utilisateur est invité à rechercher des amis en permettant à Facebook d'accéder à son carnet d'adresses de courriel. Un avis explique clairement à l'utilisateur qu'en procédant ainsi, il fournit des renseignements à Facebook. Cette étape peut également être sautée. La troisième étape invite l'utilisateur à remplir son profil, notamment en fournissant des renseignements sur ses études secondaires et postsecondaires (incluant l'année de promotion) et sur son travail. Cette tâche peut être sautée. Toujours à cette étape, l'utilisateur doit choisir, parmi une série de profils Facebook, ceux qui correspondent à des personnes qu'il connaît afin de les ajouter comme amis. Cette étape peut également être sautée.

Enfin, l'utilisateur est invité à indiquer son emplacement géographique (sa ville); on lui explique alors que cette information lui permettra de voir le profil d'autres personnes sur le réseau, et vice versa. Une autre mention précise que cet accès peut être modifié dans les paramètres de confidentialité. Cette étape peut être sautée.

Après avoir exécuté toutes ces étapes, l'utilisateur possède un profil Facebook. La page dans laquelle l'utilisateur se trouve à ce moment contient tous les amis ou les liens proposés pendant la création du compte, une barre latérale « Vous connaissez peut-être », ainsi que des bannières dans le haut pour retrouver ses amis ou encore voir et modifier son profil.

Dans la section qui permet de voir et de modifier le profil, on trouve un modèle qui contient les renseignements déjà fournis, ainsi que des espaces prévus pour indiquer d'autres renseignements selon les catégories suivantes : Informations générales (Sexe, avec l'option de l'afficher ou non dans le profil; Date de naissance en format mm/jj/aaaa, avec l'option d'afficher ou non la date en entier dans le profil; Ville natale; Situation amoureuse; Intéressé(e) par Hommes/Femmes; Je recherche Amitié/Rencontres/Une relation/Réseau professionnel; Opinions politiques; Religion); Informations personnelles (zones à remplir intitulées Activités, Intérêts, Style de musique, Émissions de télévision, Films, Livres et À propos de moi); Coordonnées (Adresses électroniques, avec l'option d'ajouter ou d'effacer des adresses; Pseudo(s) de messagerie instantanée; Téléphone mobile; Téléphone fixe; Adresse; Ville; Code postal; Site Web); Formation et emploi (Établissement d'enseignement supérieur; Promotion; Matière principale; Diplôme, avec l'option d'ajouter ou de supprimer des écoles et des matières; Lycée; Promotion, avec l'option d'ajouter ou de supprimer des écoles; Employeur; Fonction; Description; Ville; Dates, avec l'option d'ajouter des emplois).

Ainsi, les seuls renseignements obligatoires pour ouvrir un compte Facebook sont le nom au complet, l'adresse de courriel, le mot de passe, le sexe et la date de naissance. Cependant, les étapes détaillées de création de profil et le modèle qui prévoit des espaces pour certains renseignements sèment la confusion quant aux renseignements « obligatoires » et « demandés ».

Identités réelles et pseudonymes

Bien que Facebook vérifie les adresses de courriel, le site n'effectue aucune vérification indépendante du nom complet fourni, pas plus qu'il ne semble déceler les écarts entre le nom et l'adresse de courriel donnés à l'inscription. En ce sens, il n'y a aucune mesure ou vérification prévues dans le système de Facebook pour imposer l'inscription à partir d'un nom ou d'une identité véritables.

Toutefois, les conditions d'utilisation mentionnent ce qui suit :

> « Vous acceptez : (a) de fournir des informations appropriées, actuelles et complètes vous concernant dans les formulaires d'inscription du Site (« Données d'inscription »); (b) d'utiliser un identifiant et un mot de passe sécurisés; (c) de mettre à jour, au besoin, les données d'inscription et toutes autres informations que vous fournissez à la Société afin qu'elles restent appropriées, actuelles et complètes; et (d) d'être responsable de l'utilisation de votre compte et de n'importe quelles actions effectuées à l'aide de votre compte[33]. »

Mesures de protection de la vie privée

Facebook possède une série de mesures détaillées pour la protection de la vie privée[34], de même qu'une politique de confidentialité[35].

Les mesures de protection de la vie privée comptent quatre sections : Profil, Recherche, Actualités et mur, et Applications. Chaque section permet à l'utilisateur de mettre en place des mesures précises.

PROFIL : Cette section permet à l'utilisateur de gérer l'accès à ses informations générales et à ses coordonnées. Les catégories d'informations générales sont le profil, les informations personnelles, les statuts, les photos sur lesquelles l'utilisateur a été marqué, les vidéos dans lesquelles il a été marqué, les amis, les messages du mur, les informations sur la formation et les informations sur l'emploi. Les catégories de coordonnées sont le nom d'utilisateur de messagerie instantanée, le numéro de téléphone mobile, les autres numéros de téléphone, l'adresse actuelle, le site Web, le lieu de résidence et l'adresse de courriel. L'utilisateur désigne les personnes qui peuvent accéder au contenu de chacune de ces catégories : son réseau et ses amis, les personnes d'un réseau choisi et ses amis, les amis de ses amis, ou encore seulement

ses amis. Il peut également définir son propre groupe de personnes en choisissant parmi les membres des réseaux existants, par exemple les étudiants de premier cycle, les étudiants de deuxième cycle, les diplômés, le corps professoral et le personnel, dans le cas d'un établissement d'enseignement.

RECHERCHE : Cette section permet à l'utilisateur de déterminer qui, sur Facebook, sera en mesure d'accéder à son profil. Toutefois, les amis de l'utilisateur pourront toujours le retrouver à l'aide d'une recherche. Grâce à ces paramètres, l'utilisateur peut d'abord établir la visibilité de son profil dans le contexte d'une recherche, à partir des mêmes options mentionnées précédemment (son réseau et ses amis, les personnes d'un réseau choisi et ses amis, les amis de ses amis, seulement ses amis ou un groupe personnalisé). Il peut aussi définir des paramètres de recherche supplémentaires, notamment en autorisant ou non des réseaux universitaires, secondaires, professionnels ou régionaux à accéder à son profil. De plus, l'utilisateur peut déterminer les renseignements à afficher pour ceux qui recherchent son profil et les options offertes pour communiquer avec lui.

ACTUALITÉS ET MUR : Cette section permet à l'utilisateur de gérer les actions sur Facebook et les publicités sociales. En ce qui a trait aux actualités, la section indique une liste d'éléments qui ne feront jamais l'objet de publications et une liste d'applications pour lesquelles il y a possibilité de publication. De plus, la section indique que des éléments d'actualités seront publiés à l'exécution de certaines actions, notamment la modification du profil, la participation à un nouveau réseau et la mise à jour du statut. L'utilisateur peut également cocher des cases afin d'autoriser ou non des publications pour les actions suivantes : le retrait de renseignements sur le profil; l'écriture d'un commentaire sur le mur d'un ami; l'écriture d'un commentaire sur un article, une photo, un album, une vidéo ou un lien; la participation à un forum de discussion; l'ajout d'un ami; la modification de la situation amoureuse; et la désertion d'un réseau. Enfin, l'utilisateur a la possibilité d'afficher ou non les actualités dans les discussions en ligne et d'indiquer ou non l'heure de publication des actualités sur son mur. La page des publicités sociales contient l'avertissement suivant : « Facebook associe parfois des publicités aux actions pertinentes d'un ami de l'utilisateur, créant ainsi des "publicités sociales", des publicités plus intéressantes et plus adaptées à vous et vos amis. Elles respectent cependant toutes les règles de confidentialité[36]. » L'utilisateur peut décider de figurer ou non dans les publicités sociales de ses amis.

APPLICATIONS : Cette section offre une vue d'ensemble de la manière dont les applications utilisent les renseignements personnels, tout en permettant à l'utilisateur d'appliquer des paramètres de confidentialité à ses interactions dans les limites des applications. Cette page contient six mesures de protection de la vie privée. Premièrement, l'utilisateur peut restreindre les renseignements auxquels ses amis ont accès grâce à des applications qu'il n'utilise pas lui même. Il peut également décider de ne plus échanger de renseignements à partir des applications de Facebook, à condition qu'aucune application ne soit sélectionnée dans son profil. Deuxièmement, si l'utilisateur autorise une application, celle ci peut, pour assurer son bon fonctionnement, utiliser tous les renseignements du profil de l'utilisateur, à l'exception des coordonnées. Troisièmement, l'utilisateur peut se servir de la fonction Facebook Connect pour interdire à ses amis de consulter ses renseignements à partir d'autres sites Web. Quatrièmement, l'utilisateur peut empêcher le logiciel Beacon de publier des actualités sur son profil. Enfin, les deux dernières mesures portent respectivement sur le blocage d'applications, y compris une liste des applications actuellement bloquées par l'utilisateur, et sur le blocage d'invitations à utiliser des applications provenant d'amis en particulier, incluant une liste des amis dont les invitations sont actuellement bloquées.

Marquage de photos

À l'heure actuelle, Facebook est l'application préférée des internautes pour l'échange de photos[37]. En date du 29 janvier 2009, plus de 800 millions de photos étaient téléchargées sur le site chaque mois[38].

Facebook a créé l'application Photos en octobre 2005. Cette application permet à l'utilisateur de télécharger un nombre illimité de photos sur le site, au moyen d'albums pouvant contenir jusqu'à 60 photos. L'utilisateur peur régler les paramètres de confidentialité de chaque album, limitant ainsi les groupes d'utilisateurs qui auront accès au contenu de l'album.

Lorsque l'utilisateur télécharge une photo, il doit confirmer qu'il est autorisé à le faire.

Grâce à l'application Photos, l'utilisateur peut également « marquer » des personnes dans une photo en y associant des métadonnées. Si la personne marquée est un autre utilisateur de Facebook, elle sera avisée de cette action, recevra un lien pour voir la photo et pourra exiger que le marquage soit retiré. Le marquage crée également un lien entre la photo et le profil de l'utilisateur de Facebook marqué.

Une photo peut être marquée par n'importe quel utilisateur de Facebook ayant accès à la photo; on peut ajouter n'importe quel nom, y compris celui des personnes qui ne sont pas membres de Facebook. Lorsqu'un non membre est marqué dans une photo, une fenêtre contextuelle invite l'auteur du marquage à inscrire l'adresse de courriel de la personne marquée pour l'aviser et, éventuellement, l'ajouter à sa liste d'amis. Les personnes qui reçoivent ce courriel peuvent voir la photo, mais n'ont pas accès au reste du site.

Accessibilité aux renseignements des membres

Évidemment, l'accessibilité aux renseignements fait l'objet de mesures de protection de la vie privée établies par l'utilisateur.

ACTUALITÉS : Lancée en septembre 2006, cette fonction fait en sorte que l'utilisateur voie les actualités une fois qu'il se connecte à Facebook. Ces actualités comprennent des éléments recueillis parmi les

activités pratiquées sur Facebook par les personnes sur la liste d'amis de l'utilisateur. Inversement, une partie des renseignements personnels et des activités de l'utilisateur sont affichés dans les actualités de ses amis. Actuellement, l'utilisateur peut interdire l'affichage de certains renseignements dans les actualités. Il peut notamment retirer des renseignements sur son profil, écrire un commentaire sur le mur d'un ami, écrire un commentaire sur un article, une photo, une vidéo ou un lien, participer à un forum de discussion, ajouter un ami, modifier sa situation amoureuse ou déserter un réseau. Soulignons que certaines applications (comme les publicités sociales ou le logiciel Beacon) peuvent utiliser des renseignements inclus dans les paramètres de confidentialité des actualités, mais que ces paramètres n'ont aucune incidence sur ces applications. Les renseignements dont l'utilisateur autorise l'affichage dans les actualités, le cas échéant, sont définis dans les paramètres de confidentialité des applications.

RECHERCHE SUR LE SITE : Les utilisateurs de Facebook peuvent se joindre à plusieurs réseaux sur le site, notamment celui d'une école, d'un lieu de travail, d'une région géographique ou d'un groupe social. Ils peuvent ainsi communiquer avec d'autres membres du même réseau. L'utilisateur qui effectue une recherche sur Facebook a accès aux détails du profil des autres utilisateurs du réseau ou de ses amis. L'utilisateur qui recherche une personne qui ne fait pas partie de son réseau ni de sa liste d'amis peut (selon les paramètres de confidentialité de la personne recherchée) obtenir la confirmation que la personne en question possède un profil, mais ne verra que ses renseignements de base, soit sa photo, son nom ainsi que l'option d'envoyer un « poke » (signe d'attention).

RECHERCHE PUBLIQUE : Au départ, seuls les membres de Facebook pouvaient rechercher d'autres utilisateurs du site, et les renseignements affichés dépendaient des réseaux que les deux personnes avaient en commun. Cependant, en septembre 2007, Facebook a introduit les répertoires de recherche publique. Un répertoire de recherche publique contient habituellement la photo et le nom provenant du profil de l'utilisateur de Facebook. Les recherches publiques permettent aux non membres d'effectuer des recherches sur Facebook, en plus de permettre à certains moteurs de recherche importants d'indexer les répertoires publics. Toutefois, l'utilisateur peut appliquer des mesures de protection de la vie privée pour retirer ses renseignements des répertoires.

Publicité

Facebook tire la plupart de ses revenus de la publicité.

En août 2006, Facebook et Microsoft ont établi un partenariat stratégique pour la souscription de bannières publicitaires. En octobre 2007, cette entente a été étendue aux marchés internationaux. Microsoft est le fournisseur exclusif de Facebook pour les bannières publicitaires.

En novembre 2007, Facebook a lancé les publicités sociales[39] et une fonction pour créer des pages sur le site. Essentiellement, ces éléments permettent aux annonceurs et aux entreprises d'établir leur présence sur Facebook (ce qui, auparavant, était réservé aux particuliers), pour ensuite rentabiliser cette présence en s'associant à des utilisateurs. Lorsqu'un utilisateur visite la page d'un annonceur, un élément d'actualités est créé au sujet de cette interaction.

Les publicités sociales sont également activées par ce type d'interaction. La publicité sociale créée contient l'avis de la visite, le nom de l'utilisateur et la photo de son profil, de même qu'un texte écrit par l'annonceur. La publicité paraît ensuite dans les actualités des amis de l'utilisateur. Ce genre de publicité peut aussi cibler les amis d'un utilisateur à partir de caractéristiques démographiques communes, comme l'emplacement, la tranche d'âge, le sexe ou d'autres éléments de son profil Facebook. Grâce aux mesures de protection de la vie privée, l'utilisateur peut refuser de figurer dans des publicités sociales publiées dans les actualités de ses amis. Cependant, l'inverse ne semble pas possible : l'utilisateur ne peut refuser de recevoir de telles publicités contenant des renseignements sur ses amis.

Lancé en novembre 2007, le logiciel Beacon est l'autre mode de publicité bien connu de Facebook. Il fonctionne de manière similaire aux publicités sociales, soit en associant des utilisateurs de Facebook à des annonceurs, puis en avisant les amis de l'utilisateur. Toutefois, plutôt que de viser les interactions avec les annonceurs présents sur Facebook (comme le font les publicités sociales), Beacon affiche les interactions avec les sites Web de tiers. Les annonceurs peuvent ajouter du code à leur site Web afin de favoriser les interactions avec Beacon et ainsi déterminer quelles interactions créeront des actualités sur Facebook[40]. L'utilisateur peut bloquer le logiciel Beacon dans son profil.

Conservation des données

Facebook recueille à la fois les renseignements personnels fournis volontairement par l'utilisateur et « des données relatives à l'utilisation du site Internet que [Facebook collecte] quand [l'utilisateur interagit] avec [son site] Internet ». Ces deux types d'informations sont abordés dans la politique de confidentialité[41].

La politique de confidentialité de Facebook, mise à jour le 26 novembre 2008, peut être consultée à partir d'un lien situé au bas de n'importe quelle page du site. Voici quelques faits notables concernant cette politique : (1) elle est vérifiée par l'organisation indépendante TRUSTe; (2) elle débute par un énoncé des principes de Facebook, dans un langage simple, qui met l'accent sur le contrôle que l'utilisateur peut exercer sur ses renseignements personnels ainsi que sur l'accès aux renseignements que les autres souhaitent communiquer; et (3) elle témoigne d'un effort visible pour contourner le jargon juridique et transmettre l'information au lecteur de manière conviviale.

Les renseignements personnels fournis par l'utilisateur comprennent les renseignements donnés à l'inscription et à la configuration d'un profil, les renseignements sur les relations, les messages envoyés, les recherches, la formation de groupes et la participation à des groupes,

la création d'événements et la participation à des événements, l'ajout d'applications ainsi que d'autres renseignements transmis au moyen des différentes fonctions de Facebook. Selon la politique de confidentialité, ces renseignements sont recueillis pour offrir un service et des fonctions personnalisés. Lorsque les renseignements sont mis à jour, une copie de sauvegarde des versions antérieures est conservée « pendant un certain temps » pour permettre la récupération des informations, au besoin.

Facebook enregistre le type de navigateur et l'adresse IP de tous les visiteurs du site. De plus, il utilise des témoins (« cookies »), notamment des témoins d'identification (qui sont supprimés à la fermeture du navigateur) et des témoins permanents (que l'utilisateur peut supprimer ou bloquer dans les paramètres de son navigateur). Bien que la politique de confidentialité décrive le type de renseignements recueillis et la raison de leur collecte, elle omet de préciser leur période de conservation.

Par ailleurs, Facebook recueille et conserve les renseignements fournis par ses utilisateurs au sujet de non membres. Selon la politique de confidentialité, un non membre peut communiquer avec Facebook pour demander que ses renseignements soient retirés de la base de données du site.

Fermeture de compte

Initialement, le processus de fermeture de compte sur Facebook posait certaines difficultés. Un compte pouvait être désactivé et, par le fait même, rendu inaccessible au public, mais son contenu était conservé sur les serveurs de Facebook, soi disant dans le but de faciliter le rétablissement du profil des utilisateurs qui souhaitaient rouvrir leur compte. Pour supprimer de manière permanente ses renseignements personnels, l'utilisateur pouvait les retirer de son profil un à un. Il s'agissant d'un processus laborieux, certes, mais efficace pour gérer les renseignements recueillis d'un profil; cependant, le profil Facebook lui-même n'était pas détruit.

Le 29 février 2008, Facebook a modifié son processus de fermeture de compte afin de permettre à ses utilisateurs de communiquer directement avec le site pour exiger que leur compte soit supprimé de façon permanente. Autrement, l'utilisateur a toujours la possibilité de désactiver son compte plutôt que de le fermer. Ses renseignements sont alors conservés sur les serveurs de Facebook, sans toutefois être accessibles aux autres utilisateurs.

Applications tierces

En mai 2007, Facebook a créé sa plateforme d'applications, à partir de laquelle les développeurs tiers peuvent créer des applications qui utilisent les fonctions de base de Facebook. Dans le cadre de cette plateforme, un langage de balisage propre à Facebook a été introduit pour permettre de personnaliser l'aspect et la convivialité des applications.

Ainsi, la plateforme lancée par Facebook permet aux tiers de créer des applications qui interfacent avec la base de données du site. Même si elles ne sont pas développées par Facebook, ces applications fonctionnent de manière similaire aux applications de Facebook. En conséquence, elles peuvent généralement publier des éléments dans les actualités de l'utilisateur et accéder à certains de ses renseignements.

Pour qu'une application tierce puisse fonctionner sur Facebook, les hôtes ou les développeurs de l'application doivent recevoir les renseignements personnels contenus sur Facebook. C'est au moment de l'installation d'une application que l'on indique à l'utilisateur les options d'échange de renseignements[42] et la manière dont l'application interagira avec son compte Facebook.

Les conditions d'utilisation des applications stipulent que lorsque l'utilisateur ajoute une application tierce, il accepte de partager tous ses renseignements, à l'exception de ses coordonnées :

> « Parmi les renseignements affichés sur Facebook, citons notamment les suivants, dans la mesure où ils sont visibles sur le site : votre nom; votre photo de profil; votre sexe; votre date de naissance; votre lieu de naissance (ville, province ou État, pays); votre lieu de résidence actuel (ville, province ou État, pays); vos opinions politiques; vos activités; vos intérêts; votre style de musique; vos émissions de télévision préférées; vos films préférés; vos livres préférés; vos citations favorites; le texte contenu dans votre section À propos de moi; votre situation amoureuse; vos intérêts amoureux; vos intérêts relationnels; vos plans pour l'été; les réseaux d'utilisateurs de Facebook auxquels vous appartenez; votre parcours scolaire; votre parcours professionnel; les cours que vous suivez; les copies des photos contenues dans vos albums Facebook; les métadonnées associées à vos albums photos Facebook (date de téléchargement sur le site, nom de l'album, commentaires sur les photos, etc.); le nombre total de messages envoyés ou reçus; le nombre total de messages non lus dans votre boîte de réception Facebook; le nombre total de « pokes » envoyés ou reçus; le nombre total de publications sur votre mur; la liste de vos amis sur Facebook; votre historique social; et les événements associés à votre profil »[43] [Traduction].

Comme le souligne le site de l'EPIC, il n'est pas anodin qu'une application tierce ajoutée par l'utilisateur n'ait pas seulement accès aux renseignements de l'utilisateur et aux modalités d'échange de ces renseignements. En réalité, d'après les conditions d'utilisation des applications, les paramètres d'accès par défaut touchent de nombreux renseignements sur les amis de l'utilisateur et sur tout autre membre de réseau auquel l'utilisateur a lui même accès. Ainsi, « sans aucune intervention de la part de l'utilisateur, une personne n'ayant jamais ajouté d'application verra ses renseignements transmis à une application tierce dès qu'un de ses amis ou un membre d'un réseau commun ajoute l'application »[44] [Traduction].

> Dans les conditions d'utilisation générales, Facebook décline toute responsabilité quant aux dommages causés par l'installation ou l'utilisation de ces applications; par contre, les conditions de service des développeurs de Facebook imposent des restrictions concernant l'utilisation des renseignements des utilisateurs, y compris les exigences suivantes :
>
> - le développeur doit accorder le même respect que Facebook à la vie privée de l'utilisateur. S'il recueille des données personnelles, il doit décrire en détail ce qu'il compte en faire au moyen d'une politique de confidentialité;
> - le développeur doit faire preuve d'honnêteté et d'exactitude quant au fonctionnement de ses applications et à la façon dont les renseignements recueillis sont utilisés. Aucune fausse représentation n'est permise;
> - le développeur peut divulguer des renseignements de la plateforme de Facebook à un utilisateur uniquement si les renseignements ont été recueillis au nom de cet utilisateur;
> - le développeur peut conserver les renseignements de l'utilisateur en mémoire cache pour une période maximale de 24 heures afin d'optimiser le rendement de ses applications;
> - toute activité pratiquée à partir de la plateforme de Facebook qui entraîne le non respect des droits de la personne, de la propriété intellectuelle ou de la loi, ou encore la création de pourriels ou de courriels d'hameçonnage, est interdite[45].

De cette façon, toute information qu'une application génère ou recueille de manière autonome peut être conservée indéfiniment et être associée à d'autres renseignements de Facebook qui peuvent également être conservés, comme l'identifiant de l'utilisateur. À première vue, il semble peut-être y avoir contradiction entre la période maximale de mise en mémoire cache énoncée dans les conditions de service des développeurs et l'autorisation de conserver certains renseignements indéfiniment. Toutefois, la nuance se situe entre les renseignements de Facebook à proprement dit et les renseignements générés par l'application. Facebook maintient qu'un tiers ne peut conserver les renseignements du site pendant plus de 24 heures, mais que les informations générées par l'application tierce sont distinctes des renseignements de Facebook et peuvent donc être conservées indéfiniment.

Récemment, Chris Kelly (agent principal de protection de la vie privée et chef de la politique publique mondiale pour Facebook) a répondu à une question sur la surveillance de la communauté de développeurs tiers. Il a déclaré que Facebook surveille effectivement toutes les demandes de renseignements soumises par les applications, tout en laissant entendre que Facebook adoptera peut-être des mesures plus strictes, notamment en mettant en place un programme maison de validation des applications qui permettra la révision interne des données afin de s'assurer que seules les données pertinentes sont recueillies[46].

Collecte des renseignements personnels des non membres

Facebook effectue la collecte des renseignements personnels des non membres à partir des comptes de ses utilisateurs, par exemple lorsqu'un utilisateur parle de Facebook à un ami non membre (à l'aide des fonctions d'importation de coordonnées ou de recherche d'amis) ou qu'un non membre est marqué dans une photo. Selon la politique de confidentialité, les coordonnées sont recueillies et conservées pour envoyer au non membre des avis, des invitations ou un maximum de deux rappels.

Même à la suite de l'envoi des avis et des rappels, Facebook conserve les renseignements pour enregistrer le nouveau lien établi avec un ami (si l'invitation est acceptée), permettre à l'utilisateur de voir les invitations qu'il a envoyées et évaluer le taux de réussite du programme de référence du site.

étudiants
base de données
communauté
contenu
occasion
originalité
améliorer
compagnons
capacité
potentiel
accessibilité
journaux
relations
unique
expérience
établissement
solutions
statut
formation
amélioration
intégration
sécurité
applications
ouverture
créativité
amis
débrouillard
acceptation
discussion
journaux
messages
mondial
entreprise
rentable
implantation
possibilité
cadeaux virtuels
emploi
inscription
échange
expansion
identification
adaptable
statistiques
carrières
développer
comptes
publicité
personnel
contacts
activation
avis
communication
mandat
documentation
divertissement
personnalité
Hi5

Hi5

www.hi5.com

Mandat

hi5 se décrit comme « un endroit pour rencontrer des amis en ligne » [Traduction].

Historique

Le site hi5 a été fondé en 2003 par Ramu Yalamanchi, entrepreneur d'origine indo américaine et actuel PDG. En janvier 2003, grâce à un investissement initial de 250 000 $, Yalamanchi et Akash Garg ont d'abord lancé Sona, un site de rencontre en ligne destiné au marché de l'Asie du Sud. Ce site visait à reproduire le concept du site match.com à l'échelle internationale[47].

En décembre 2003, le site a été lancé de nouveau sous le nom de hi5, un site de réseau social international[48]. Au départ, ce site a été lancé en anglais sur tous les marchés.

Selon les fondateurs du site, hi5 comptait un million d'utilisateurs après six mois d'existence (en juillet 2004) et, en juin 2008, il s'y ajoutait « un million d'utilisateurs par semaine »[49] [Traduction].

Rapidement, les fondateurs ont ciblé les marchés hispanophones lorsqu'ils ont constaté, d'une part, la popularité de leur site dans les régions visées et, d'autre part, certaines affinités parmi les utilisateurs hispanophones. Un autre facteur les a incités à exploiter ce marché : à l'époque, MySpace ne permettait pas aux utilisateurs situés à l'extérieur des États Unis de s'inscrire. On les filtrait à partir de leur adresse IP. Inversement, hi5 visait précisément les marchés internationaux.

Information financière

L'entreprise est rentable depuis octobre 2004.

Le site semble touché par la crise économique mondiale. On rapporte des mises à pied et la perte d'annonceurs en raison de la diminution du nombre de visiteurs uniques[50].

Depuis 2008, hi5 tire également des profits de la vente de cadeaux virtuels. Chaque cadeau peut être acheté avec des « pièces », elles-mêmes achetées avec de l'argent réel. Le prix unitaire des cadeaux équivaut à 1 $US[51].

Profil démographique des utilisateurs

À l'échelle mondiale, plus de 80 millions de personnes possèdent un compte hi5, et le site accueille près de 46 millions de visiteurs uniques par mois (selon les statistiques d'avril 2008 fournies par hi5)[52]. En juillet 2008, hi5 déclarait que, selon les chiffres enregistrés par l'outil de mesure Media Metrix de comScore pour juin 2008, il était « le site de réseautage social ayant connu la plus forte croissance pendant la première moitié de 2008 »[53] [Traduction]. Au cours du même mois, comScore annonçait que le site accueillait plus de 50 millions de visiteurs uniques par mois[54].

Le site hi5 est le service de réseau social le plus populaire auprès des hispanophones[55]. Dans l'ordre, les pays qui comptent le plus grand nombre de membres sont le Mexique (13,9 %), la Thaïlande (13,7 %), le Portugal (6,3 %), le Pérou (5,9 %) et les États Unis (5,6 %). Le Canada ne figure pas parmi les 25 pays qui comptent le plus grand nombre de membres.

Par ailleurs, 53 % des utilisateurs sont des hommes, et 43 % sont âgés de 15 à 24 ans. La deuxième tranche d'âge en importance est le groupe des 25 à 34 ans, qui constitue 22 % des utilisateurs[56]. Le pourcentage des utilisateurs américains masculins est supérieur à la moyenne. Parmi ces utilisateurs, 40 % ont un revenu annuel inférieur à 30 000 $ et 57 % n'ont pas de diplôme d'études postsecondaires[57].

Les données recueillies par l'outil Site Analytics montrent qu'en octobre 2008, hi5 a accueilli un peu plus de 2,3 millions de visiteurs uniques américains par jour[58]. La tendance annuelle de 2008 affiche donc une faible baisse par rapport au nombre d'utilisateurs enregistrés en octobre 2007, soit 2,4 millions. Une autre entreprise de statistiques témoigne, quant à elle, d'une baisse générale du nombre quotidien de visiteurs au cours des six derniers mois. Au début de décembre 2008, cette tendance se poursuivait, avec une part d'à peine 2 % de tous les utilisateurs d'Internet par jour[59].

Renseignements relatifs à l'inscription

Pour ouvrir un compte hi5, l'utilisateur doit fournir son prénom et son nom, son adresse de courriel (afin de recevoir une confirmation) ainsi que sa date de naissance.

L'utilisateur est ensuite redirigé vers une page qui lui permet d'accéder à son carnet d'adresses de courriel pour transférer les coordonnées d'amis sur hi5. Toutefois, cette étape peut être sautée. hi5 mentionne qu'il demande toujours à l'utilisateur la permission de conserver son adresse de courriel et son mot de passe ou de communiquer avec ses amis.

Par la suite, l'utilisateur est invité à télécharger une photo dans son profil, à condition qu'il soit autorisé à utiliser cette photo et que cette dernière respecte la politique de hi5 en matière d'image. Cette étape peut également être sautée.

La troisième étape consiste à inscrire le code d'activation envoyé à l'adresse de courriel fournie à hi5.

Une fois l'ouverture du compte confirmée, l'utilisateur est redirigé vers la page « Rechercher des amis ». Il a alors le choix (a) d'autoriser hi5 à repérer ses amis à partir de n'importe quel logiciel de messagerie en ligne ou (b) de rechercher des amis sur hi5 à partir de leur adresse de courriel.

Après avoir ouvert une session, l'utilisateur est invité à ajouter des renseignements à son profil, selon les catégories suivantes : Infos générales, Photo, Contact et Centres d'intérêt.

INFOS GÉNÉRALES : Les informations générales comprennent le prénom, le nom, le sexe, la date de naissance, la ville natale, les intérêts sur hi5, le statut, la religion, les langues, le groupe ethnique et le champ « Moi ». Fait intéressant, à l'exception du prénom, des langues, du groupe ethnique et du champ « Moi », l'utilisateur peut contrôler l'accessibilité à tous ses renseignements grâce aux options suivantes : Tout le monde peut y accéder, Seuls mes amis peuvent y accéder et Personne ne peut y accéder.

PHOTO : L'utilisateur est invité à télécharger une photo sur le site pour l'intégrer à son profil.

CONTACT : Les coordonnées comprennent les adresses de courriel, les noms d'utilisateur de messagerie instantanée, les numéros de téléphone mobile, le pays d'origine, le code postal, l'adresse et l'adresse URL hi5. Ici aussi, l'utilisateur est en mesure de configurer l'accessibilité à certains de ses renseignements, y compris les noms d'utilisateur de messagerie instantanée, les numéros de téléphone mobile et le pays d'origine.

CENTRES D'INTÉRÊT : Cette catégorie est constituée des champs Centres d'intérêt, Musique préférée, Films préférés, Émissions de télé préférées, Livres préférés et Citation préférée.

Identités réelles et pseudonymes

Bien que hi5 vérifie les adresses de courriel, le site n'effectue aucune vérification indépendante du nom complet fourni, pas plus qu'il ne semble déceler les écarts entre le nom et l'adresse de courriel donnés à l'inscription. En ce sens, il n'y a aucune mesure ou vérification prévues dans les ressources technologiques de hi5 pour imposer l'inscription à partir d'un nom ou d'une identité véritables.

Mesures de protection de la vie privée

Outre la possibilité de configurer l'accessibilité aux renseignements d'un profil, hi5 a mis en place un ensemble de mesures de protection de la vie privée pour permettre à l'utilisateur de fixer les normes de confidentialité de son compte, selon les catégories suivantes : le profil, les paramètres des messages et des courriels, les paramètres des photos, les paramètres des mises à jour d'amis, les paramètres du statut en ligne et la gestion des utilisateurs bloqués.

PROFIL : L'utilisateur peut déterminer qui a accès à son profil (tous les utilisateurs ou ses amis seulement), si les autres utilisateurs peuvent ou non savoir qu'il a consulté leur profil, quels utilisateurs peuvent lui envoyer des commentaires sur son profil et si ces commentaires sont autorisés automatiquement ou non (pour tous les utilisateurs, les amis seulement ou personne).

MESSAGES ET ADRESSES COURRIEL : L'utilisateur peut choisir les personnes dont il souhaite recevoir des demandes d'amis, dont il désire recevoir des messages (tous les utilisateurs, les amis seulement ou personne) et dont il souhaite recevoir des « fives » (tous les utilisateurs, les amis seulement ou personne). Il peut aussi indiquer s'il désire ou non recevoir des notifications d'anniversaire, des notifications par courriel et des bulletins d'information.

PARAMÈTRES DES PHOTOS : L'utilisateur peut déterminer si ses amis peuvent ou non marquer ses photos, quels utilisateurs peuvent commenter ses photos et si ces commentaires sont autorisés automatiquement ou non (pour tous les utilisateurs, les amis seulement ou personne).

MISE À JOUR D'AMIS : Comme les mini actualités et les actualités de Facebook, ce paramètre permet à l'utilisateur de déterminer si ses amis peuvent ou non voir les mises à jour de son profil à partir de leur propre compte et quels utilisateurs peuvent voir ces mises à jour sur leur profil (tous les utilisateurs, les amis seulement ou personne).

STATUT EN LIGNE : L'utilisateur peut décider si ses amis verront son statut en ligne.

Marquage de photos

Grâce à l'application Photos, l'utilisateur peut « marquer » des personnes dans une photo en y associant des métadonnées. Si la personne marquée est un autre utilisateur de hi5, elle sera avisée de cette action, recevra un

lien pour voir la photo et pourra exiger que le marquage soit retiré. Le marquage crée également un lien entre la photo et le profil de l'utilisateur de hi5 marqué.

Selon les paramètres de confidentialité réglés par l'utilisateur, seuls ce dernier ou ses amis peuvent marquer ses photos. N'importe qui peut être marqué, y compris les personnes qui ne sont pas membres de hi5. Lorsqu'un non membre est marqué dans une photo, une fenêtre contextuelle invite l'auteur du marquage à inscrire le nom et l'adresse de courriel de la personne marquée pour l'aviser et, éventuellement, l'ajouter à sa liste d'amis. Les personnes qui reçoivent ce courriel peuvent voir la photo, mais n'ont pas accès au reste du site.

Accessibilité aux renseignements des membres

MISES À JOUR : Le profil de l'utilisateur contient des mises à jour sur ses activités. Selon les paramètres de confidentialité, ces mises à jour peuvent être consultées par les visiteurs du profil de l'utilisateur et être affichées sur la page d'accueil de ses amis.

RECHERCHE SUR LE SITE : L'utilisateur peut rendre son profil accessible à tous les utilisateurs (y compris aux non membres de hi5) ou à ses amis uniquement. Bien qu'il soit possible de restreindre l'accès à certains renseignements d'un profil, il semble impossible de retirer complètement le profil des résultats de recherche. Par ailleurs, une fonction de recherche est offerte à l'utilisateur. Ce dernier peut entrer un nom ou une adresse de courriel dans le champ « Rechercher » situé dans le haut de la page d'accueil de hi5, pour ensuite cliquer sur la flèche adjacente (ou appuyer sur la touche « Entrée » de son clavier). L'utilisateur peut préciser sa recherche, notamment en indiquant l'adresse de courriel, le nom, l'âge ou le lieu de résidence de la personne recherchée.

RECHERCHE PUBLIQUE : Les profils hi5 peuvent faire l'objet d'une recherche publique et sont, par défaut, accessibles à tous les utilisateurs du site.

Publicité

La foire aux questions (FAQ) de hi5 indique clairement que pour maintenir la gratuité de son service, hi5 a recours à la publicité[60].

Dans la section commerciale du site qui porte sur la publicité, on affirme que « grâce au ciblage par adresse IP et par caractéristiques démographiques des profils, hi5 transmet les messages publicitaires à un public précis. Le site offre une vaste gamme de produits publicitaires, notamment des bannières à affichage ciblé, un placement média diversifié et des commandites sur mesure[61] » [Traduction].

La politique de protection de la vie privée de hi5[62] énonce clairement que les publicités diffusées proviennent d'entreprises de publicité tierces, et que ces entreprises peuvent avoir accès aux renseignements fournis par l'utilisateur et aux renseignements personnels recueillis par le site. Bien que le nom, l'adresse, l'adresse de courriel et le numéro de téléphone ne soient pas transmis aux annonceurs, d'autres renseignements personnels comme l'âge, le sexe, le lieu de résidence, les statistiques sur les visites du site, l'adresse IP ainsi que l'information sur le fournisseur d'accès à Internet ou l'opérateur de téléphonie mobile peuvent être communiqués afin de faciliter la personnalisation du service.

Soulignons également que cette politique permet à hi5 de dépersonnaliser les renseignements personnels pour ensuite les utiliser à sa discrétion.

Conservation des données

Le site hi5 recueille les renseignements fournis par l'utilisateur de même que ce qu'il qualifie « d'informations personnelles recueillies via les ressources technologiques ».

Parmi les renseignements fournis par l'utilisateur, citons les renseignements relatifs à l'inscription (nom, adresse de courriel, sexe, date de naissance, code postal), le numéro de téléphone, toute autre information inscrite au profil, les informations fournies sur n'importe quel réseau de hi5 (journaux, témoignages, groupes, forums de discussion), ainsi que l'adresse de courriel et le contenu liés à tout courriel envoyé à hi5. Tous ces renseignements servent à offrir « certaines fonctionnalités que la communauté hi5 met à la disposition de ses membres »[63].

Tout en établissant une nette distinction entre les renseignements « personnels » et les renseignements « anonymes », la politique de protection de la vie privée de hi5 contient une clause intéressante selon laquelle le site peut (a) analyser à ses propres fins toute information recueillie et (b) supprimer les renseignements permettant l'identification des informations recueillies afin de les rendre anonymes[64].

La politique de protection de la vie privée contient une section distincte traitant des renseignements personnels recueillis au moyen de ressources technologiques, notamment les adresses IP, le type de navigateur, le système d'exploitation, le numéro de téléphone servant aux communications par SMS, ainsi que la date et l'heure des visites et des actions effectuées au cours des visites (collectées au moyen de témoins et d'adresses URL). Encore une fois, hi5 déclare que ces renseignements sont recueillis « afin de rendre nos services et solutions plus utiles et pour personnaliser votre expérience de la communauté hi5, afin qu'elle réponde à vos intérêts et vos besoins spécifiques »[65].

Toujours dans la section sur les renseignements recueillis au moyen de ressources technologiques, on explique que si l'utilisateur effectue une recherche à l'aide d'une barre d'outils de hi5 ou d'un tiers, le site peut recueillir automatiquement des informations anonymes le concernant, mais aucune information personnelle. Les termes « informations anonymes » et « informations personnelles » sont définis dans la politique de protection de la vie privée.

Fermeture de compte

Selon la politique de protection de la vie privée, l'utilisateur qui souhaite fermer son compte peut cliquer sur un lien prévu à cet effet dans les paramètres du compte. Il sera invité à répondre à un sondage en indiquant son lieu de résidence, les raisons pour lesquelles il ferme son compte, son sexe, les autres services de SRS utilisés et ce que hi5 aurait pu faire pour l'encourager à garder son compte ouvert. Toutefois, il est possible de fermer un compte sans répondre au sondage. La FAQ précise qu'une fois le compte fermé, l'utilisateur ne peut plus accéder à hi5 ni utiliser les fonctions du site.

Notons que la FAQ de hi5 contient de l'information sur la réactivation de compte. On y explique qu'il suffit d'ouvrir une session à l'aide du nom d'utilisateur et du mot de passe du compte fermé. Le site proposera à l'utilisateur de réactiver son compte. Même si une partie ou la totalité des renseignements liés au compte à réactiver peuvent avoir été supprimés, le simple fait d'offrir une fonction de réactivation suggère que la fermeture de compte dans hi5 est en réalité une désactivation et non une suppression.

Applications tierces

En date de septembre 2008, hi5 offrait « au-delà de 2 000 applications tierces totalisant plus de 72 millions d'installations »[66] [Traduction].

Dans ses conditions de service, hi5 précise qu'il ne contrôle pas les applications tierces et que, par conséquent, il n'est pas responsable du contenu de telles applications, il n'offre aucune garantie concernant ce contenu et il n'est pas tenu responsable des conséquences de l'utilisation de ce contenu[67].

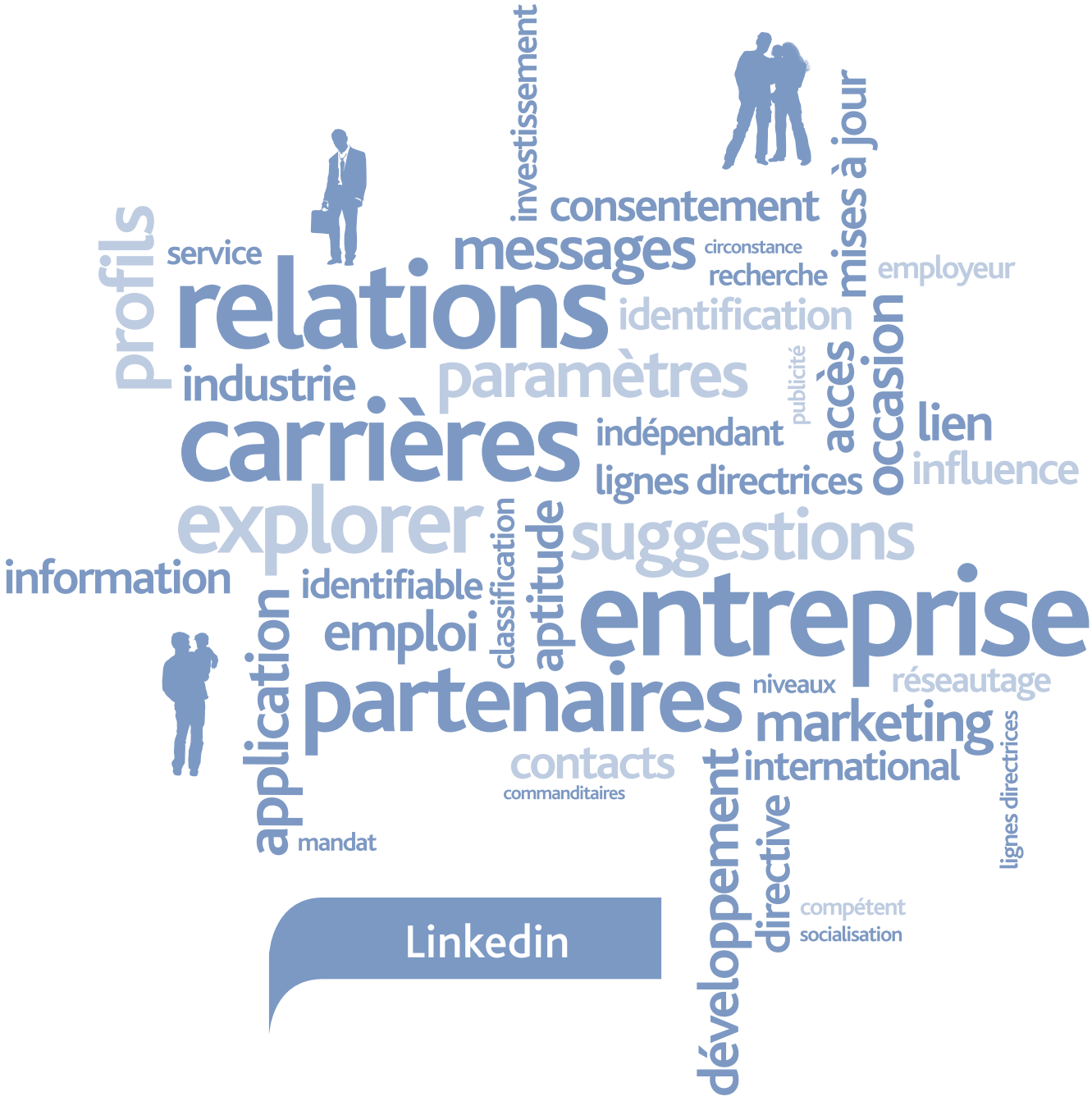
La question des applications tierces est abordée à la fois dans les conditions de service et dans le contrat de licence des développeurs. Les développeurs n'ont pas le droit de recueillir des renseignements sur un utilisateur à d'autres fins que celles de leur application. En outre, ils doivent se conformer à la politique de protection de la vie privée de hi5 et au contrat de licence des développeurs, en plus d'obtenir la permission expresse de l'utilisateur. Par ailleurs, les développeurs doivent conserver les renseignements ainsi recueillis pour une période n'excédant pas 24 heures, mettre en place des mesures et une politique de protection de la vie privée (qui offrent une protection équivalente ou supérieure à celle de hi5) et consentir à éliminer tout renseignement sur un utilisateur lorsque celui-ci supprime leur application[68].

Collecte des renseignements personnels des non membres

Le site hi5 recueille les renseignements personnels des non membres principalement par la recherche d'amis, les invitations à s'inscrire et le marquage de photos. Dans sa politique de protection de la vie privée, hi5 mentionne qu'il conserve ces renseignements pour communiquer avec le non membre afin de l'inviter à visiter le site et à confirmer le lien établi avec un ami (si l'invitation est acceptée), ainsi que pour évaluer le taux de réussite du programme de référence du site. Si un non membre souhaite que ses renseignements soient supprimés de la base de données de hi5, il peut écrire à l'adresse de courriel mentionnée dans la politique de protection de la vie privée[69].

Divers

En novembre 2007, hi5 s'est joint à l'initiative OpenSocial, un ensemble commun d'interfaces API développées par Google pour faciliter le déploiement rapide d'applications de réseau social. Pour sa part, hi5 a lancé le premier outil de traduction OpenSocial pour les développeurs d'applications tierces en septembre 2008[70].


investissement
consentement
mises à jour
profils
service
messages
circonstance
recherche
employeur
relations
identification
occasion
industrie
paramètres
publicité
accès
carrières
indépendant
lien
lignes directrices
influence
explorer
suggestions
classification
aptitude
information
identifiable
entreprise
application
emploi
partenaires
niveaux
réseautage
marketing
contacts
international
commanditaires
lignes directrices
développement
directive
mandat
compétent
socialisation
Linkedin

Linkedin

www.linkedin.com

Mandat

Selon les conditions d'utilisation du site, « LinkedIn [a] pour objet de fournir un service pour faciliter [le] réseautage professionnel entre les Utilisateurs partout dans le monde. Le site est destiné à permettre aux Utilisateurs [de] se connecter uniquement à d'autres Utilisateurs qu'ils connaissent au moment de la connexion et [d']approfondir leurs relations professionnelles avec ces Utilisateurs »[71].

Plutôt que d'axer ses services sur les amis, le site permet à ses utilisateurs d'établir et de mettre à jour une liste de coordonnées de personnes avec qui ils entretiennent une relation professionnelle de confiance. Les personnes dans cette liste sont appelées « relations ». L'utilisateur peut inviter quiconque (membre du site ou non) à devenir une relation. Les relations peuvent ensuite être gérées de la manière suivante :

> « LinkedIn est un outil efficace pour créer des listes exhaustives de relations, puisque le réseau développé par l'utilisateur est constitué de ses propres relations, des relations de ses relations (relations au deuxième degré) et des relations de ses relations au deuxième degré (relations au troisième degré). À partir de ce réseau, l'utilisateur peut s'informer sur des offres d'emploi, des occasions d'affaires ou des personnes, ou encore faire des recherches en ce sens. LinkedIn sert également d'intermédiaire entre employeurs et candidats en diffusant des renseignements professionnels au sujet de ces groupes. Le site suit des lignes directrices strictes en matière de confidentialité. Toutes les relations établies sont confirmées mutuellement et les personnes n'apparaissent sur le réseau de LinkedIn que s'ils y consentent explicitement »[72] [Traduction].

Historique

Le site LinkedIn a été fondé en mai 2003, lorsque les cinq créateurs ont invité 300 de leurs principales relations à s'inscrire. En moins d'un mois, le site comptait 4 500 membres. À la fin de 2003, ce chiffre atteignait 81 000, pour ensuite grimper à plus de 500 000 avant même le premier anniversaire du lancement du site[73].

Information financière

LinkedIn offre des services gratuits, mais aussi des fonctions « premium » additionnelles payantes. Le premier service de ce genre, LinkedIn Carrières, a été lancé en mars 2005.

LinkedIn a été financé par plusieurs partenaires. En octobre 2003, la société Sequoia Fund y a investi 4,7 millions de dollars. En octobre 2004, Greylock Partners y a injecté 10 millions de dollars. En janvier 2007, le montant total des investissements des sociétés Bessemer Venture Partners et European Founders Fund se chiffrait à 12,8 millions de dollars. En juin 2008, la société Bain Capital Ventures a investi 53 millions de dollars. Plus récemment, en octobre 2008, les sociétés Goldman Sachs, Bessemer Venture Partners, The McGraw-Hill Companies et SAP Ventures ont ajouté 22 millions de dollars aux montants déjà investis dans LinkedIn[74].

Les revenus prévus de LinkedIn pour 2008 sont de 75 à 100 millions de dollars.

Profil démographique des utilisateurs

Dès sa création, LinkedIn a établi sa présence sur la scène internationale. Actuellement, la majorité de ses utilisateurs sont aux États-Unis (48,8 %), en Inde (11,3 %), au Royaume Uni (5,1 %), en Allemagne (3,6 %) et en Chine (3,5 %). Le Canada occupe le huitième rang avec 2,4 % des utilisateurs[75].

Une entreprise de statistiques rapporte qu'aux États Unis seulement, plus de 8,2 millions de visiteurs se sont rendus sur le site pendant le mois d'octobre 2008[76]. Ce chiffre marque une croissance stable depuis octobre 2007, mois au cours duquel le site avait accueilli un peu moins de 3 millions de visiteurs uniques.

Au cours de l'été 2008, TechCrunch a publié une série de diapositives comparant les utilisateurs de LinkedIn à ceux d'autres sites de réseautage professionnel. Selon ces renseignements, la moyenne d'âge des utilisateurs est de 41 ans, et 53,5 % des utilisateurs ont un revenu de

ménage de plus de 100 000 $, la moyenne étant de 109 703 $. Les statistiques montrent que 64 % des utilisateurs sont des hommes, que 34 % d'entre eux possèdent un téléphone intelligent ou un ANP et qu'ils sont 80,1 % à détenir au moins un diplôme d'études postsecondaires, dont 37 %, un diplôme d'études supérieures[77].

Renseignements relatifs à l'inscription

Pour s'inscrire, l'utilisateur doit fournir les renseignements suivants : prénom, nom, adresse de courriel, mot de passe, pays, code postal (un avis précise que seule la région sera visible), emploi, industrie, formation, province, établissement d'enseignement et années de fréquentation. Par la suite, l'utilisateur est redirigé vers une page où il peut configurer son utilisation de LinkedIn. Il peut ainsi définir différents critères de recherche de renseignements et indiquer les raisons pour lesquelles il désire recevoir des communications à partir du réseau. L'utilisateur peut ensuite enregistrer ses choix.

Après l'enregistrement, l'utilisateur est invité à confirmer l'ouverture de son compte LinkedIn par courriel. Une fois l'ouverture confirmée, l'utilisateur doit ouvrir une session. Il accède alors à une page où il peut inscrire les adresses de courriel qui serviront à rechercher des relations déjà membres de LinkedIn.

Après avoir parcouru ces étapes, l'utilisateur apprend que 15 % de son profil a été rempli et qu'il peut y ajouter ou y modifier des renseignements[78]. L'utilisateur qui choisit de modifier son profil est redirigé vers une page où d'autres renseignements lui sont demandés, notamment son poste actuel, ses emplois précédents, sa formation, des recommandations obtenues d'autres utilisateurs de LinkedIn, ses préférences de communication et l'adresse URL de son site Web. Il y a également des catégories de renseignements à réponse libre, comme le curriculum vitae, les prix et distinctions, les compétences professionnelles et les spécialités. Par ailleurs, on suggère à l'utilisateur d'enrichir son profil en ajoutant des applications de partenaires de LinkedIn, dont certaines apparaissent à l'écran. Enfin, l'utilisateur peut préciser le type de messages qu'il autorise (Introductions et InMails, ou Introductions seulement), déterminer les occasions qui l'intéressent et, dans une zone prévue à cette fin, offrir des conseils aux autres utilisateurs qui souhaitent communiquer avec lui. LinkedIn suggère d'inclure dans cette zone les disponibilités ainsi que le type de projets ou d'occasions recherchés.

Identités réelles et pseudonymes

Dans les conditions d'utilisation de LinkedIn, on stipule que le site n'est pas dans l'obligation de vérifier l'identité des utilisateurs (d'ailleurs, il ne le fait pas). En effet, au moment de l'inscription, seule l'adresse de courriel est validée; aucun autre renseignement n'est vérifié, du moins en apparence. Toutefois, à la section « À faire et à ne pas faire » des conditions d'utilisation, l'utilisateur est tenu de fournir des informations exactes.

Par ailleurs, les préférences du profil permettent à l'utilisateur de choisir s'il veut afficher son nom au complet ou seulement son prénom et la première lettre de son nom de famille.

Mesures de protection de la vie privée

Dans la section « À propos de LinkedIn » du site de l'entreprise, on affirme que « LinkedIn a adopté les recommandations du Safe Harbor Privacy Framework, mis en place par la Communauté Européenne et le Département du Commerce des États Unis, pour harmoniser leur législation respective en matière de protection des informations personnelles. La politique de confidentialité et les conditions d'utilisation de LinkedIn respectent la législation européenne et ont été certifiées. Toutes les mises en relation entre personnes sur LinkedIn sont volontaires et doivent être mutuellement acceptées. Personne ne peut apparaître sur le réseau LinkedIn sans en avoir été informé et sans y avoir explicitement consenti »[79] De plus, LinkedIn est titulaire d'une licence en vertu du programme de l'organisme TRUSTe.

Les mesures de protection de la vie privée de LinkedIn se trouvent dans l'onglet « Compte et Préférences ».

Les préférences de confidentialité sont divisées en huit catégories : Publicité d'un partenaire; Enquêtes; Consultation de la liste de vos relations; Consultation des profils; Voir les photos des profils; Actualisation de votre profil et de votre statut; Annuaire des prestataires de services; et Applications autorisées.

PUBLICITÉ D'UN PARTENAIRE : L'utilisateur peut permettre ou non la personnalisation, l'enrichissement ou le ciblage de publicités sur le site NYTImes.com et sur d'autres sites de LinkedIn.

ENQUÊTES : L'utilisateur indique s'il souhaite ou non être sollicité pour participer à des études de marché en ligne portant sur son secteur d'activité.

CONSULTATION DE LA LISTE DE VOS RELATIONS : L'utilisateur peut interdire ou non à chacune de ses relations de voir la liste de ses autres relations (toutefois, il ne peut cacher une relation commune).

CONSULTATION DES PROFILS : L'utilisateur peut déterminer les renseignements qui sont transmis aux utilisateurs dont il consulte le profil. Il a le choix de diffuser le nom et le titre de son profil uniquement ou des informations anonymes telles que son secteur et sa fonction. Il peut également décider de ne diffuser aucun renseignement.

VOIR LES PHOTOS DES PROFILS : Plutôt que de gérer l'affichage de sa propre photo de profil, l'utilisateur peut déterminer les photos auxquelles il aura accès (aucune photo, celle de ses relations, celle des membres de son réseau ou celle de tous les utilisateurs).

ACTUALISATION DE VOTRE PROFIL ET DE VOTRE STATUT : L'utilisateur doit d'abord indiquer s'il souhaite ou non publier les mises à jour de son profil et ses recommandations. Ensuite, il doit déterminer s'il souhaite ou non informer ses relations de telles mises à jour (s'il refuse, ses renseignements ne figureront pas dans les nouvelles de son entreprise ou de son secteur sur le réseau).

ANNUAIRE DES PRESTATAIRES DE SERVICES : Si l'utilisateur est recommandé en tant que prestataire de services, il peut choisir de figurer dans l'annuaire des prestataires de services.

APPLICATIONS AUTORISÉES : Cette liste comprend les applications que l'utilisateur a téléchargées et installées dans son profil.

En plus des préférences de confidentialité comprises dans les paramètres du profil, certaines préférences liées au profil et aux renseignements personnels ont également des répercussions sur la protection de la vie privée, y compris la possibilité de configurer l'accessibilité à la photo et aux renseignements personnels d'un membre.

Marquage de photos

Les utilisateurs, de même que les groupes, peuvent télécharger une photo dans leur profil. Toutefois, contrairement à d'autres SRS, LinkedIn ne prend pas en charge le téléchargement de plusieurs photos, la création d'albums photos et l'ajout de métadonnées à des photos par le marquage. Les conditions d'utilisation stipulent que les photos doivent être à caractère professionnel.

Accessibilité aux renseignements des membres

NOUVELLES : Si l'utilisateur le permet dans ses préférences de confidentialité, ses recommandations ainsi que les mises à jour de son profil et de son statut seront affichées dans son profil et seront accessibles à ses relations.

RECHERCHE SUR LE SITE : Il existe de nombreuses façons d'effectuer une recherche sur LinkedIn. L'utilisateur peut ajouter des relations à partir de leur carnet d'adresses de courriel. Les relations qui sont déjà membres de LinkedIn auront une icône « In » à côté de leur nom. Les relations qui ne sont pas membres peuvent être invitées à s'inscrire. L'utilisateur peut également rechercher des relations à partir de réseaux ou de groupes existants. Dans l'onglet « Ajouter des personnes », l'utilisateur peut sélectionner « Collègues » ou « Anciens élèves », pour ensuite voir ceux qui sont membres de LinkedIn et choisir lesquels il souhaite inviter à joindre ses relations. Enfin, soulignons que LinkedIn permet à ses membres de rechercher un emploi par mots clés et, par conséquent, de voir le contenu d'autres profils.

RECHERCHE PUBLIQUE : Par défaut, les profils LinkedIn peuvent faire l'objet d'une recherche publique. Cependant, dans les paramètres de son compte, l'utilisateur peut choisir s'il souhaite ou non que son profil soit accessible à partir d'une recherche publique sur le Web. Le cas échéant, il peut décider des renseignements à afficher dans les résultats de recherche : Informations de base (nom, industrie, lieu, nombre de recommandations); Photo; Titre du profil; Résumé professionnel; Compétences; Postes actuels (détaillés ou non); Postes précédents (détaillés ou non); Sites Web; Centres d'intérêts; Groupes; Distinctions et prix; et Intéressé(e) par.

Publicité

Certes, la politique de confidentialité de LinkedIn mentionne que le site ne procède ni à la vente, ni à la location, ni à la diffusion des renseignements personnels relatifs à l'identité de ses membres à des tiers à des fins commerciales, mais cela ne signifie pas que ces renseignements ne sont pas utilisés à des fins publicitaires. En fait, la politique explique que des données anonymes agrégées sur l'utilisation des services de LinkedIn sont recueillies et peuvent être transmises à des tiers à différentes fins, dont la publicité. Les utilisateurs peuvent être sélectionnés par poste de travail, industrie, situation géographique ou entreprise. Toutefois, précisons que la politique contient aussi une adresse de courriel à laquelle les membres peuvent écrire pour demander que leurs renseignements soient exclus des recherches agrégées ou des produits découlant de données agrégées sur les activités des utilisateurs sur le site.

À l'été 2008, LinkedIn a lancé une forme de publicité commanditée appelée DirectAds. DirectAds permet à l'utilisateur de créer des publicités qui sont ensuite ciblées selon l'âge, le sexe, l'industrie ou l'ancienneté des membres à qui elles sont destinées. Par la suite, ces publicités sont affichées dans la page d'accueil et le profil des utilisateurs visés. À ce jour, DirectAds n'est offert qu'aux États-Unis[80].

Pour la publicité à plus grande échelle, LinkedIn propose trois moyens différents de cibler les utilisateurs : envoyer les publicités à tous les professionnels, toutes industries et professions confondues; envoyer les publicités à certaines catégories de professionnels dans LinkedIn, notamment les professionnels des TI, les entrepreneurs ou les spécialistes du marché financier; ou envoyer les publicités à un public personnalisé, selon l'industrie, l'ancienneté, le poste, la taille de l'entreprise, la situation géographique, le nombre de relations ou le sexe[81].

Enfin, la politique de confidentialité indique également que LinkedIn peut insérer des balises Web (« Web beacons ») dans les réseaux de publicité, à même les pages du site, afin que ces réseaux puissent effectuer des vérifications, des recherches et des rapports anonymes et agrégés pour des annonceurs, et envoyer des annonces publicitaires à des utilisateurs pendant qu'ils visitent d'autres sites Web. On indique également la marche à suivre pour se soustraire à l'utilisation des balises Web.

Conservation des données

La politique de confidentialité de LinkedIn décrit différentes catégories de renseignements recueillis.

D'abord, LinkedIn recueille les renseignements personnels fournis par l'utilisateur au moment de son inscription, notamment son nom, son adresse de courriel, son pays de résidence, son code postal, sa profession et son mot de passe.

LinkedIn établit une distinction claire entre les renseignements obligatoires pour l'inscription et les renseignements facultatifs, soit ceux qui sont ajoutés au profil. La politique précise néanmoins que ces renseignements permettent d'optimiser le fonctionnement du site. LinkedIn affirme également qu'il recueille des renseignements à partir du site Web principal et du site Service Clientèle afin de répertorier les besoins des membres, d'y répondre et de proposer « les niveaux appropriés de service »[82].

Enfin, LinkedIn recueille des renseignements liés à la technologie, y compris les fichiers de blogues, les témoins permanents et les témoins temporaires. De plus, LinkedIn peut recueillir les fichiers IP ainsi que des renseignements sur le navigateur et le système d'exploitation de ses utilisateurs. En soi, les adresses IP ne sont pas considérées comme des renseignements personnels permettant l'identification, et, parallèlement, LinkedIn promet de ne jamais transmettre à des tiers le lien entre une adresse IP et les renseignements personnels d'un utilisateur sans le consentement de ce dernier, à moins d'y être contraint par la loi[83].

Fermeture de compte

LinkedIn affirme que la fermeture d'un compte entraîne la suppression du profil de l'utilisateur. Une fois son compte fermé, l'utilisateur ne peut plus accéder aux renseignements enregistrés concernant son compte ou ses relations, et le profil ne peut plus faire l'objet d'une recherche sur le site ni sur le Web. Toutefois, la politique de confidentialité précise qu'après la fermeture, certaines données peuvent être conservées pour lutter contre la fraude ou l'utilisation abusive, ainsi que pour des raisons commerciales comme l'analyse de données anonymes agrégées ou le rétablissement du compte.

Lorsqu'un utilisateur souhaite non seulement fermer son compte, mais aussi supprimer tous ses renseignements de LinkedIn, il doit écrire à l'adresse de courriel fournie dans la politique de confidentialité. LinkedIn promet de répondre à la demande dans un délai de trois jours ouvrables[84].

Applications tierces

LinkedIn offre des applications tierces, en plus d'établir des ententes de partenariat avec des tiers.

APPLICATIONS : Les applications sont conçues par des développeurs. En cliquant sur l'onglet Applications, l'utilisateur accède à la page « Applications proposées », où il peut aussi rechercher d'autres applications. L'utilisateur peut ajouter jusqu'à 15 applications dans son profil et 12 applications dans sa page d'accueil. L'ajout d'une application permet au développeur d'accéder aux renseignements sur le profil et les relations de l'utilisateur. Les conditions d'utilisation stipulent qu'avant d'utiliser une application nouvellement installée, l'utilisateur doit accepter les conditions d'utilisation et la politique de protection de la vie privée du développeur.

PARTENAIRES : Les partenaires sont une sous-catégorie de développeurs avec lesquels LinkedIn entretient une relation privilégiée. LinkedIn déclare collaborer uniquement avec des partenaires de confiance. Par conséquent, toute application désignée comme le produit d'un partenaire « de confiance » peut avoir automatiquement accès aux renseignements sur les comptes à des fins de prestation de services.

La politique de confidentialité est parfaitement claire à ce sujet :

> « Les Développeurs Tiers doivent donner leur accord sur les limites imposées en matière d'accès, [de] stockage et [d']usage de vos données. Cependant, bien que nous concluions des accords contractuels et prenions des mesures techniques pour limiter toute utilisation abusive de ces données par ces Développeurs Tiers, il est possible que nous n'ayons pas contrôlé ni approuvée [sic] des Développeurs Tiers, et nous ne sommes pas en mesure de garantir que tout Développeur Tiers respectera ces contraintes et accords. Certaines de vos actions via [sic] les Applications de la Plateforme seront affichées pendant vos connexions. Vous devez savoir que votre utilisation de toute Application de la Plateforme s'effectue "en l'état", sans aucune garantie quant aux actions des Développeurs Tiers. »

Collecte des renseignements personnels des non-membres

Il arrive que les renseignements personnels d'un non membre soient transmis à LinkedIn lorsqu'un utilisateur invite cette personne à s'inscrire ou l'ajoute à sa liste de relations. Ces renseignements sont conservés par LinkedIn uniquement pour envoyer des invitations et des rappels.

On ignore cependant comment les non membres peuvent demander que leurs renseignements personnels soient retirés de la base de données de LinkedIn.

Divers

Dans sa politique de confidentialité, LinkedIn affirme que les renseignements autres que ceux expressément demandés à l'inscription doivent être considérés comme « sensibles », mais que la fourniture de tels renseignements sous entend le consentement explicite à leur emploi aux fins mentionnées dans les conditions d'utilisation. À ce sujet, le site indique que l'utilisateur peut annuler son consentement, mais que cette action n'a pas d'effet rétroactif.

Par ailleurs, la politique de confidentialité de LinkedIn précise que le site peut divulguer des renseignements à un tiers dans le cadre d'une réorganisation ou d'une cession d'actifs, et que le tiers aura le droit de continuer à utiliser ces renseignements. Curieusement, rien n'indique

que le tiers serait par le fait même assujetti aux conditions d'utilisation. Ainsi, une fois les actifs cédés, le consentement à l'utilisation des renseignements serait encore valable, alors que l'obligation de protéger ces renseignements tomberait.


censure
fondé
efficace
entretenir
actuel
promotions
photobucket
plateforme de publication
social
facile
personnel
région
magasinage
contrôlé
publicité
art
sophistiqué
convivial
statistiques
éducatif
identité
recherches
site
administrable
expressif
affichable
développer
applications
scrapbook
gratuit
virtuel
interaction
intérêts
personnaliser
développer
langue
réseautage
témoins
base de données
public
marketing
étudiants
vie privée
continu
accessible
LiveJournal

LiveJournal

www.livejournal.com

Mandat

Dans le profil de l'entreprise, LiveJournal est présenté comme une plateforme de publication communautaire, un mélange entre un blogue et un SRS[85]. À cette fin, l'utilisateur dispose de trois plateformes : une première pour créer, personnaliser et, éventuellement, diffuser un journal Web; une deuxième pour dresser et mettre à jour une liste d'amis afin d'inclure dans son propre journal le contenu du journal d'amis et un contenu sélectionné en format RSS; et une troisième permettant d'afficher son profil, notamment ses coordonnées, son autobiographie, ses centres d'intérêt, ses amis, les communautés dont il fait partie, les établissements scolaires qu'il a fréquentés et des images (téléchargées à partir de sources externes).

En tant que projet Open Source, le site LiveJournal fonctionne grâce à des logiciels serveurs libres. La plupart des applications utilisent également un code source libre[86].

Historique

Le site LiveJournal a été lancé par Brad Fitzpatrick en avril 1999.

En 2005, la société Six Apart a acheté la société mère de LiveJournal, Danga Interactive. Le fondateur de cette dernière, Brad Fitzpatrick, a continué de participer au projet à titre de membre du personnel de Six Apart jusqu'en 2007.

En décembre 2007, l'entreprise pointcom russe SUP a acheté LiveJournal et a fondé la société LiveJournal Inc. pour exploiter le site. Même si les conditions de service précisent que le site est toujours régi par les lois de la Californie, où se trouve le siège social de LiveJournal Inc. (qui compte un bureau satellite à Moscou), le fait que LiveJournal appartienne à une entreprise russe a suscité des inquiétudes au sujet de la confidentialité des renseignements personnels et de la possibilité pour le gouvernement russe de consulter ou de censurer ces informations[87].

En Russie, LiveJournal occupe actuellement la majeure partie de la blogosphère, puisqu'il héberge plus de 80 des 100 blogues russes les plus populaires[88].

Information financière

LiveJournal offre six types de comptes; l'affichage des publicités, les fonctions offertes et l'accès aux services varient en fonction du type choisi.

COMPTE DE BASE : Le compte de base est gratuit pour tous, mais propose un nombre limité de fonctions. Avant le 12 mars 2008, ce type de compte était offert sans publicité. En août 2008, le nouveau processus de création de comptes de base intégrait l'affichage de publicités.

COMPTE PRÉCURSEUR : Depuis septembre 2000, ce type de compte n'est plus offert aux nouveaux membres. Ces derniers profitaient de fonctions avancées qui n'étaient pas offertes dans le compte de base, mais n'avaient pas accès aux fonctions du compte payant.

COMPTE PLUS : Le compte Plus offre les services de base, auxquels s'ajoutent des fonctions avancées et un espace de stockage accru. Ce type de compte est gratuit, mais est financé par la publicité que voient les utilisateurs de LiveJournal et les personnes qui consultent le profil de ces utilisateurs.

COMPTE PAYANT : Le compte payant est assorti de conditions précises et offre une foule de fonctions avancées. Ce type de compte n'est pas transférable ni remboursable.

COMPTE PERMANENT : Ce type de compte n'est pas offert aux nouveaux utilisateurs. En fait, le compte permanent permet d'accéder gratuitement à toutes les fonctions du compte payant. Il est généralement réservé aux fondateurs ou aux administrateurs de LiveJournal, ou à quiconque ayant participé au développement du site.

COMPTE COMMANDITÉ : Le compte commandité donne un accès gratuit aux services, y compris à la plupart des fonctions du compte payant. Les coûts liés à ce type de compte sont financés par des commanditaires. Par ailleurs, le site comprend une boutique de cadeaux virtuels que l'on peut offrir à ses amis sur LiveJournal à partir de 0,99 $US l'unité. De plus, l'utilisateur peut acheter des extensions, comme des icônes ou de l'espace de stockage supplémentaires.

Profil démographique des utilisateurs

La société Alexa a déterminé le pourcentage d'utilisateurs de LiveJournal par pays. Les cinq pays comptant le plus grand nombre d'utilisateurs sont la Russie (29,5 %), les États Unis (24,7 %), l'Ukraine (3,5 %), Singapour (3,4 %) et le Royaume Uni (2,9 %). Le Canada se classe au 11e rang avec 2,1 % du nombre total d'utilisateurs[89].

Tout comme Facebook, LiveJournal a sa propre page de statistiques, dont certaines sont mises à jour quotidiennement. Le site héberge plus de 17 millions de comptes, dont un peu moins de 2 millions sont toujours actifs. L'âge moyen des utilisateurs est de 20 ans, la majorité ayant de 18 à 24 ans[90].

En ce qui a trait au trafic, une entreprise de statistiques rapporte qu'aux États Unis, 4,5 millions de visiteurs se sont rendus sur le site en octobre 2008. De plus, la majorité des utilisateurs font partie du groupe d'âge des 18 à 34 ans. Enfin, ces statistiques montrent un pourcentage à peu près égal d'utilisateurs détenant un diplôme d'études postsecondaires et d'utilisateurs non diplômés[91].

Renseignements relatifs à l'inscription

Étonnamment, la personne qui veut ouvrir un compte LiveJournal n'est pas tenue de fournir son prénom ni son nom de famille. Elle doit plutôt entrer son nom d'utilisateur (pseudonyme ou autre) ainsi que son adresse de courriel, son mot de passe (un encadré indique que le mot de passe doit contenir des chiffres et des lettres) et sa date de naissance (un encadré indique que cette date est requise par la loi, mais que seuls le jour et le mois sont affichés par défaut). Elle doit aussi taper correctement le code captcha.

Après avoir fourni ces renseignements, accepté les conditions de service et la politique sur la protection de la vie privée, puis indiqué s'il veut recevoir ou non des annonces de LiveJournal, l'utilisateur est redirigé vers la page « Configuration rapide ». Cette page lui permet de choisir un thème (apparence et mise en page) pour son journal et de fournir d'autres renseignements personnels. On indique clairement que tous les champs à remplir sont facultatifs. On demande le nom (le pseudonyme fourni à l'inscription est inscrit par défaut), le sexe (avec l'option de ne pas le préciser) et le lieu de résidence (pays, État ou province, ville). On prévoit également une zone pour indiquer les centres d'intérêt : musique, films, émissions de télévision, livres, passe temps et autres. Enfin, une zone permet à l'utilisateur de fournir une biographie ou d'autres renseignements.

Après avoir choisi d'ajouter ou non des informations à son profil, l'utilisateur peut sélectionner un compte de base ou un compte payant. Une fois son compte LiveJournal configuré, l'utilisateur n'a plus qu'à l'activer par courriel. Il est ensuite redirigé vers une page de LiveJournal qui l'informe des différentes fonctions, comme les profils, les listes d'amis, les journaux et les communautés.

L'utilisateur peut télécharger des icônes sur le site pour les intégrer à une entrée de journal. Il peut s'agir de photos sur lesquelles apparaît l'utilisateur ou de toute autre image jugée acceptable. LiveJournal offre à l'utilisateur une foule d'icônes à rechercher, à télécharger et à utiliser.

Identités réelles et pseudonymes

LiveJournal n'oblige pas l'utilisateur à révéler son identité réelle. Ce dernier peut s'inscrire en entrant le nom de son choix (pseudonyme ou autre). Toutefois, les adresses de courriel fournies lors de l'inscription sont validées.

Fait intéressant, les conditions de service de LiveJournal stipulent qu'au moment de l'inscription, l'utilisateur doit « fournir des renseignements personnels exacts, complets et à jour dans tous les champs à remplir » [Traduction].

Mesures de protection de la vie privée

Comparativement à d'autres sites de réseau social ou de blogage, LiveJournal offre une vaste gamme de mesures de protection de la vie privée (p. ex. filtres, groupes personnalisés, communautés et entrées de journal pour amis seulement). D'une part, un niveau de sécurité minimal peut être associé à l'ensemble du journal. D'autre part, des paramètres de confidentialité peuvent être réglés pour chaque entrée de journal, ce qui permet à l'utilisateur de désigner une entrée comme étant publique (accessible à tous les utilisateurs), pour amis seulement (accessible uniquement aux utilisateurs sur sa liste d'amis), privée (accessible à lui-même seulement) ou personnalisée (accessible à un groupe d'utilisateurs choisis)[92].

À l'aide des outils de gestion de profil, l'utilisateur peut aussi décider de ne pas rendre les renseignements de son profil visibles.

Marquage de photos

L'utilisateur peut ajouter des images à ses entrées de journal au moyen du langage HTML, du site Photobucket (un site tiers sur lequel l'utilisateur doit ouvrir un compte pour télécharger des photos dans LiveJournal) ou de l'utilitaire ScrapBook de LiveJournal. Pour ajouter des images à un commentaire ou à un profil, il faut utiliser le langage HTML.

L'utilisateur peut configurer certains paramètres de sécurité de l'utilitaire ScrapBook en choisissant de rendre son profil visible pour le public (tout le monde), les utilisateurs inscrits (utilisateurs qui ont ouvert une session LiveJournal) ou tous les groupes (membres de sa liste d'amis), ou en désignant son profil comme privé (accessible à lui-même uniquement). L'utilisateur peut également appliquer des niveaux de sécurité à chaque album et, par le fait même, à toutes les photos de l'album.

Pour des raisons de sécurité, LiveJournal ne permet pas l'utilisation de langages de script pour intégrer des objets dans le site. Il est donc interdit de marquer des photos à l'aide de métadonnées. L'utilisateur peut insérer manuellement un lien dans le corps d'une entrée de journal, mais ce lien ne mènera pas directement à la photo.

Accessibilité aux renseignements des membres

ACTUALITÉS : Contrairement aux autres sites examinés, LiveJournal n'affiche pas d'actualités liées aux profils. Toutefois, à partir de sa liste d'amis, l'utilisateur reçoit des entrées publiées par ses amis, ses communautés et les fils RSS auxquels il est abonné.

RECHERCHE SUR LE SITE : LiveJournal offre différentes méthodes de recherche. L'utilisateur peut rechercher d'autres membres à partir du nom (pseudonyme ou autre), de l'adresse de courriel ou de l'identifiant de messagerie instantanée, dans la mesure où ces renseignements sont accessibles au public. De plus, l'utilisateur peut effectuer une recherche en fonction de la communauté, du centre d'intérêt, des dernières entrées de journal ou de l'école, à partir des pages des amis de ses amis, de façon aléatoire, ou encore au moyen de la fonction « Explorer LJ ». Les titulaires de comptes avec fonctions avancées ont accès à d'autres modes de recherche, y compris par répertoire et par région.

RECHERCHE PUBLIQUE : Il est impossible de configurer un profil sur LiveJournal sans qu'il ne soit visible. Cependant, l'utilisateur peut modifier les paramètres de sécurité pour s'assurer que ses entrées ne sont pas accessibles au public. Il peut aussi modifier son profil en y indiquant les renseignements dont il autorise l'affichage. De plus, la page « Options d'affichage » de LiveJournal permet de réduire la quantité de renseignements qui sont indexés par les moteurs de recherche publique.

Publicité

LiveJournal a recours à la publicité afin de pouvoir offrir certaines catégories de comptes gratuitement. L'affichage des publicités dépend du type de compte.

Compte de base et compte précurseur : L'utilisateur voit des publicités lorsqu'il consulte le journal, la page d'amis ou le profil d'un titulaire de compte Plus.

Compte Plus : Des publicités sont affichées dans le journal de l'utilisateur et dans la plupart des pages de LiveJournal.

Compte payant et compte permanent : Après avoir ouvert une session, l'utilisateur ne voit aucune publicité, même s'il consulte le journal d'un titulaire de compte Plus.

Utilisateur déconnecté : L'utilisateur voit des publicités lorsqu'il consulte le journal d'un titulaire de compte de base ou de compte Plus, ou les pages de LiveJournal[93].

Fait intéressant, l'utilisateur de LiveJournal a la possibilité de régler les paramètres de publicité. Pour ce faire, il doit indiquer son type de compte, son sexe, son année de naissance et son lieu de résidence (ville, État ou province, code postal, pays), puis choisir au moins cinq catégories de publicités qui l'intéressent (p. ex. arts et sciences humaines, appareils électroniques personnels, nouvelles, magasinage, et animaux de compagnie). LiveJournal promet de ne pas transmettre les renseignements personnels de l'utilisateur à des tiers.

La publicité diffusée par LiveJournal est ciblée selon les catégories préférées de l'utilisateur, le sexe, l'âge, le lieu de résidence, les centres d'intérêt ou une petite partie du contenu public. Le ciblage tient compte non seulement de l'utilisateur, mais aussi du profil des gens qui verront les publicités et des préférences de LiveJournal par rapport à la publicité. Le ciblage peut être effectué par regroupement de données, mais la politique sur la vie privée précise que ces données agrégées demeurent anonymes.

Voici un élément de la réponse à la question 267 de la FAQ de LiveJournal, qui rejoint ce qui est énoncé dans la politique sur la vie privée :

> « LiveJournal respecte toujours sa politique sur la protection de la vie privée. Votre adresse de courriel, vos renseignements personnels permettant l'identification et vos entrées protégées ne sont jamais transmis aux annonceurs ni aux partenaires. LiveJournal et ses annonceurs peuvent utiliser des témoins pour affiner le ciblage publicitaire des utilisateurs. Toutefois, ces témoins ne recueillent aucun renseignement personnel, qu'ils proviennent de LiveJournal ou de ses partenaires. » [Traduction]

Selon les conditions de service, le titulaire d'un compte autorisant les publicités doit consentir à ne pas gêner l'accès à ces publicités. La politique sur la vie privée de LiveJournal contient une clause intéressante dans laquelle sont énumérés les réseaux de publicité et les tiers avec qui LiveJournal entretient des liens, y compris leur adresse URL. De cette façon, l'utilisateur peut gérer l'utilisation de témoins par les annonceurs.

Conservation des données

La politique sur la vie privée de LiveJournal est rédigée dans un langage clair et cohérent. Selon les principes de la politique, LiveJournal recueille les renseignements suivants :

- les renseignements relatifs à l'inscription, à l'utilisation des produits et services de LiveJournal et au contenu publié;
- les renseignements personnels fournis dans le cadre de promotions ou de concours sur le site LiveJournal;
- les renseignements agrégés dépersonnalisés;
- les renseignements au sujet des transactions, tels que les données de cartes de crédit;
- les renseignements liés à la technologie, tels que les adresses IP, les témoins, les pages recherchées et les journaux de serveur.

Ces renseignements sont utilisés à l'interne seulement et ne sont pas vendus.

Fermeture de compte

Lorsque l'utilisateur décide de fermer son compte, il est avisé que ses renseignements seront conservés pour une période de 30 jours, puis

supprimés de façon permanente. De plus, un sondage est proposé à l'utilisateur pour déterminer les raisons pour lesquelles il a choisi de fermer son compte LiveJournal.

Applications tierces

Les applications tierces ne sont pas mentionnées dans les conditions de service ni dans la politique sur la vie privée.

Collecte des renseignements personnels des non membres

Le contenu publié par un non membre à titre d'invité est recueilli par LiveJournal. Parallèlement, tout renseignement sur un non-membre qui est fourni dans le journal d'un utilisateur peut être recueilli dans le cadre du processus de collecte et de conservation des données de LiveJournal. Ni les conditions de service ni la politique sur la protection de la vie privée ne contiennent de clauses sur la suppression de tels renseignements du site.

Divers

Soulignons que, contrairement aux autres SRS, LiveJournal permet aux détenteurs ou aux administrateurs de journaux de voir les adresses IP rattachées aux commentaires, si cette fonction particulière a été activée.


MySpace
public
jeunesse
musique
commentaires personnels
scolarité
photos
profils
settings
concours
accès
musicians
groupes
expression de soi
personnel
unique
réseautage
messages privés
applications
alias
personnalisé
avis
revenu
intérêts
ciblé
loisirs
personnel
échange
bulletins
publicité
personnalité
groupes
style de vie
surveillé
petites annonces
sondages
tiers
amis
interaction
accessible
blogage
messagerie
repérage
usage
fourni par l'utilisateur
actualités à jour
visiteurs
internet
enquêtes

MySpace

www.myspace.com

Mandat

Le slogan de l'entreprise est « a place for friends » (un endroit pour les amis).

MySpace est également décrit comme « un site qui vise particulièrement les jeunes en leur permettant de s'identifier à des marques et à des groupes et de s'exprimer »[94] [Traduction]. Les utilisateurs du site peuvent consulter le profil d'autres utilisateurs, bloguer, échanger des courriels et se joindre à des groupes. MySpace offre également du contenu musical et vidéo ainsi que des annonces classées. Les artistes peuvent établir leur présence sur le site, ajouter des amis, transmettre de la musique en continu et même en vendre[95].

MySpace est conçu pour que l'utilisateur puisse personnaliser la mise en page et les couleurs de son profil, pratiquement sans aucune restriction, tant que les publicités ne sont pas couvertes ni obscurcies. Cette condition peut engendrer certains problèmes, comme la surcharge de pages dans le navigateur par un utilisateur sans expérience, ou certains risques de sécurité liés à l'ajout de code dans les pages.

Historique

MySpace a été fondé en 2003 en tant que site de réseau social au sein de la « communauté virtuelle », un groupe de sites Web. En janvier 2004, il a été lancé comme site autonome[96].

MySpace a été acheté par NewsCorp le 19 juillet 2005 et fait maintenant partie de la division Fox Interactive Media.

Actuellement, le site héberge 200 millions de comptes et accueille 110 millions d'utilisateurs actifs chaque mois.

Information financière

MySpace est un site gratuit financé par la publicité. Cependant, il pourrait éventuellement offrir des services de qualité payants[97].

En ce qui concerne les revenus, le PDG de MySpace affirme ceci : « Notre stratégie internationale est différente de celle de nos compétiteurs. Nous misons sur la publicité promotionnelle, et 95 % de tous nos revenus publicitaires proviennent des neuf mêmes pays »[98] [Traduction].

La toute nouvelle plateforme MyAds de MySpace contribue aux revenus. En novembre 2008, après seulement trois mois d'existence, elle générait en moyenne de 140 000 $ à 180 000 $ par jour. Les revenus de MySpace en 2008 sont évalués à 750 millions de dollars; ses revenus pour l'exercice se terminant en juin 2009 sont évalués à 1 milliard de dollars[99].

Profil démographique des utilisateurs

À l'échelle internationale, la majeure partie des utilisateurs de MySpace se trouvent aux États Unis (70,4 %), en Allemagne (3,5 %), au Royaume-Uni (3,4 %), en Italie (2 %) et au Mexique (2 %). Le Canada est au neuvième rang avec 0,9 % des utilisateurs[100].

Au cours du mois d'octobre 2008, MySpace a accueilli 55 millions de visiteurs uniques, ce qui illustre une tendance à la baisse par rapport aux 66 millions de visiteurs uniques qui avaient envahi le site en décembre 2007[101].

Selon les statistiques fournies par MySpace, 25 % des Américains utilisent le site et 85 % des utilisateurs ont 18 ans et plus. On compte en moyenne 300 000 inscriptions par jour.

Au Canada, MySpace affirme qu'en date du mois d'octobre 2008, le site accueillait 4 465 000 visiteurs uniques par mois. De plus, 62,7 % des utilisateurs sont des hommes et 47,3 %, des femmes. Enfin, 35,1 % des utilisateurs sont âgés de 18 à 34 ans et 34,2 % sont âgés de 35 à 54 ans[102].

Renseignements relatifs à l'inscription

Pour ouvrir un compte, l'utilisateur doit fournir les renseignements suivants : adresse de courriel, mot de passe, pseudonyme ainsi que prénom et nom, lieu de résidence (pays, province ou État, code postal), date de naissance (incluant l'option de l'afficher ou non), sexe, site et langue préférés, et code captcha. Il doit ensuite cocher une case pour confirmer qu'il accepte les conditions d'utilisation et la politique de confidentialité.

L'utilisateur entame ensuite un processus en trois étapes. Il doit d'abord télécharger une photo de profil, puis fournir des renseignements sur ses études (nom de l'établissement fréquenté, ville, province ou État, pays, nombre d'années). Enfin, il est invité à rechercher des amis à l'aide de son

carnet d'adresses de courriel (une fenêtre contextuelle indique alors que MySpace ne conservera pas le mot de passe entré pour accéder au compte). Chacune de ces étapes peut être sautée.

Une fois qu'il a répondu au courriel de confirmation, l'utilisateur peut commencer à personnaliser son profil, en y ajoutant d'autres informations ou en choisissant les couleurs et la mise en page. À cette étape, l'utilisateur dispose d'une foule d'onglets : Coordonnées, Compte, Mot de passe, Confidentialité, Pourriels, Notifications, Applications, MySpaceID, Portable, Calendrier et Divers.

Les coordonnées demandées dans le modèle sont le pseudonyme (l'utilisateur est encouragé à fournir plusieurs pseudonymes, que ce soit des noms réels ou d'anciens noms d'utilisateur, pour permettre aux autres utilisateurs de le retrouver plus facilement), le prénom et le nom (une case à cocher permet d'afficher ou non le nom complet lorsque le pseudonyme et la photo sont présentés), le nom de jeune fille, l'adresse de courriel, une autre adresse de courriel (l'utilisateur est avisé que cette adresse sera utilisée à des fins de recherche seulement), l'identifiant de messagerie instantanée, et l'emplacement géographique (pays, province ou État, ville, code postal).

Identités réelles et pseudonymes

Dans les renseignements relatifs à l'inscription, MySpace distingue le nom d'utilisateur et le pseudonyme. Même s'il doit obligatoirement fournir son prénom et son nom, l'utilisateur peut choisir des les afficher ou non, ou d'afficher seulement le pseudonyme.

À l'exception de l'adresse de courriel, aucun renseignement n'est vérifié.

Selon les conditions d'utilisation de MySpace, l'utilisateur doit fournir des informations véridiques et correctes à l'inscription et les maintenir à jour[103].

Mesures de protection de la vie privée

Au moment de configurer son profil, l'utilisateur peut se servir de l'onglet « Paramètres : Confidentialité » pour définir les paramètres suivants : s'il veut ou non qu'une icône « en ligne » soit associée à son profil; s'il autorise ou non ses amis à voir sa date de naissance; s'il autorise ou non d'autres utilisateurs à transmettre par courriel les photos qu'il a téléchargées; s'il veut ou non bloquer les utilisateurs de moins de 18 ans; s'il souhaite ou non avoir une liste des autres utilisateurs bloqués; et s'il veut que son profil soit vu par tout le monde, par toute personne de 18 ans et plus ou par ses amis seulement.

Même s'ils ne sont pas conçus comme des mesures de protection de la vie privée, les onglets de paramètres permettent à l'utilisateur de déterminer le volume de pourriels qu'il est prêt à recevoir ainsi que de gérer ses communications, comme les messages, les demandes d'amis, les commentaires, les invitations à joindre des groupes, les invitations à des événements et les invitations de messagerie instantanée. De la même façon, dans l'onglet Notifications, l'utilisateur peut décider des actions dont il souhaite être avisé par courriel sur MySpace, y compris les messages, les commentaires, les demandes d'amis, les commentaires sur les photos, le marquage de photos, les inscriptions à des vidéos, les inscriptions à des blogues, les commentaires sur les blogues, les invitations à joindre des groupes, les réponses écrites sur les forums et les invitations à des événements. L'utilisateur peut également se désabonner du bulletin électronique mensuel de MySpace.

La section MySpaceID indique à l'utilisateur qu'il peut lier des services de tiers à son compte MySpace. Les services liés seront affichés dans la page; l'utilisateur peut choisir les données qu'il veut échanger avec chaque service ou supprimer complètement le lien.

Enfin, dans l'onglet Applications, l'utilisateur décide s'il souhaite ou non recevoir des messages et des commentaires provenant des applications. Il définit également les paramètres de confidentialité pour les applications installées par ses amis (il peut décider de ne pas partager de données, de partager seulement les données de base, ou de permettre l'accès à ses photos et à ses albums photos publics ainsi qu'à ses données de base). Cette page fournit également à l'utilisateur une liste des applications qu'il utilise ainsi qu'une liste des applications qu'il a bloquées.

Marquage de photos

Les membres de MySpace sont autorisés à marquer des personnes dans une photo. Un lien est alors créé entre la photo et le profil de la personne marquée.

Lorsque l'utilisateur tente de marquer un non membre dans une photo, une fenêtre contextuelle demande l'adresse de courriel du non-nombre et offre de lui envoyer le lien de la photo par courriel.

Accessibilité aux renseignements des membres

ACTUALITÉS : La section « Que font mes amis » permet à l'utilisateur de voir le fil d'actualités décrivant les activités réalisées par les personnes sur sa liste d'amis. Cette section comprend également des onglets qui permettent à l'utilisateur de préciser les renseignements sur ses amis qu'il désire voir dans ses actualités et, inversement, les renseignements qui seront affichés à son sujet dans les actualités de ses amis.

RECHERCHE SUR LE SITE : L'utilisateur peut rechercher d'autres utilisateurs de MySpace par nom, adresse de courriel ou identifiant de messagerie instantanée. Il peut limiter le transfert de renseignements dans le cadre d'une recherche en indiquant qu'il s'agit d'un profil privé.

RECHERCHE PUBLIQUE : Les moteurs de recherche publique peuvent indexer les renseignements publics inclus dans le profil d'un utilisateur.

Publicité

À la fin de 2008, MySpace a développé des plateformes de publicité ciblée et intéressée.

La plateforme MyAds permet aux annonceurs de cibler les utilisateurs selon leur sexe, leur âge et leur emplacement géographique (pays, région, province ou État, code postal). La FAQ de MyAds (destinée aux annonceurs)

explique que MySpace ne peut garantir l'exactitude des renseignements qui servent au ciblage puisqu'ils sont fournis par l'utilisateur. De plus, MySpace n'utilise aucune technologie de géolocalisation afin d'améliorer le ciblage géographique[104].

Les conditions d'utilisation de MySpace indiquent également que certains messages publicitaires peuvent provenir d'entreprises publicitaires tierces qui emploient des technologies, comme les témoins, pour recueillir des renseignements et des données. L'utilisateur peut cliquer sur une adresse de courriel pour s'enquérir des techniques et de la politique de confidentialité de ces entreprises et pour refuser une telle collecte d'informations[105].

Conservation des données

MySpace recueille, au moment de l'inscription, l'adresse de courriel, le prénom et le nom, le code postal, le sexe et la date de naissance. MySpace peut également recueillir des renseignements liés à des activités du site comme les tirages au sort, les concours et les sondages, des renseignements trouvés sur le site et des renseignements fournis à MySpace à des fins d'examen ou de communication.

MySpace peut également recueillir le contenu d'un profil, comme la date de naissance, les intérêts, les loisirs, les habitudes de vie, les groupes auxquels appartient l'utilisateur, les vidéos, les photos, les messages privés, les bulletins et les commentaires personnels.

MySpace recueille aussi des données techniques comme l'adresse IP de l'utilisateur, des données agrégées et son type de navigateur. MySpace affirme que ces renseignements servent à gérer et à améliorer les services offerts, à surveiller l'utilisation du site et à garantir la sécurité des transactions.

La politique de confidentialité de MySpace établit une distinction intéressante entre les données d'inscription et les autres informations du profil : « MySpace détermine les fins de la collecte, de l'utilisation et de la divulgation des données d'inscription que vous fournissez et, en tant que tel, fait office de contrôleur des données en lien avec ces renseignements. Comme c'est le Membre, et non MySpace, qui détermine les fins de la collecte, de l'utilisation et de la divulgation des Informations du profil, MySpace ne tient pas lieu de contrôleur des données en lien avec les Informations du profil que les Membres ajoutent à leur profil ».

Fermeture de compte

Dans la section « Modifier mon compte », l'utilisateur peut cliquer sur le bouton « Annuler le compte ». Il recevra ensuite par courriel la marche à suivre pour fermer son compte. MySpace précise que la fermeture est permanente et que même si l'adresse de courriel de l'utilisateur peut être réutilisée à des fins de réinscription, le profil devra être recréé car les renseignements qui y sont liés ne seront pas conservés.

Applications tierces

Les applications de MySpace sont semblables à celles qu'on trouve sur Facebook, comme Portable, Nouvelles, Petites annonces, Karaoké et Sondages.

Le 5 février 2008, MySpace annonçait que les utilisateurs pouvaient désormais ajouter des applications de jeu, de courriel et autres à leur compte MySpace. La plateforme de développement MySpace a été lancée en mars 2008. MySpace insiste sur le fait que les développeurs n'ont accès qu'aux données publiques et que les utilisateurs peuvent limiter l'accès de leur compte à leurs amis seulement, empêchant ainsi les développeurs d'en consulter le contenu. Chaque application tierce offre aux développeurs des pages spéciales grâce auxquelles ils peuvent vendre des annonces, des messages de commandite et des produits. Cependant, aucune publicité n'apparaîtra dans les applications elles-mêmes une fois qu'elles seront installées[106].

MySpace travaille également au lancement de MySpace Music :

> « Le projet, qui relie les droits musicaux des grandes maisons de disques au contenu musical de MySpace et à ses utilisateurs, sera lancé par bon nombre de partenaires, y compris McDonald's, Sony Pictures, State Farm et Toyota. On rapporte que chacune de ces campagnes publicitaires s'élève à des millions de dollars, voire des dizaines de millions »[107] [Traduction],

Dans ses conditions d'utilisation, MySpace décline toute responsabilité quant au contenu, à l'exactitude des données et aux opinions exprimées sur les sites Web liés aux applications tierces, et déclare que ces sites ne sont pas contrôlés ni vérifiés de quelque manière que ce soit par MySpace. Essentiellement, l'utilisateur qui accède aux sites de tiers le fait à ses propres risques et périls[108].

En outre, la politique de confidentialité stipule que MySpace n'exerce aucun contrôle sur les développeurs tiers, leurs applications n'étant pas conçues par MySpace. MySpace conseille à ses membres de ne fournir aucun renseignement personnel à une application tierce, à moins qu'ils ne connaissent la partie avec laquelle ils sont en interaction[109].

Collecte des renseignements personnels des non membres

La question des renseignements personnels des non membres n'est pas abordée dans les conditions d'utilisation ni dans la politique de confidentialité. Cependant, au moment de marquer une photo, l'utilisateur peut entrer l'adresse de courriel d'un non membre pour lui envoyer le lien vers la photo. De même, l'utilisateur peut rechercher un membre en entrant son adresse de courriel ou son identifiant de messagerie instantanée (MySpace n'indique pas si ces renseignements sont conservés ou non).

Divers

La section « Accès » de la politique de confidentialité de MySpace accorde aux membres le droit (chaque fois que cela est possible) de prendre connaissance des données d'inscription que MySpace conserve sur eux. MySpace corrigera les renseignements personnels comportant des erreurs, pour autant que le membre l'en informe. Rien n'indique si ce droit s'étend au-delà des données d'inscription.


telefun
membres
france
promotions
personnalité
description physique
utilisateur
vidéo
audio
social
conditions de service
inconnus
biographie
ouvrir
tout sur moi
optionnel
langue
activation
téléchargements
concours
visiteurs
expression
mobile
opinions
sonneries
gens
commentaires
blogues de la semaine
situation amoureuse
activité principale
interactif
amis
visible
clavardage
sms
sécurité
modèle
inviter
historique
français
téléphonie
blogage
blogues vedettes
collect information
jeux
personnalisation
conception
ciblage
relations interpersonnelles
adolescent
SkyRock

SkyRock

www.skyrock.com

Mandat

Le logo de Skyrock comprend le slogan « Free People Network » (le réseau des gens libres).

Dans ses conditions générales d'utilisation (CGU), Skyrock est décrit comme « une plateforme interactive, laquelle comprend, sans que cette énumération puisse être considérée comme exhaustive, des services d'hébergement de journaux personnels illustrés en ligne (blog[ue]s), de profils, de dialogues en direct (chat), de dépôts de commentaires, de contenus éditoriaux, d'informations, de jeux et concours, de courriers électroniques, de messageries instantanées, de forums, d'envois de SMS, de téléchargements de sonneries et logos pour téléphones mobiles »[110]. On le décrit également comme une « plateforme française de blogues pour adolescents »[111] [Traduction].

Historique

Skyrock Property est une entreprise privée française dont le siège social est situé à Paris, en France. Elle a été fondée en 1985 par Pierre Bellanger en tant que station radiophonique française. Le site Web Skyrock.com, lié à la station radiophonique, a été mis en ligne le 13 mai 1998.

Le site Skyrock.com est édité par la société par actions simplifiée Telefun. Les services en ligne de Telefun forment maintenant une entité distincte de Skyrock Music[112].

En 2002, M. Bellanger a fondé la plateforme de blogues Skyrock (Skyblogs), qui a servi à développer le site de réseau social actuel.

En mai 2007, le site de réseau social a été rebaptisé Skyrock.com et est devenu « un réseau social complet grâce à de nouvelles fonctions comme l'ajout d'amis, la messagerie, le clavardage et les profils »[113] [Traduction].

Information financière

AXA Private Equity détient 70 % des parts de Skyrock[114]. Selon le site Web d'AXA, le projet de développement de Skyrock s'articule autour des principaux axes suivants :

- croissance sur la partie Internet et Mobile (25 % du CA), grâce à l'augmentation du nombre de blogues, les nouvelles fonctionnalités (audio, vidéo), la montée en puissance de la publicité en ligne sur le site Internet dédié aux blogues (nouveaux annonceurs, opérations spéciales), et le développement d'une offre de téléphonie;
- croissance de l'activité radio (75 % du CA), avec le plan de réallocation de fréquence 2006, une augmentation potentielle de la couverture nationale de la radio de 33 millions d'habitants à 45 millions[115].

Skyrock est à vendre depuis juin 2008. Un article mentionne que « ses revenus sont passés de moins de 5 millions d'euros en 2005 à moins de 10 millions d'euros en 2006, pour atteindre 15 millions d'euros l'an dernier [en 2007]. On estime que ses revenus s'élèveront à 20 ou 25 millions d'euros en 2008 »[116] [Traduction].

Profil démographique des utilisateurs

À l'échelle internationale, la majeure partie des utilisateurs de Skyrock se trouvent en France (72,8 %), en Belgique (8 %), en Suisse (3,8 %), en Algérie (3,2 %) et au Maroc (2,1 %). Le Canada arrive au sixième rang avec 1,8 % des utilisateurs. Seulement 0,5 % des utilisateurs sont Américains[117].

Le nombre d'utilisateurs uniques recensé a beaucoup varié au cours de l'année, passant de 600 000 en janvier 2008 à un peu moins de 200 000 en décembre 2008[118].

Selon les statistiques de février 2008, « Skyblogs compte plus de 22 millions d'utilisateurs inscrits, 14 millions de blogues actifs et 5,3 millions de profils. Le site se classe au 17e rang mondial pour les pages visitées, accueille plus de 20,2 millions de visiteurs uniques par mois et contient pas moins de 1,8 milliard de commentaires, 22,5 millions de vidéos et 400 millions de photos »[119] [Traduction].

Renseignements relatifs à l'inscription

Pour ouvrir un compte, l'utilisateur doit fournir les renseignements suivants : nom d'utilisateur, adresse de courriel, mot de passe, langue,

sexe, date de naissance, pays et code postal. Il peut également entrer son prénom et son nom. À la première page, l'utilisateur indique s'il souhaite ou non que les autres membres de Skyrock puissent le retrouver grâce à son courriel, à son prénom ou à son nom, et s'il souhaite ou non être informé des offres promotionnelles. L'utilisateur doit ensuite confirmer qu'il a pris connaissance des conditions d'utilisation et qu'il s'engage à les respecter, puis il doit taper le code captcha.

Après avoir entré ces informations, l'utilisateur passe à la page « Blog & Profil », où il doit donner un titre à son blogue (obligatoire) et le décrire. Il doit ensuite fournir sa date de naissance (obligatoire). De plus, s'il le désire, il peut indiquer son pays, sa région et sa ville, puis se présenter brièvement. L'utilisateur peut également télécharger une photo dans son profil et choisir un papier peint.

Ensuite, l'utilisateur doit activer son profil en répondant au courriel de confirmation qui lui est envoyé. Une fois son compte activé, l'utilisateur est redirigé vers une page de bienvenue, où il est invité à créer un blogue (avec des photos et des vidéos, par exemple), à remplir son profil et à inviter des amis sur Skyrock.

Si l'utilisateur veut personnaliser son profil, il doit cliquer sur « Crée ton profil ». Il pourra ajouter les renseignements suivants : sexe, date de naissance (seul renseignement obligatoire), pays, région et ville, situation, type de personne recherchée, activité principale, lieu de résidence, caractère, statut de fumeur ou de non-fumeur, description physique (couleur des cheveux et des yeux, taille, poids), et langue parlée. Le modèle offre aussi une zone de présentation (courte biographie) et des options « J'aime » et « Je déteste ».

Identités réelles et pseudonymes

À l'inscription, l'utilisateur doit fournir un pseudonyme (il peut également, s'il le veut, fournir son prénom et son nom). L'adresse de courriel entrée est validée, mais aucun autre renseignement n'est vérifié.

Les CGU précisent que l'utilisateur doit fournir « des informations vraies, exactes, à jour et complètes sur son identité et son âge comme demandé dans le formulaire d'inscription »[120].

Mesures de protection de la vie privée

Il ne semble pas y avoir de mesures de protection de la vie privée offertes aux utilisateurs du site.

Lorsqu'il modifie son profil, l'utilisateur peut décocher la case « Afficher les visites ».

Marquage de photos

L'utilisateur peut afficher jusqu'à 24 photos dans son profil. Aucune aide ne semble offerte pour l'association de métadonnées aux photos.

Accessibilité aux renseignements des membres

ACTUALITÉS : La page d'accueil de Skyrock contient beaucoup de renseignements sur les autres utilisateurs. Elle indique le nombre de blogues et de profils sur le site ainsi que le nombre de clavardeurs qui sont actuellement en ligne. On peut voir le Blog & Profil de la semaine, avec la photo, le nom d'utilisateur et la description (par exemple « J'aime rendre les gens heureux ») du membre, de même que des liens vers son blogue et son profil. La page d'accueil permet également de se joindre à des séances de clavardage sur Skyrock. De plus, elle offre un historique des blogs vedettes, avec la photo, le nom d'utilisateur et la description du membre associé à chaque blogue. Il y a également une fenêtre qui montre la photo et le nom d'utilisateur de huit nouveaux membres. On trouve aussi une liste des 100 meilleurs blogues, une liste de blogues de musique et une liste des dernières vidéos.

RECHERCHE SUR LE SITE : Au milieu de la page d'accueil, un outil de recherche permet à l'utilisateur de trouver le profil d'un membre en fonction du sexe et du pays. L'utilisateur peut également effectuer une recherche avancée à l'aide des critères suivants : option Gars, Filles, ou Gars ou fille; âge; pays; situation (Célibataire, Indifférent, En couple); type de personne recherchée par le membre (Qui recherche); intérêts du membre (Est ici pour); activité principale; lieu de résidence; caractère; couleur des yeux; taille; couleur des cheveux; et statut de fumeur ou de non-fumeur.

RECHERCHE PUBLIQUE : Les profils de Skyrock peuvent faire l'objet d'une recherche publique sur le Web. Un profil ainsi trouvé comprend normalement des renseignements comme le nom d'utilisateur, la photo, la description, des liens vers des contacts, la possibilité d'ajouter la personne comme ami, une liste d'amis et une liste des blogues préférés. Il semble impossible de limiter l'accès public à ces renseignements.

Publicité

La croissance de Skyrock est attribuable à son association à la station radiophonique du même nom et à l'autopublicité intermédia[121].

La clause 3.i des CGU de Skyrock mentionne ceci au sujet de la publicité :

> « En contrepartie du caractère gratuit des Services qui lui sont offerts par TELEFUN, l'Utilisateur autorise TELEFUN à associer au Contenu que l'Utilisateur diffuse sur l'un [des Services] des messages publicitaires ou promotionnels de type textes, images, vidéo ou sons, choisis par TELEFUN et ce sous toutes formes. Plus généralement, l'Utilisateur accepte que TELEFUN puisse utiliser (et y faire référence) le Contenu diffusé par l'Utilisateur pour assurer la promotion de ses Services. En aucun cas l'Utilisateur ne peut prétendre à une quelconque rémunération ou rétribution au titre de la présente autorisation. Si l'Utilisateur souhaite révoquer la présente autorisation, il lui appartiendra de procéder à la clôture de son Compte Personnel. Ladite révocation ne pourra avoir d'effets que pour l'avenir. Toute action publicitaire ou promotionnelle qui

> pourrait être engagée par TELEFUN au moment de la clôture de son Compte Personnel par l'Utilisateur se poursuivra jusqu'à son terme. »

Skyrock vend bel et bien de la publicité pour promouvoir son site, mais il n'indique pas clairement s'il utilise à cette fin les renseignements diffusés sur son site.

Conservation des données

Skyrock recueille les renseignements, les données, les textes, les logiciels, la musique, les sons, les photos, les images, les vidéos, les messages et tout autre contenu. Les CGU expliquent clairement que les données techniques peuvent être recueillies notamment à partir des témoins et des adresses IP.

Fermeture de compte

L'utilisateur peut décider de fermer son profil ou de supprimer son blogue Skyrock. S'il choisit la deuxième option, il sera averti que toutes ses informations (blogue, profil, photos, etc.) seront perdues.

La clause 2.d des CGU prévoit ceci :

> « À la clôture du Compte Personnel d'un Utilisateur, pour quelque cause que ce soit, les données relatives à ce compte[,] et en particulier les données de trafic, sont effacées ou rendues anonymes. Cependant [les opérations visant à effacer ou à rendre anonymes certaines catégories de données pourront être différées pour une durée maximale d'un an] en vue d'assurer la sécurité des installations de TELEFUN et pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, [au besoin, la mise à disposition de l'information à l'autorité judiciaire]. »

Applications tierces

Bien que Skyrock offre de nombreuses applications, elles semblent être internes plutôt que tierces.

Collecte des renseignements personnels des non-membres

Comme l'inscription n'est pas obligatoire pour lire les blogues sur Skyrock, le site recueille les renseignements des non membres grâce aux données de trafic. Dans le cas du clavardage, des concours et des autres applications, il se peut que Skyrock recueille certains renseignements personnels de non membres. Pour ce qui est du marquage de photos, Skyrock peut recueillir l'adresse de courriel d'un non membre pour lui envoyer un lien vers une photo. Les CGU ne contiennent aucune clause à ce sujet ni sur la façon dont un non membre peut supprimer ses renseignements de Skyrock.

D: Analyse comparative

Renseignements relatifs à l'inscription

Renseignements obligatoires et renseignements demandés

Le « Mémorandum de Rome » recommande aux fournisseurs de « faire preuve d'honnêteté et de clarté quant aux renseignements requis pour la prestation de services de base »[122] [Traduction]. À première vue, cette recommandation semble être respectée : sur chacun des six sites examinés, on demande d'abord à l'utilisateur de fournir certains renseignements pour pouvoir s'inscrire, puis, au moyen d'invites, on lui permet de remplir son profil en entrant d'autres informations.

Par contre, si on regarde la marche à suivre dans son ensemble, la distinction est beaucoup moins nette. L'utilisateur qui établit son profil franchit les étapes comme s'il s'agissait d'un seul et même processus : il fournit les renseignements obligatoires à l'inscription, active son compte par courriel, puis établit son profil en donnant plus de renseignements. Ainsi, il se peut que l'utilisateur ne fasse pas la différence entre les renseignements obligatoires pour l'inscription et les renseignements complémentaires au profil.

De plus, chaque site utilise un modèle de création de profil, comprenant des catégories de renseignements à fournir et des champs à remplir. Ainsi, on peut croire que ces renseignements, s'ils ne sont pas obligatoires, sont du moins demandés par le site ou qu'il est recommandé de les entrer. La distinction n'est certainement pas claire pour l'utilisateur.

Les politiques de confidentialité de LinkedIn et de MySpace établissent clairement cette distinction. LinkedIn précise que les renseignements autres que les renseignements obligatoires sont jugés « sensibles », mais qu'en fournissant de tels renseignements, l'utilisateur consent de façon explicite à leur emploi prévu dans les conditions d'utilisation. Quant à MySpace, il déclare contrôler les données obligatoires fournies à l'inscription, mais pas les informations que les membres ajoutent à leur profil.

D'après Susan Barnes, « en demandant ce type de renseignements et en établissant des exigences relatives à l'inscription, on semble indiquer aux jeunes qu'ils peuvent communiquer des renseignements personnels en ligne en toute sécurité »[123] [Traduction]. Même si l'article de M^me^ Barnes est axé sur l'utilisation par les jeunes des réseaux sociaux, on peut en conclure que lorsqu'un utilisateur est invité par un site à fournir des renseignements précis, il hésite moins et éprouve un sentiment de sécurité.

Recommandation 1 : Les sites doivent s'efforcer de se conformer à la recommandation de Rome voulant que les renseignements obligatoires à la prestation des services soient définis plus clairement. Cependant, cette mesure n'est peut-être pas suffisante en soi.

Recommandation 2 : Les sites doivent reconnaître que la distinction entre les renseignements obligatoires et les renseignements demandés ou suggérés pour compléter le profil ou pour optimiser l'utilisation du site n'est pas claire, et que, par conséquent, il peut être insidieux d'appliquer des normes différentes à chaque type d'information.

Sécurité

Au moment de l'inscription, certaines étapes liées à la sécurité ont attiré notre attention.

Facebook, LiveJournal, MySpace et Skyrock utilisent tous des algorithmes de test captcha[124] dans leurs pages d'inscription, pour s'assurer que les comptes sont créés par des personnes et non des robots. L'ENISA recommande aux sites d'« exercer un contrôle d'authentification et d'accès accru lorsque cela est nécessaire »[125] [Traduction].

Recommandation 3 : On doit inciter les sites à inclure des algorithmes captcha afin d'assurer une meilleure authentification et un meilleur contrôle.

De la même façon, pour ce qui est du choix de mot de passe, soulignons que certains sites offrent un encadré qui explique les normes de sécurité minimales ou qui indiquent que le mot de passe choisi respecte ces normes. Il s'agit encore une fois d'une mesure de sécurité simple, mais

combien importante pour la protection de comptes contenant des renseignements personnels.

Recommandation 4 : On doit inciter les sites à établir et à expliquer les normes de sécurité minimales en ce qui a trait aux mots de passe de comptes.

L'obligation de fournir sa date de naissance pour ouvrir un compte est une question litigieuse. Si certains sites demandent la date de naissance, le site LiveJournal va plus loin : sa page de création de compte contient un encadré affirmant que cette date est requise par la loi, mais que pour renforcer la sécurité, le site n'affiche par défaut que le jour et le mois de naissance. De la même façon, le processus d'inscription de LinkedIn requiert un code postal, mais un encadré explique que seule la région est affichée. Voilà encore une bonne façon de recueillir les renseignements nécessaires à l'inscription tout en limitant l'accès public aux renseignements personnels permettant l'identification. Les sites doivent au moins envisager d'expliquer que la collecte de la date de naissance est exigée par la loi et d'établir une distinction entre les renseignements d'inscription et de profil. Ainsi, la date de naissance fournie par l'utilisateur ne sera pas automatiquement affichée dans son profil, sauf si l'utilisateur en décide autrement en fournissant cette date une seconde fois à l'établissement du profil.

Recommandation 5 : Les sites doivent établir une distinction nette entre les renseignements obligatoires pour l'inscription et les informations du profil. Les renseignements recueillis lors de l'inscription ne doivent pas se retrouver automatiquement dans le profil, sauf si l'utilisateur les ajoute lui-même.

Recommandation 6 : Dans la mesure du possible, les sites doivent élaborer des codes qui permettent à l'utilisateur d'indiquer son emplacement géographique sans avoir à fournir des renseignements personnels comme le code postal.

Paramètres

Jones et Soltren recommandent aux sites d'appliquer des paramètres de confidentialité aux informations fournies dans un profil. De tous les sites passés en revue, seul hi5 le fait : au moment de définir son profil, l'utilisateur peut choisir les personnes qui auront accès à ses renseignements (à l'exception du prénom, de la langue, de l'origine ethnique et de la section « À propos de moi »), en l'occurrence tout le monde, ses amis seulement ou personne. Même si nous reviendrons sur cette question à la section sur les mesures de protection de la vie privée, les sites doivent, dans la mesure du possible, offrir des paramètres de confidentialité à l'étape de l'établissement du profil, de façon à éclairer l'utilisateur dans ses décisions.

Recommandation 7 : Dans la mesure du possible, les sites doivent créer un lien entre les pages de définition du profil et les paramètres de confidentialité, ce qui éclairera l'utilisateur dans ses décisions.

Identités réelles et pseudonymes

Le « Mémorandum de Rome » recommande aux fournisseurs d'introduire l'option de création et d'utilisation de pseudonymes et d'encourager ce choix[126]. Les sites examinés emploient diverses stratégies. Facebook et hi5 ne permettent ni l'utilisation d'un pseudonyme ni l'affichage limité des renseignements. LinkedIn offre l'option d'afficher seulement le prénom et la première lettre du nom de famille. MySpace exige le prénom et le nom, mais permet d'afficher seulement le pseudonyme. LiveJournal ne demande qu'un pseudonyme pour s'inscrire. Skyrock demande un pseudonyme, mais permet d'entrer le prénom et le nom.

Recommandation 8 : L'utilisateur doit au moins avoir l'option de fournir et d'utiliser un pseudonyme pour ses comptes SRS.

Mesures de protection de la vie privée

Dans son rapport d'étude sur l'utilisation des réseaux sociaux et sur les attitudes et comportements des utilisateurs, l'UK Office of Communications constate que l'utilisateur présume que les sites de réseau social ont réglé toutes les questions liées à la protection de la vie privée et à la sécurité[127]. Par conséquent, s'il est important de vérifier l'existence de mesures de protection de la vie privée, il faut aussi connaître l'accessibilité de ces mesures, les paramètres par défaut et le niveau d'autodétermination de l'information qu'elles offrent à l'utilisateur.

Selon l'étude de Hewitt et de Forte, « les étudiants qui ont soulevé des inquiétudes à l'égard de la protection de la vie privée ignoraient les options de confidentialité offertes sur le site (comme la création de profils spéciaux et limités qui ne peuvent être vus que par certains utilisateurs) ou ne croyaient pas que ces options étaient conformes à leurs attentes et à leurs expériences quant à la confidentialité sur le site »[128] [Traduction]. Encore une fois, il importe que la convivialité des mesures de protection de la vie privée corresponde à la compréhension et à l'utilisation des fonctions du site.

Paramètres par défaut

Les recherches montrent que « les utilisateurs n'ont pas tendance à changer les paramètres par défaut »[129] [Traduction]. C'est pourquoi ces paramètres sont importants. L'ENISA recommande donc de définir les paramètres par défaut appropriés[130]. Évidemment, les sites doivent trouver un équilibre entre le désir de l'utilisateur de protéger ses renseignements personnels et de tirer le plus profit de l'utilisation du site, d'une part, et l'intérêt du site à vouloir recueillir des données pour satisfaire aux besoins de l'utilisateur et adopter un modèle financé par la publicité, d'autre part. Il serait pour le moins souhaitable que les paramètres de confidentialité puissent être désactivés plutôt qu'activés[131], et que les sites pèchent par excès de prudence tout en offrant à l'utilisateur la possibilité d'augmenter le niveau d'échange et de visibilité des renseignements.

Recommandation 9 : Les paramètres par défaut doivent protéger les renseignements personnels plutôt que d'en imposer l'échange.

Recommandation 10 : La formulation est importante. L'utilisateur doit pouvoir choisir d'augmenter le niveau d'échange des renseignements, plutôt que d'avoir l'impression de désactiver des paramètres de confidentialité.

Intégration des mesures de protection de la vie privée
Des six sites étudiés, ceux qui proposent des mesures de protection de la vie privée les offrent en tant que solutions ponctuelles que l'utilisateur doit rechercher avant d'appliquer.

Selon l'ENISA, « les SRS doivent utiliser, dans la mesure du possible, de l'information contextuelle pour renseigner les personnes en temps réel »[132] [Traduction]. De même, le « Mémorandum de Rome » fait observer ceci à propos des mesures de protection de la vie privée : « Même si cette information est présentée à l'écran d'inscription à un service, et que l'utilisateur peut y accéder plus tard s'il le souhaite, l'objectif d'informer l'utilisateur des conséquences potentielles de ses actions pendant l'utilisation du service (…) sera mieux servi par des fonctions intégrées et contextuelles qui diffusent l'information au moment opportun »[133] [Traduction].

Rappelons que hi5 offre des mesures de protection de la vie privée aux étapes d'inscription et d'établissement du profil (l'utilisateur peut déterminer le niveau de confidentialité de ses renseignements lorsqu'il les entre pour la première fois). L'utilisateur peut également retourner à l'onglet « Paramètres de confidentialité » pour changer ou augmenter le niveau de contrôle de ses renseignements. Quoi qu'il en soit, le simple fait d'associer des paramètres de confidentialité à la fourniture de renseignements demeure une bonne stratégie recommandée à tous les sites.

Recommandation 11 : Dans la mesure du possible, les sites doivent créer un lien entre les pages de fourniture de renseignements et les paramètres de confidentialité, ce qui éclairera l'utilisateur dans ses décisions.

LiveJournal adopte aussi une méthode stratégique pour intégrer des mesures de protection de la vie privée. Il permet à l'utilisateur d'établir des mesures pour l'ensemble d'un journal ou pour chaque entrée, en choisissant de rendre certains éléments visibles pour tous, pour les amis seulement ou pour l'auteur seulement. LiveJournal permet également la création de communautés, où les messages qui y sont destinés y demeurent plutôt que d'apparaître dans le journal de l'utilisateur. Un message peut être réservé uniquement aux amis de l'utilisateur. En sélectionnant le niveau de confidentialité pour chaque entrée, plutôt qu'en établissant des paramètres globaux une seule fois, l'utilisateur participe activement à la protection de ses renseignements personnels. Bien que cette stratégie semble difficile à appliquer aux actualités, les sites devraient envisager de l'utiliser au moins pour chaque élément affiché, que ce soit des messages, des notes ou d'autres entrées personnelles.

Recommandation 12 : Les mesures de protection de la vie privée ne doivent pas être globales ni distinctes. Dans la mesure du possible, les sites doivent intégrer des paramètres de confidentialité à chaque fonction pour que l'utilisateur puisse exercer un contrôle accru sur l'échange de ses renseignements.

Marketing
Le « Mémorandum de Rome » recommande aux sites de « permettre à l'utilisateur de contrôler l'usage secondaire de ses données de profil et de trafic, notamment à des fins commerciales, en lui offrant la possibilité de définir des renseignements confidentiels sur le profil (opinions politiques, orientation sexuelle, etc.) et le trafic, plutôt que des renseignements généraux »[134] [Traduction]. Aucune des mesures de protection de la vie privée offertes sur les sites examinés ne suit cette recommandation. Les onglets de mesures de protection de la vie privée doivent au moins comprendre une section qui indique clairement les renseignements pouvant être utilisés à des fins publicitaires et qui permet à l'utilisateur de configurer l'utilisation de ses renseignements personnels. Si ces données sont mentionnées dans les politiques de confidentialité et les conditions d'utilisation, encore faut il qu'elles soient incluses dans les mesures de protection de la vie privée.

Recommandation 13 : Les paramètres de confidentialité doivent comprendre une section qui indique clairement les renseignements pouvant être utilisés à des fins publicitaires et qui permet à l'utilisateur de configurer l'utilisation de ses renseignements personnels à ces fins.

Actualités
Les mesures de protection de la vie privée de Facebook offrent beaucoup de paramètres liés aux actualités, comme une liste des actions qui ne seront jamais affichées, une liste des applications qui peuvent transmettre des informations à la liste et une série d'options que l'utilisateur peut bloquer de ses actualités.

Recommandation 14 : On doit encourager les sites à ajouter des contrôles granulaires pour informer l'utilisateur des renseignements qui seront échangés dans les actualités internes et lui permettre de les personnaliser.

Recherche
La recherche d'autres utilisateurs sur le site est une fonction essentielle. Par conséquent, il est important que les sites intègrent des mesures de protection de la vie privée qui permettent à l'utilisateur de déterminer les critères selon lesquels il pourra être recherché, de limiter sa visibilité dans les recherches et de sélectionner les renseignements qui seront affichés dans les résultats de recherche.

Recommandation 15 : Les mesures de protection de la vie privée doivent permettre à l'utilisateur de choisir lesquels de ses renseignements peuvent être recherchés.

Recommandation 16 : Les mesures de protection de la vie privée doivent permettre à l'utilisateur de comprendre quels renseignements seront affichés dans les résultats de recherche et de les choisir en conséquence.

Recommandation 17 : Les mesures de protection de la vie privée doivent permettre à l'utilisateur de contrôler sa visibilité dans les recherches internes.

Facebook permet également à l'utilisateur de choisir les moyens de communication offerts aux gens qui auront trouvé son profil; hi5 permet à l'utilisateur de déterminer les personnes dont il accepte les demandes d'amis ainsi que la façon dont on peut communiquer avec lui. Les sites sont encouragés à adopter de telles mesures.

Recommandation 18 : On recommande aux sites d'ajouter des mesures de protection de la vie privée qui permettent à l'utilisateur de choisir s'il peut ou non être contacté grâce à la recherche interne et, le cas échéant, la façon dont il peut être joint.

Applications

La question des applications tierces sera approfondie plus loin dans cette analyse. Quoi qu'il en soit, une des options clés des mesures de protection de la vie privée doit être la capacité de l'utilisateur à gérer la communication de ses renseignements personnels avec des tiers.

Facebook offre à l'utilisateur le choix de ne pas utiliser certaines applications, comme Beacon et Facebook Connect, en plus de lui permettre de gérer le type de renseignements qui sont vus par ses amis lorsqu'il utilise des applications non communes. Cependant, en ce qui a trait aux applications tierces, Facebook permet à l'utilisateur de refuser l'échange de renseignements avec des applications seulement s'il n'utilise aucune application. Cela ne dissipe évidemment pas les inquiétudes soulevées par de nombreuses personnes, à savoir que les applications tierces peuvent accéder non seulement aux renseignements personnels de l'utilisateur qui se sert de l'application, mais aussi des amis de cet utilisateur. Certains voient donc leurs renseignements transmis à des applications à leur insu ou sans leur consentement explicite. Les mesures de protection de la vie privée de MySpace, en revanche, permettent à l'utilisateur de régler les paramètres de confidentialité de ses renseignements relativement à l'utilisation des applications par ses amis, lui permettant ainsi de ne communiquer aucun renseignement, de ne communiquer que des renseignements généraux, ou de communiquer tous ses renseignements publics. On doit encourager les sites à adopter le modèle de MySpace, ce qui protégerait davantage l'utilisateur contre la communication non autorisé de ses renseignements personnels avec les applications.

Recommandation 19 : Les mesures de protection de la vie privée doivent permettre à l'utilisateur de contrôler l'échange de ses renseignements personnels avec les applications tierces lorsque ses amis ou lui-même utilisent ces applications.

Commentaires et messages du mur

Comme le souligne Patricia Lange, surtout dans un environnement libéral (presque automatique) d'amitié, l'entrée de commentaires et de messages sur le mur est un aspect important du processus social de ces sites[135]. Quant à danah boyd, elle s'intéresse aux effets que les commentaires des autres peuvent avoir sur un utilisateur compte tenu de leur visibilité et de la façon dont ils sont intégrés dans le profil de l'utilisateur[136]. Ainsi, vu l'importance des commentaires et leurs répercussions possibles sur le comportement de l'utilisateur, leur utilisation et leur visibilité doivent pouvoir être contrôlées par des mesures de protection de la vie privée. À ce sujet, les mesures proposées par hi5 méritent d'être mentionnées : elles permettent à l'utilisateur de décider qui peut lui envoyer des commentaires et si ces commentaires sont acceptés automatiquement ou non. Dans la négative, l'utilisateur doit accepter les commentaires pour qu'ils puissent être affichés.

Recommandation 20 : L'utilisateur doit pouvoir gérer la réception et la visibilité des commentaires d'autres utilisateurs à l'aide de mesures de protection de la vie privée.

Photos

Même si la question des photos sera abordée plus en détail à la section suivante, il est à noter que les mesures de protection de la vie privée de hi5 permettent à l'utilisateur de décider si ses amis peuvent ou non marquer les photos qu'il télécharge, s'ils peuvent ou non commenter ces photos, et si ces commentaires sont automatiquement acceptés ou doivent être acceptés manuellement avant d'être affichés.

Marquage de photos

Trois des sites étudiés (Facebook, hi5 et MySpace) permettent d'associer aux photos des métadonnées qui identifient les membres et les non-membres.

Actuellement, l'utilisateur peut « marquer » des personnes dans une photo. Un lien est alors créé entre la photo et le profil de l'utilisateur marqué. Ce dernier est avisé du marquage, reçoit un lien pour voir la photo et peut décider de retirer le marquage.

Un non membre peut également être marqué dans une photo. Le site recueille alors son nom et son adresse de courriel et lui envoie un lien vers la photo.

Consentement

Le « Mémorandum de Rome » et l'ENISA émettent tous deux des recommandations concernant le consentement au marquage de photos. Le Mémorandum précise que « le marquage de photos (…) nécessite d'abord le consentement de la personne concernée »[137] [Traduction], alors que l'ENISA recommande aux sites d'« exiger le consentement des personnes concernées avant d'inclure des marques dans une image »[138] [Traduction].

Aucun des sites étudiés n'exige de consentement avant l'ajout d'une marque dans une photo. Au contraire, quiconque a accès à la photo peut la marquer, et c'est seulement par la suite qu'on en informe la personne concernée et qu'on lui donne le choix de retirer la marque.

Recommandation 21 : On doit encourager les sites à adopter les recommandations du « Mémorandum de Rome » et de l'ENISA, c'est-à-dire de modifier le processus de marquage de photos en permettant à l'utilisateur de marquer des photos, mais en attendant le consentement des personnes marquées avant de créer la marque.

Marquage des non membres

Le marquage des non membres est une question problématique. Il se peut que la personne ignore qu'elle a été marquée; par conséquent, elle n'a aucun contrôle sur ses renseignements personnels. De plus, les modèles actuels de marquage des non membres recueillent l'adresse de courriel de la personne concernée afin de l'avertir qu'elle a été marquée. Comme le souligne Grimmelmann, « les personnes qui décident de ne pas se joindre à Facebook indiquent clairement qu'elles préfèrent garder leurs renseignements confidentiels, et ce choix doit être honoré »[139] [Traduction]. Ainsi, il ne faut pas afficher les renseignements personnels (nom lié à une photo) des non-membres sur le site, ce qui élimine le besoin de recueillir d'autres renseignements personnels (adresse de courriel) pour les aviser.

Recommandation 22 : On ne doit pas pouvoir marquer des non membres dans les photos affichées sur un site.

Mesures de protection de la vie privée

Certains sites offrent un contrôle limité sur les photos et les photos marquées dans leurs mesures de protection de la vie privée : Facebook, par exemple, permet à ses utilisateurs de choisir les personnes qui peuvent voir les photos dans lesquelles ils sont marqués.

Cela ne veut pas dire que ces sites n'offrent aucune mesure de protection de la vie privée concernant les photos. La plupart des sites qui acceptent les photos permettent à l'utilisateur de fixer le niveau de sécurité de chaque photo et de chaque album. Cependant, ces paramètres sont généralement liés aux applications de photos elles mêmes, et non inclus dans les mesures de protection de la vie privée. Les sites doivent envisager de centraliser les mesures de protection de la vie privée en les combinant aux paramètres de confidentialité des photos.

Recommandation 23 : Les paramètres de confidentialité des photos doivent être intégrés aux autres paramètres de confidentialité pour faciliter leur compréhension et leur utilisation.

Rappelons que dans ses mesures de protection de la vie privée, hi5 permet à l'utilisateur de décider si les autres peuvent marquer ou non les photos qu'il télécharge.

Recommandation 24 : Les photos ne doivent pas pouvoir être marquées par défaut; l'utilisateur doit pouvoir choisir si ses photos peuvent être marquées ou non.

Les sites doivent également envisager d'ajouter un paramètre de confidentialité qui permet à l'utilisateur de ne jamais être marqué dans une photo[140].

Recommandation 25 : Les paramètres de confidentialité doivent permettre à l'utilisateur de choisir s'il veut ou non être marqué dans les photos.

Accessibilité aux renseignements des membres

L'accessibilité au profil des autres est, dans une certaine mesure, une des fonctions principales des réseaux sociaux. Après tout, si un membre d'un réseau social n'est pas visible, n'est pas disponible pour être ajouté comme ami et n'est pas joignable, il est inutile qu'il fasse partie de ce réseau. Cependant, l'impératif de la visibilité influe sur les décisions à l'égard de la confidentialité. Adam N. Joinson émet l'hypothèse que « les fonctions de surveillance et de recherche sociale de Facebook peuvent expliquer, en partie, pourquoi tant d'utilisateurs sont relativement tolérants lorsqu'il est question des paramètres de confidentialité. Si la recherche sociale est un bien public, la règle de réciprocité veut qu'en permettant d'être surveillé, on puisse aussi surveiller les autres »[141] [Traduction].

Pour expliquer la réticence de l'utilisateur à restreindre activement l'accessibilité à ses renseignements, Sören Preibusch et coll. suggèrent d'analyser les données selon quatre niveaux : les données « privées » (qui servent uniquement à l'utilisation interne du site, comme l'adresse de courriel fournie lors de l'inscription); les données « de groupe » (qui servent à l'utilisation interne du site et qui sont accessibles à un groupe limité, comme un réseau); les données « communautaires » (qui servent à l'utilisation interne du site et qui sont accessibles à tous les utilisateurs inscrits et connectés, comme la situation, les contacts, les informations de profil et les photos de profil); et les données « publiques » (disponibles dans le cadre des activités des membres du site et accessibles à quiconque, comme le fait que l'utilisateur possède un profil sur le site et son nom d'utilisateur.)[142]. Bien que cette hiérarchie ne semble pas régler entièrement le problème, elle peut aider les sites à conceptualiser les renseignements au moment d'établir les paramètres par défaut. L'utilisateur doit toutefois pouvoir contrôler l'accès à ses données grâce à des mesures de protection de la vie privée.

Généralement, les renseignements de l'utilisateur deviennent accessibles aux autres par l'une des trois fonctions suivantes : les actualités, la recherche sur le site et la recherche publique.

Actualités

Le « Mémorandum de Rome » recommande de permettre « la réduction de la visibilité des informations de profil »[143] [Traduction].

Monica Chew et coll. font observer ceci : « Le manque de contrôle sur les données liées aux activités peut compromettre la vie privée d'un utilisateur de deux façons. Premièrement, il se peut que l'utilisateur ignore les événements qui font partie de ses données d'activité. Deuxièmement, il se peut qu'il ignore les personnes qui ont accès à ses données d'activité »[144] [Traduction]. Les auteurs émettent ainsi cinq recommandations sur les actualités : 1) l'utilisateur doit être informé des renseignements qui figurent dans les actualités; 2) l'utilisateur doit pouvoir choisir les renseignements qui figurent dans les actualités; 3) l'utilisateur doit être explicitement informé des personnes qui ont accès aux actualités; 4) l'utilisateur doit pouvoir choisir les personnes qui ont accès à ses actualités; et 5) les développeurs doivent créer leurs applications de façon à ce que le processus de création d'actualités soit plus conforme aux attentes de l'utilisateur[145].

Certains sites, notamment Facebook, hi5 et MySpace, offrent à leurs utilisateurs un certain niveau de contrôle sur les renseignements qui figurent dans les actualités et sur les personnes qui peuvent y accéder. MySpace permet également à l'utilisateur de choisir le type de renseignements qu'il peut recevoir de ses amis. On doit encourager les sites à offrir le plus de flexibilité possible concernant le choix des renseignements affichés dans les actualités et des personnes qui y ont accès. La mesure récemment adoptée par Facebook, qui consiste à permettre la création de groupes pour gérer les paramètres d'affichage, doit être encouragée.

Recommandation 26 : On doit encourager les sites à offrir à l'utilisateur le plus de flexibilité possible concernant le choix des renseignements qui figurent dans les actualités et des personnes qui y ont accès.

Recherche sur le site

Les six sites étudiés offrent des moteurs de recherche interne permettant à l'utilisateur de trouver des personnes par nom ou par adresse de courriel. Certains sites permettent d'effectuer une recherche à partir d'autres informations du profil, comme l'emplacement géographique, les intérêts et la situation amoureuse.

Certains sites permettent à l'utilisateur de choisir s'il peut ou non faire l'objet d'une recherche (LiveJournal), de déterminer qui peut le rechercher (hi5) ou de limiter les renseignements visibles dans les résultats de recherche (Facebook, LinkedIn et MySpace).

Le « Mémorandum de Rome » recommande aux sites de permettre « la réduction de la visibilité dans les fonctions de recherche communautaire »[146] [Traduction]. Danah boyd affirme avoir surpris de nombreux interviewés, qui croyaient que leur profil était confidentiel, en leur montrant qu'un membre d'un réseau peut consulter le profil d'un autre membre[147]. L'utilisateur doit comprendre la notion de visibilité et disposer des outils nécessaires pour gérer de tels paramètres. Entre autres, il doit pouvoir choisir si son profil est automatiquement visible ou non sur les réseaux élargis.

Recommandation 27 : L'utilisateur doit savoir exactement quelles sont les informations de son profil qui sont affichées dans les résultats de recherche.

Recommandation 28 : L'utilisateur doit disposer des outils de confidentialité nécessaires pour gérer ses paramètres de visibilité dans les recherches.

Recommandation 29 : La visibilité automatique sur les réseaux élargis ne doit pas être un paramètre par défaut dans les recherches internes.

Recherche publique

Sur les six sites examinés, les profils sont indexés par les moteurs de recherche publique et, par conséquent, consultables par les non membres. Dans certains cas, les non membres peuvent également effectuer des recherches sur le site.

Le « Mémorandum de Rome » précise que « par défaut, les profils ne doivent pas être indexés par les moteurs de recherche »[148] [Traduction], ce qui n'est pas le cas actuellement. Facebook active l'indexation par défaut, mais l'utilisateur peut la désactiver. De même, hi5, LiveJournal, MySpace et Skyrock indexent par défaut les profils dans les moteurs de recherche publique. LinkedIn active aussi l'indexation par défaut, mais cela est moins surprenant compte tenu du fait qu'il s'agit d'un site de réseautage professionnel et non personnel. L'option de retirer son profil des recherches publiques n'est pas suffisante : les sites doivent se conformer à la recommandation du « Mémorandum de Rome » et configurer la non-indexation par défaut (tout en permettant à l'utilisateur d'activer l'indexation).

Recommandation 30 : Par défaut, les profils ne doivent pas être indexés par les moteurs de recherche.

L'ENISA recommande également aux sites de « porter attention aux résultats de recherche : les données doivent être anonymes ou ne pas être affichées du tout, sinon l'utilisateur doit savoir qu'elles figureront dans les résultats de recherche et qu'il peut décider de les retirer »[149] [Traduction]. Sur la plupart des sites, un profil désigné comme « privé » ou encore des renseignements « privés » ou « pour amis seulement » ne sont pas affichés ou ne sont affichés qu'en partie. De plus, LiveJournal offre des outils qui permettent à l'utilisateur de réduire sa visibilité dans les recherches et de régler les paramètres de sécurité de chaque entrée, ce qui empêche tout renseignement non public d'être affiché dans les résultats de recherche publique. LinkedIn, tout en donnant accès par défaut aux profils, permet à l'utilisateur de choisir s'il veut ou non faire l'objet d'une recherche et, le cas échéant, quels renseignements sont affichés. On doit encourager les sites à offrir davantage de paramètres à l'utilisateur pour qu'il puisse gérer l'affichage de ses renseignements personnels dans les résultats de recherche publique.

Recommandation 31 : L'utilisateur doit pouvoir choisir si ses renseignements de profil peuvent ou non faire l'objet d'une recherche publique et, les cas échéant, quels renseignements sont affichés.

Publicité

La publicité est un élément clé du modèle opérationnel de la plupart des SRS. Comme l'explique Matthew Hodge, il s'agit d'une relation cyclique : l'utilisateur a droit à un compte gratuit et peut établir son profil sur l'espace de stockage de l'ordinateur central du site, auquel il peut accéder en tout temps. En retour, le site obtient des « appels de fichier » et accueille plusieurs utilisateurs. Pour que leurs annonces produisent l'effet escompté, les spécialistes du marketing veulent s'assurer qu'ils ont un public et qu'ils pourront bien le cibler. L'existence du site de même que la collecte et l'utilisation des renseignements par le site contribuent grandement à cet objectif. Enfin, la gratuité des services offerts sur le site est garantie par l'achat d'espace publicitaire par ces spécialistes[150]. Sören Preibusch et coll. abondent en ce sens, en ajoutant que ce modèle séduit les annonceurs non seulement parce qu'il leur permet de cibler un public, mais aussi parce qu'il permet un ciblage précis. En effet, les renseignements fournis volontairement ont un taux d'exactitude plus élevé, et la visibilité des réseaux facilite la validation des catégories de cibles[151].

Transparence

Les sites reconnaissent l'importance relative de la publicité pour leur fonctionnement et annoncent clairement dans leur politique de confidentialité et dans leurs conditions d'utilisation que les renseignements recueillis sont utilisés à des fins publicitaires. Il semble néanmoins que les utilisateurs ne comprennent pas tout à fait ces avis. Comme le font remarquer Jones et Soltren, « cette communication de données est parfaitement légale et, en retour, l'utilisateur peut se servir gratuitement d'un site très pratique et populaire. Malheureusement, ce ne sont pas tous les utilisateurs qui comprennent les conditions; notre sondage montre que 46 % des utilisateurs de Facebook croient que le site ne peut pas communiquer leurs renseignements avec des tiers »[152] [Traduction].

Recommandation 32 : On doit encourager les sites à faire preuve de plus de transparence à propos de leurs relations avec les annonceurs et à mettre cette information à l'avant-plan lorsque l'utilisateur s'inscrit.

Clarté

En plus de sensibiliser l'utilisateur à la présence et au rôle de la publicité, les sites doivent décrire plus clairement le lien entre la collecte de renseignements et les ventes publicitaires.

Le « Mémorandum de Rome » précise ceci :

> « Un exemple frappant est celui de l'énoncé du type "Nous ne communiquerons jamais vos renseignements personnels à des tiers". Bien que cette déclaration semble exacte aux yeux des fournisseurs de services, certains d'entre eux ne réussissent pas à expliquer clairement que, par exemple, pour afficher des annonces dans les fenêtres de navigation d'un utilisateur, il se peut qu'ils transmettent son adresse IP à un tiers qui fournit le contenu des annonces, dans certains cas à partir des renseignements de profil traités par le réseau social »[153] [Traduction].

Même si la politique de confidentialité de chaque site mentionne que certains renseignements sont utilisés à des fins publicitaires, aucune ne précise la nature de ces renseignements ni les modalités d'échange. Les sites ont plus tendance à énumérer les renseignements personnels qui ne seront pas communiqués (nom, adresse de courriel, etc.) qu'à décrire ceux qui le seront ou pourraient l'être.

Recommandation 33 : On doit encourager les sites à être plus clairs en ce qui a trait aux renseignements qui sont utilisés à des fins publicitaires ou qui pourraient l'être.

Regroupement des renseignements

Plusieurs sites disent regrouper les renseignements avant de les communiquer, pour faciliter le ciblage publicitaire. Cependant, comme le mentionne l'EPIC, « les sites (…) ne précisent pas le type de renseignements agrégés qu'ils offrent aux annonceurs, pas plus qu'ils ne soulignent la possibilité que les tiers « désagrègent » ces renseignements »[154] [Traduction]. Ce point doit être mentionné dans la politique de confidentialité.

Recommandation 34 : Les sites doivent informer l'utilisateur du type de renseignements agrégés qu'ils fournissent aux annonceurs.

LinkedIn offre une adresse de courriel aux utilisateurs qui veulent que leurs renseignements soient exclus des recherches agrégées ou des produits sur la base de données agrégées.

Soulignons également que hi5 affirme qu'outre le nom, l'adresse, l'adresse de courriel et le numéro de téléphone, les renseignements peuvent être dépersonnalisés, et qu'ils ne constituent plus alors des renseignements personnels et peuvent ainsi être utilisés à la discrétion du site. Compte tenu du fait que les changements technologiques risquent de pouvoir éventuellement transformer les renseignements anonymes en renseignements personnels, il est déconseillé aux sites de communiquer des renseignements anonymes à des tiers.

Recommandation 35 : On doit encourager les sites à appliquer les normes les plus élevées en matière de dépersonnalisation et de regroupement de renseignements personnels avant de communiquer ces renseignements à des tiers.

Recommandation 36 : Les renseignements anonymes non agrégés ne doivent pas être partagés avec des tiers.

Tiers
Certains sites mentionnent leurs partenaires publicitaires à leurs utilisateurs. Facebook précise que Microsoft est son partenaire exclusif pour les bannières publicitaires. La politique de confidentialité de LiveJournal comprend une section qui décrit les annonceurs associés au site et offre des adresses URL pour permettre à l'utilisateur de consulter la politique de confidentialité de ces annonceurs et de gérer ses paramètres de confidentialité en conséquence. De la même façon, MySpace offre une adresse de courriel pour s'informer au sujet des techniques et de la politique de confidentialité des annonceurs et pour refuser la collecte de renseignements personnels à des fins publicitaires.

Solutions de rechange à la publicité
Le « Mémorandum de Rome » recommande aux sites d'envisager de facturer leurs services plutôt que d'utiliser les informations de profil à des fins commerciales[155] Des sites étudiés, seul LiveJournal offre cette possibilité. Le site offre six types de comptes, y compris un compte de base sans publicité et aux fonctions limitées, un compte payant sans publicité mais aux fonctions avancées, ainsi qu'un compte Plus dont les fonctions payantes sont financées par la publicité plutôt que par l'utilisateur. Cette solution paraît intéressante à première vue, mais les sites doivent être prudents : un système qui diminue ou élimine la protection de la vie privée des gens qui ne sont pas en mesure de payer peut poser problème.

Exclusion
Des sites comme Facebook et MySpace ont différents programmes de publicité, soit les publicités directes et les publicités générales sur bannières. Ils peuvent ainsi offrir à l'utilisateur l'option d'être exclu des publicités directes (publicités sociales et Beacon pour Facebook, DirectAds pour MySpace), une stratégie qui doit être encouragée. Il ne faut cependant pas confondre l'exclusion de ces programmes et l'exclusion des publicités sur l'ensemble du site (ou l'utilisation des renseignements personnels à des fins de ciblage publicitaire).

Sur Skyrock, le seul moyen pour un utilisateur d'être exclu des publicités est de fermer son compte.

Recommandation 37 : L'utilisateur doit avoir la possibilité d'être exclu des publicités directes.

Balises Web
La politique de confidentialité de LinkedIn précise que des balises Web peuvent être placées par des annonceurs et que l'utilisateur peut choisir de ne pas les utiliser.

Recommandation 38 : La publicité sur le site ne doit pas comprendre l'utilisation de balises Web de tiers ou de méthodes de surveillance similaires.

Contribution de l'utilisateur au ciblage
Selon Grimmelmann, « en permettant à l'utilisateur de choisir la façon dont son profil sera utilisé à des fins commerciales, Facebook l'encouragerait à se forger une identité sociale »[156] [Traduction]. À l'heure actuelle, LinkedIn et LiveJournal permettent à leurs utilisateurs de choisir le type de publicités et d'offres qui les intéressent le plus. Tous les sites devraient adopter cette méthode, car non seulement elle sensibilise l'utilisateur à la présence de la publicité, mais elle fournit également aux annonceurs de l'information plus utile pour le ciblage, ce qui leur garantit l'intérêt de l'utilisateur pour certaines catégories de publicités.

Recommandation 39 : Les sites doivent envisager de faire participer l'utilisateur au processus de publicité directe.

Publicités d'engagement
Le 31 janvier 2009, Facebook annonçait la création de la nouvelle fonction Engagement Ads, qui « permettra aux multinationales de cibler ses membres de façon précise pour évaluer la popularité de nouveaux produits. Les entreprises pourront interroger les membres spécialement choisis sur des sujets aussi personnels que leur état matrimonial ou leur orientation sexuelle »[157] [Traduction]. Comme la fonction n'est pas encore mise en œuvre, il est difficile de connaître les mesures de protection de la vie privée qui seront offertes par Facebook à ce sujet. Grimmelmann fait remarquer que Facebook a tendance à lancer une fonction, puis à attendre les plaintes avant de la retirer partiellement[158]. On espère cette fois ci que Facebook avertira ses utilisateurs de l'existence du programme avant de le mettre en œuvre et qu'il leur donnera le temps de choisir s'ils veulent y participer ou non. Autrement, la participation au programme ne doit pas être automatique, et les renseignements personnels ne doivent pas, dans la mesure du possible, être communiqués aux annonceurs.

Conservation des données

De toute évidence, tous ces sites doivent recueillir et conserver certains renseignements personnels et techniques liés aux comptes. Plutôt que d'analyser les principes de chaque site, penchons-nous sur certaines questions liées à la politique de confidentialité et à la conservation des données.

Politique de confidentialité
Pour chacun des six sites, la politique de confidentialité (ou, dans le cas de Skyrock, les conditions générales d'utilisation qui incluent les conditions de protection des données) n'est pas négociable et l'inscription au site sous-entend l'acceptation des conditions. Cependant, avant l'inscription, aucune fenêtre contextuelle n'apparaît pour permettre à l'utilisateur de lire la politique de confidentialité. Tout au plus, l'utilisateur doit cocher une case pour indiquer qu'il accepte les conditions d'utilisation et la politique de confidentialité. Les sites doivent penser à mettre ces documents en premier plan.

Recommandation 40 : Les sites doivent mettre en premier plan leur politique de prestation de services afin que l'utilisateur puisse la lire avant de s'inscrire.

Objectifs de la collecte de renseignements

Jones et Soltren s'attaquent à la politique de confidentialité de Facebook en soulignant que (a) l'utilisation des renseignements recueillis n'est pas expliquée et que (b) la nature des renseignements pouvant être communiqués est définie de façon trop générale[159]. Afin d'illustrer leur point de vue, ils expliquent qu'ils ont demandé à des utilisateurs de Facebook s'ils croyaient que la politique du site autorise la communication de leurs renseignements personnels à d'autres entreprises. Ainsi, 47 % des utilisateurs croient (à tort) que Facebook ne peut pas communiquer leurs renseignements[160]. Ce problème n'est pas exclusif à Facebook. Au contraire, toutes les politiques de confidentialité sont vagues en ce qui a trait à chaque type de renseignements, à la raison de leur collecte et à la façon dont ils peuvent être utilisés ou communiqués. Tout en étant conscients que ces modèles opérationnels sont récents et appelés à changer, les sites doivent définir le plus clairement possible les objectifs de la collecte.

Recommandation 41 : Les politiques doivent définir les objectifs de la collecte de renseignements.

Recommandation 42 : Les politiques doivent décrire clairement les renseignements qui peuvent être communiqués, les destinataires éventuels et les raisons d'une telle communication.

Période de conservation

Les sites doivent explicitement définir la période de conservation des données recueillies. Bien que les politiques en place indiquent que les renseignements servent à la prestation des services, on ignore si ces renseignements seront supprimés aussitôt le compte fermé et, dans la négative, pendant combien de temps (et pourquoi) ils seront conservés avant d'être supprimés. Seul Skyrock propose une clause à cet effet, qui stipule que lorsqu'un compte est fermé, les données sont supprimées ou dépersonnalisées.

Recommandation 43 : Les politiques doivent définir explicitement la période de conservation des renseignements recueillis.

Dans sa politique, Skyrock avertit l'utilisateur que la suppression ou la dépersonnalisation des renseignements peuvent prendre jusqu'à un an pour des raisons de sécurité ou d'application de la loi, ou encore pour des raisons d'ordre juridique. Compte tenu des risques liés à la re-personnalisation de données anonymes, les sites ne doivent pas pouvoir dépersonnaliser et utiliser les renseignements personnels d'un membre qui a fermé son compte.

Recommandation 44 : La fermeture d'un compte annule le consentement à l'utilisation de renseignements personnels par le site. Les sites ne doivent pas utiliser les renseignements conservés après la fermeture d'un compte.

Accès

La collecte et la conservation de renseignements personnels soulèvent la question de l'accès, peu abordée (voire jamais) dans la politique des sites. Certains peuvent prétendre que puisque les renseignements personnels sont visibles pour l'utilisateur, le droit d'accès est respecté[161], mais ce n'est pas nécessairement le cas. En effet, comme les renseignements personnels sont recueillis par des moyens technologiques (témoins, adresses IP, navigateur) et fournis par l'utilisateur et d'autres personnes, un droit d'accès permettrait de mieux comprendre la portée des renseignements personnels recueillis et utilisés par le site.

MySpace est le seul site dont la politique traite du droit d'accès, mais il est clair que ce droit et les privilèges de modification ne s'appliquent qu'aux renseignements obligatoires pour l'inscription; ils ne concernent pas les autres informations facultatives du profil. Ce droit d'accès n'est pas suffisant. L'utilisateur doit pouvoir consulter et modifier tous ses renseignements personnels recueillis par le site.

Recommandation 45 : L'utilisateur doit pouvoir consulter et modifier tous ses renseignements personnels recueillis par un site

Sanctions

Les sanctions doivent être assez sévères pour être dissuasives. Bien que les politiques interdisent plusieurs comportements (envoi de pourriels, exploration de données, utilisation d'un moteur de balayage, utilisation de données à des fins commerciales), la violation des conditions ne fait qu'entraîner la fermeture du compte. Comme le soulignent Jones et Soltren, la perte du compte n'est pas une sanction suffisante[162], pas plus qu'elle n'est dissuasive (compte tenu du fait que seule l'adresse de courriel est utilisée pour valider le compte), puisqu'on peut simplement en ouvrir un autre.

Recommandation 46 : Les sanctions liées à la violation des conditions d'utilisation doivent être assez sévères pour être dissuasives.

Changements et avis

La plupart des politiques de confidentialité et des conditions d'utilisation exigent de l'utilisateur qu'il se tienne informé des changements aux politiques ou indiquent que le site émettra un avis public à la suite de tels changements. Ce type de consentement général est inapproprié : le consentement doit être considéré comme un processus actif et continu[163]. Par conséquent, un avis doit être publié pour chaque changement, peu importe la forme. Pour les changements secondaires, un avis public suffit, mais pour les changements qui ont des répercussions sur les conditions, un courriel ou toute autre communication privée seraient plus appropriés. De plus, comme le souligne l'EPIC, il ne suffit pas d'aviser l'utilisateur : il faut lui expliquer clairement le changement et les répercussions[164].

Recommandation 47 : Si un changement est apporté sans qu'un avis ne soit publié, le fait que l'utilisateur continue d'utiliser le site ne doit pas signifier qu'il accepte les nouvelles conditions.

Recommandation 48 : Les avis de changement doivent inclure une explication de la portée et des répercussions du changement.

Comme le souligne Grimmelmann, l'utilisateur consent aux conditions initiales (au moment de son inscription). L'introduction de nouvelles fonctions modifie le service et requiert donc un nouveau consentement[165]. Encore une fois, le fait que l'avis soit public ou privé peut dépendre de la portée du changement proposé, mais l'utilisateur doit bien sûr être avisé avant l'entrée en vigueur du changement.

Recommandation 49 : Les avis de changement aux politiques doivent être publiés avant l'entrée en vigueur du changement.

Fermeture de compte

Sur certains sites, la distinction entre la « désactivation » et la « fermeture » d'un compte est floue. Ces actions doivent être clairement différenciées et les répercussions de chacune doivent être communiquées à l'utilisateur avant qu'il prenne sa décision.

Recommandation 50 : La distinction entre la « désactivation » et la « fermeture » d'un compte doit être claire.

Désactivation

L'utilisateur doit avoir la possibilité de désactiver son compte. Actuellement, les sites indiquent que lorsqu'un compte est désactivé, les renseignements qu'il contient sont conservés mais ne sont pas visibles pour les utilisateurs du site. Les renseignements ne doivent pas être conservés indéfiniment : la période de conservation doit être clairement indiquée, et les comptes qui ne sont pas réactivés pendant cette période doivent être fermés.

Recommandation 51 : La désactivation d'un compte ne doit pas entraîner la conservation permanente des renseignements. Une période de conservation limitée doit être fixée et communiquée à l'utilisateur au moment de la désactivation.

Recommandation 52 : Un compte qui n'est pas réactivé avant la fin de la période précisée doit être fermé.

Fermeture

Selon l'ENISA, « les fournisseurs doivent offrir des moyens pratiques pour supprimer complètement les données »[166] [Traduction]. Facebook, LinkedIn et MySpace requièrent plus qu'un simple clic pour fermer un compte. Facebook et LinkedIn demandent à l'utilisateur d'envoyer une demande de fermeture par courriel (LinkedIn garantit une réponse dans les cinq jours ouvrables); MySpace permet à l'utilisateur de demander l'annulation du compte en cliquant sur un bouton, mais lui envoie ensuite la marche à suivre par courriel.

Recommandation 53 : Les sites doivent offrir à l'utilisateur des moyens pratiques pour supprimer complètement ses données.

L'inquiétude des fournisseurs concernant le fait que l'utilisateur puisse fermer son compte sur un coup de tête pour ensuite vouloir le réactiver est compréhensible. LiveJournal indique à l'utilisateur qui veut fermer son compte que ses renseignements seront conservés pendant 30 jours, après quoi ils seront supprimés de façon permanente.

Fermeture partielle

Skyrock permet à l'utilisateur de supprimer son blogue au complet ou simplement son profil. De la même façon, Facebook offre la possibilité de supprimer certaines fonctions sans toutefois fermer le compte, ce qui permet à l'utilisateur de gérer ses renseignements.

Sondages

Sur certains sites, l'utilisateur qui veut fermer son compte est redirigé vers un sondage. Il peut alors indiquer les raisons pour lesquelles il utilise actuellement le site, les autres SRS qu'il utilise, ce qui aurait pu l'inciter à rester, etc. Aucun de ces sondages n'est obligatoire pour annuler ou fermer le compte. Cependant, on ne sait pas pourquoi ces informations sont recueillies ni pendant combien de temps elles seront conservées; on ignore également si elles seront liées à des renseignements personnels de quelque manière que ce soit.

Recommandation 54 : Les informations recueillies par sondage à la fermeture d'un compte ne doivent pas être liées aux renseignements personnels de l'utilisateur.

Applications tierces

Quatre des six sites intègrent des applications tierces. Par définition, ces applications ne sont pas créées par les sites, mais plutôt par des tiers qui possèdent une licence de développement. Les sites qui utilisent des applications tierces indiquent tous dans leurs conditions d'utilisation qu'ils ne sont pas responsables des données de telles applications. Soulignons cependant que les sites ont conclu des ententes contractuelles avec les développeurs, lesquelles prévoient que les applications sont accessibles par le site et qu'il y a échange de renseignements entre le site et les applications.

Recommandation 55 : Les sites qui concluent des ententes avec des développeurs tiers doivent établir des exigences claires (contractuelles ou autres) qui imposent aux développeurs d'offrir le niveau approprié de protection des renseignements personnels.

Comme le souligne Joinson, « de nombreuses applications ont un but social (se comparer aux autres, poser des questions à ses amis, voir le profil de ses voisins, etc.) et contournent souvent certains paramètres de confidentialité par défaut »[167] [Traduction]. C'est pourquoi elles suscitent des inquiétudes au sujet de la confidentialité.

Clarté

Les sites doivent expliquer clairement les principes et les procédures relativement aux applications tierces, en plus de préciser le type de renseignements personnels qui sont communiqués aux développeurs tiers.

Recommandation 56 : Les politiques doivent définir clairement le type de renseignements personnels qui sont communiqués aux développeurs tiers.

Recommandation 57 : Les politiques doivent définir clairement les principes et les procédures relativement aux développeurs tiers.

Mesures

Lorsqu'un utilisateur ajoute une application tierce, il doit accepter de communiquer ses renseignements. Pour le moment, un énoncé général explique à l'utilisateur quels renseignements peuvent être communiqués. Par contre, « comme ces conditions de service sont présentées dans chacune des applications et que la majorité des applications ne semblent pas utiliser de renseignements personnels, l'avertissement devient inutile »[168] [Traduction]. Dans la mesure du possible, chaque développeur doit obtenir le consentement à l'échange de renseignements avant l'ajout de l'application.

Recommandation 58 : Chaque développeur tiers doit expliquer les modalités d'échange de renseignements et obtenir le consentement de l'utilisateur avant l'ajout de l'application.

Recommandation 59 : Avant de pouvoir accéder à une application tierce, l'utilisateur doit consentir à communiquer ses renseignements à l'application.

Recommandation 60 : Les développeurs tiers ne doivent ni exiger ni recueillir des renseignements qui ne sont pas nécessaires à l'application.

LinkedIn définit deux types d'applications tierces, soit celles créées par des développeurs et celles créées par un sous-ensemble de développeurs, appelés « partenaires ». Même si l'utilisateur ajoute des applications de partenaires à ses propres risques et périls, LinkedIn souligne que les partenaires sont soumis à un certain contrôle et que, par conséquent, le consentement à l'échange des renseignements requis peut être envisagé. Cela pose un problème, car lorsque des renseignements personnels sont transmis à des tiers, le consentement doit être explicite et non implicite.

Recommandation 61 : Le consentement à l'échange de renseignements personnels avec des applications tierces doit être un processus actif et explicite, et non implicite.

Comme il a été mentionné à la section sur les mesures de protection de la vie privée, l'utilisateur doit avoir la possibilité de contrôler le niveau d'échange de ses renseignements personnels avec des applications tierces. Facebook permet à l'utilisateur de gérer le type de renseignements qui sont vus par ses amis lorsqu'il utilise des applications non communes. De plus, l'utilisateur peut refuser l'échange de renseignements avec des applications, mais seulement s'il n'utilise aucune application. Cela ne dissipe évidemment pas les inquiétudes soulevées par de nombreuses personnes, à savoir que les applications tierces peuvent accéder non seulement aux renseignements personnels de l'utilisateur qui se sert de l'application, mais aussi des amis de cet utilisateur. Certains voient donc leurs renseignements transmis à des applications à leur insu ou sans leur consentement explicite. Les mesures de protection de la vie privée de MySpace, en revanche, permettent à l'utilisateur de régler les paramètres de confidentialité de ses renseignements relativement à l'utilisation des applications par ses amis, lui permettant ainsi de ne communiquer aucun renseignement, de ne communiquer que des renseignements généraux, ou de communiquer tous ses renseignements publics. On doit encourager les sites à adopter le modèle de MySpace, ce qui protégerait davantage l'utilisateur contre l'échange non autorisé de ses renseignements personnels avec les applications.

Recommandation 62 : Les mesures de protection de la vie privée doivent permettre à l'utilisateur de contrôler le niveau d'échange de ses renseignements personnels avec des applications tierces, autant lorsqu'il accède lui-même à l'application que lorsque ses amis y accèdent.

Mise en application

Bien que les sites qui intègrent des applications tierces régissent les activités des développeurs grâce à un contrat de licence, les conditions d'utilisation de ces sites indiquent également que ces derniers ne sont pas responsables des applications tierces et que l'utilisateur qui accède au contenu de tiers le fait à ses propres risques et périls. Selon Felt et Evans, « les politiques de confidentialité doivent être mises en application par la plateforme et viser toutes les données fournies au site de réseau social »[169] [Traduction].

Rappelons que Facebook a récemment adopté une position plus proactive, en annonçant le resserrement de ses mesures de surveillance des demandes de renseignements personnels par les applications tierces, ainsi que le développement d'un programme de validation des applications maison qui garantira que seules les données pertinentes sont recueillies. On doit encourager les sites à adopter ce genre de mesures.

Recommandation 63 : Les sites doivent mettre en application les conditions de leurs contrats avec des développeurs tiers, surtout en ce qui a trait à la collecte, à l'utilisation et à la conservation des renseignements personnels de l'utilisateur.

Recommandation 64 : La politique de confidentialité doit être mise en application par le site et viser toutes les données fournies au site.

Réduction du niveau d'échange au minimum

Après avoir analysé 150 applications de Facebook, Felt et Evans en sont venus à la conclusion suivante : « presque toutes les applications peuvent continuer de fonctionner en utilisant une interface limitée qui n'offre l'accès qu'à un graphe social anonyme et aux signets des données de l'utilisateur »[170] [Traduction]. On doit encourager les sites à étudier la théorie de confidentialité par serveur mandataire (« privacy-by-proxy ») proposée par Felt et Evans, et à travailler avec les développeurs afin

de réduire au minimum l'échange des renseignements requis pour le fonctionnement des applications.

La plateforme de développement MySpace permet aux développeurs d'accéder aux renseignements publics seulement. Ainsi, ils ne peuvent pas consulter les renseignements que l'utilisateur désigne comme privés. Cette mesure appuie les conclusions de Felt et Evans, qui soutiennent que « les applications n'ont pas besoin de tous les renseignements personnels qu'elles collectent. Bien que les deux-tiers des applications dépendent des renseignements publics d'amis, rares sont celles qui nécessitent un accès aux renseignements confidentiels »[171] [Traduction]. En s'engageant à réduire l'échange de renseignements avec les applications tierces, les sites doivent travailler avec les développeurs afin que, dans la mesure du possible, seuls les renseignements publics soient requis pour faire fonctionner les applications.

Recommandation 65 : Les sites doivent travailler avec les développeurs tiers à réduire au minimum l'échange des renseignements requis pour le fonctionnement des applications.

Recommandation 66 : Les sites doivent travailler avec les développeurs tiers afin que, dans la mesure du possible, seuls les renseignements publics soient requis pour faire fonctionner les applications.

Collecte des renseignements personnels des non membres

Utilisateurs

Le « Mémorandum de Rome » recommande aux fournisseurs d'informer les utilisateurs de ce qu'ils doivent faire et ne pas faire concernant les renseignements de tiers dans leur profil (p. ex. le moment opportun pour demander le consentement de la personne concernée et les conséquences possibles du non-respect des règles)[172]. Actuellement, même si l'utilisateur doit confirmer qu'il est autorisé à télécharger du contenu (comme une photo sur laquelle apparaît une autre personne), il ignore pourquoi il doit faire preuve de prudence, quelles sont les pratiques exemplaires à adopter et quelles sont les sanctions en cas d'infraction.

Recommandations 67 : Les sites doivent fournir à l'utilisateur des directives claires sur la gestion des renseignements de tiers dans son profil.

Collecte et conservation

Chacun des sites permet à l'utilisateur de rechercher une personne par adresse de courriel et, par conséquent, peut recueillir l'adresse de courriel des non-membres. À l'exception de LiveJournal, tous les sites recueillent les adresses de courriel pour inviter les non-membres sur le site. LinkedIn permet à ses utilisateurs d'ajouter des non-membres à leur liste de relations. Facebook, hi5, MySpace et Skyrock permettent à l'utilisateur de marquer un non-membre dans une photo et de fournir son adresse de courriel. Comme le fait remarquer Grimmelmann, « les personnes qui décident de ne pas se joindre à Facebook indiquent clairement qu'elles préfèrent garder leurs renseignements confidentiels, et ce choix doit être honoré »[173] [Traduction]. Les sites doivent tenir compte de cette réalité et ne pas conserver les renseignements personnels des non-membres, par exemple lorsque l'utilisateur fournit l'adresse de courriel d'un non-membre pour lui permettre de recevoir des communications.

Recommandation 68 : Les sites ne doivent ni recueillir ni conserver les renseignements personnels des non-membres.

Suppression

Seules les politiques de Facebook et de hi5 indiquent aux non-membres comment ils peuvent exiger que leurs renseignements personnels soient supprimés du site. Un site qui recueille les renseignements personnels des non-membres doit leur offrir la possibilité de supprimer leurs renseignements de la base de données.

Recommandation 69 : Les sites qui recueillent les renseignements personnels des non-membres doivent clairement leur indiquer la marche à suivre pour demander la suppression de leurs renseignements du site.

Avis

Même si un non-membre peut demander la suppression de ses renseignements personnels d'un site, il paraît déraisonnable de s'attendre à ce qu'il surveille les SRS afin de savoir si ses renseignements ont été recueillis. D'après Grimmelmann, chacun des sites doit « offrir au non-membre cette option de suppression dès qu'il a assez de renseignements sur lui (p. ex. adresse de courriel et identifiant de messagerie instantanée), et éliminer de ses serveurs tout autre renseignement lié à l'adresse de courriel de cette personne »[174] [Traduction].

Recommandation 70 : Lorsqu'un site recueille les renseignements personnels d'un non membre, il doit l'en informer automatiquement et lui offrir la possibilité de supprimer ses renseignements du site.

Recommandation 71 : Lorsqu'un non membre demande la suppression de ses renseignements personnels, tout renseignement lié à cette personne doit être supprimé du site.

E: CONCLUSION

La principale observation de Nissenbaum est la suivante : « il n'existe aucune sphère de la vie qui ne soit pas régie par des normes sur la circulation des renseignements ni aucun renseignement pour lequel tout est permis »[175] [Traduction]. En ce sens, toute violation par rapport aux conventions et aux attentes dans un contexte précis serait perçue comme une violation de la protection des renseignements personnels par les personnes qui s'inscrivent dans ce contexte. L'auteure mentionne deux normes différentes dont la violation constituerait une atteinte à la vie privée : la norme sur la pertinence des renseignements recueillis et la norme sur la circulation et la communication des renseignements. Fait intéressant, les exemples qu'elle a utilisés dans son article original concordent avec les questions liées à la confidentialité sur les SRS.

Premièrement, Nissenbaum suggère que d'« utiliser les renseignements recueillis dans un contexte donné pour les placer dans un contexte différent »[176] [Traduction] constitue une violation de la norme sur la pertinence des renseignements.

Deuxièmement, en ce qui à trait à la circulation des renseignements, « la confidentialité est généralement requise par défaut, c'est-à-dire qu'une personne s'attend à ce que les propos qu'elle échange avec ses amis restent confidentiels et ne soient pas transmis de façon arbitraire »[177] [Traduction].

Les problèmes liés à la confidentialité sur les SRS découlent souvent d'un écart entre la compréhension qu'a l'utilisateur du contexte et la portée réelle des renseignements qui circulent à l'intérieur et à l'extérieur des SRS. L'utilisateur peut avoir l'impression que ses renseignements personnels ont été mal utilisés ou mal distribués lorsqu'ils sont divulgués à des fins publicitaires, lorsqu'ils sont indexés par les moteurs de recherche publique ou lorsqu'ils ont des répercussions sur un public plus large que celui perçu par l'utilisateur. Un SRS qui souhaite offrir des mesures concrètes de protection de la vie privée doit évaluer et comprendre les attentes de ses utilisateurs. Lorsque leur modèle opérationnel l'exige, les sites doivent également fournir à l'utilisateur des explications précises sur leurs pratiques pour lui permettre de mieux comprendre le contexte dans lequel il interagit.

Matthew Hodge souligne un fait intéressant concernant le caractère privé des renseignements sur un SRS, espace en apparence public. Il compare les SRS à un coffret de sûreté dans une banque publique ou à un local de stockage public[178]. Dans cette optique, le fait de vouloir protéger le caractère privé en demandant à l'utilisateur de reconnaître le caractère public des coffrets de sûreté et des locaux de stockage pose évidemment problème. Au lieu d'insister sur le caractère public de l'espace, on cherche à le rendre privé en offrant des outils comme des serrures de porte, des mots de passe et des espaces plus petits au sein des grands espaces publics.

De la même façon, pour garantir la confidentialité sur un SRS, on doit fournir à ses utilisateurs les outils qui leur permettront non seulement de comprendre le contexte dans lequel circulent leurs renseignements (en énonçant clairement les principes et en situant le contexte global de l'échange de renseignements), mais aussi de définir le niveau d'échange approprié et les mesures qui assureront un tel niveau de protection. Il ne s'agit pas d'un processus global : les ententes et les mesures de protection de la vie privée ne prennent toute leur importance que lorsqu'elles sont établies en fonction de chaque site, puis intégrées aux pratiques habituelles de ces espaces.

F: NOTES EN BAS DE PAGE

1 danah boyd and Nicole Ellison. (2007). Social Network Sites: Definition, History, and Scholarship. JCMC, 13 (1). [Special Issue of JCMC on Social Network Sites, Eds.: danah boyd and Nicole Ellison.]

2 boyd & Ellison supra note 1 at 2

3 Alexa Top 100 Sites in Canada. Shows Facebook at #3, MySpace at #15, Skyrock at #44 and LiveJournal at #89.

4 European Union (2009) Press Release: Social Networking: Commission brokers agreement among major web companies. 10 February 2009

5 European Union (2009) Safer Social Networking: The Choice of Self-Regulation

6 See for example Steeves, Valerie (2004). Young Canadians in a Wired World, Phase II – Trends and Recommendations. Ottawa: Media Awareness Network; Livingstone, Sonia and Magdalena Bober. (2003). UK Children Go Online: Listening to Young People's Experiences. London: Economic and Social Research Council; Livingstone, Sonia & Magdalena Bober. (2003). Children's Use of the Internet: Reflections on the Emerging Research Agenda. New Media & Society 5(2): 147-166; Livingstone & Bober (2004). UK Children Go Online: Surveying the Experiences of Young People and their Parents. London: Economic and Social Research Council ; and Sonia Livingstone (2006). Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. Computers, Phones, and the Internet: Domesticating Information Technology. Eds. Kraut, R. E., M. Brynin and S. Kiesler. New York: Oxford University Press.

7 Adam Thierer (2007) Social Networking and Age Verification: Many Hard Questions; No Easy Solutions Progress & Freedom Foundation Progress on Point Paper No. 14.5

8 Ralph Gross and Alessandro Acquisti. (2005). Information Revelation and Privacy in Online Social Networks. Proceedings of WPES'05 (pp. 71-80). Alexandria, VA: Association of Computing Machinery. [Gross & Acquisti] at 9

9 Catherine Dwyer, Starr Roxanne Hiltz and Katia Passerini (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of AMCIS 2007, Keystone, CO. at 4

10 James Grimmelmann. (in review). "Facebook and the Social Dynamics of Privacy." at 43

11 Helen F. Nissenbaum (2004) Privacy as Contextual Integrity. Washington Law Review, Vol. 79, No. 1 at 137.

12 Grimmelmann supra note 10 at 2

13 Privacy International Social Network Sites and Virtual Communities 18 December 2007. Accessed 29 March 2008.

14 danah boyd (2007) "Social Network Sites: Public, Private or What?" Knowledge Tree 13 May. Accessed 1 February 2009. http://www.danah.org/papers/KnowledgeTree.pdf

15 Anders Albrechtlund (2008). Online Social Networking as Participatory Surveillance. First Monday 13 (3).

16 Alessandro Acquisti & Ralph Gross (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In P. Golle & G. Danezis (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36-58). Cambridge, U.K: Robinson College, June 28-30. at 10.

17 danah boyd (2008). Taken Out of Context: American Teen Sociality in Networked Publics. University of California-Berkeley Dissertation at 159 [boyd 2008]

18 boyd 2008 supra note 17 at 144

19 Susan B. Barnes (2006). A privacy paradox: Social networking in the United States. First Monday 11 (9), July 2006.

20 Adam N. Joinson (2008). Looking at, looking up or keeping up with people? Motives and use of Facebook. SIGCHI 2008, 1027-1036.

21 Catherine Dwyer et al supra note 9 at 2

22 Sören Preibusch, Bettina Hoser, Seda Gürses, & Bettina Berendt. (2007). Ubiquitous social networks ? opportunities and challenges for privacy-aware user modelling. Proceedings of the Workshop on Data Mining for User Modelling at UM 2007, Corfu, Greece, June 2007 p 4.

23 This is not to say that SNS' do not have the requisite privacy and data protection mechanisms incorporated into the sites. Rather, it seeks to recognize that the interests of the user in her privacy may not mirror those of the administrator and accordingly that this privacy analysis must go beyond existing controls to identify

what issues users are experiencing and how best to enable them to control their personal privacy.

24 Facebook Statistics

25 Crunch Base Company Profile: Facebook.com

26 Crunch Base profile supra note 25

27 Spencer E. Ante (5 August 2008) Has Facebook's Value Taken a Hit? Business Week

28 Michael Arrington (December 2008) Interview with Mark Zuckerberg Crunch Bas

29 Facebook Statistics supra note 24

30 Sharon Gaudin (26 January 2009) Internet Hits Major Milestone Surpassing 1 Billion Monthly Users ComputerWorld

31 Facebook Statistics supra note 24

32 Jeremiah Owyang (9 January 2008) Social Network Stats: Facebook, MySpace, Reunion Web Strategy by Jeremiah

33 Facebook Terms of Use

34 Facebook Privacy Controls

35 Facebook Privacy Policy

36 Facebook Privacy Controls: Social Ads

37 Facebook Statistics supra note 24

38 Facebook Statistics supra note 24

39 Facebook Advertising

40 Security analysis suggests that Facebook user opt-out of Beacon does not prevent the advertisers from collecting the information and sending it to Facebook – rather, it prevents the information, once received, from being sent to Feeds if the user has not opted in. With this control taking place at the Facebook level rather than the 3d party level, this means essentially that advertisers are collecting and transmitting to Facebook the information of all users of their sites, regardless of whether they have opted out of Beacon, deleted or deactivated their Facebook accounts, or are not and never have been Facebook users. Facebook claims that if it is unable to associate data it receives with a Facebook member, the data is deleted. The question of the collection of the data and its transmission to Facebook remains an issue, however, and the design of Beacon and the activities of those 2d parties who integrate the program onto their sites are ripe for further privacy examination. See (3 December 2007) Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking Users Who Opt Out of Are Not Logged In CA Security Advisor Research Blog.

41 Facebook Privacy Policy supra note 35

42 The standard template asks a user whether they will allow the application to: know who they are and access their information; put a box in their Facebook profile; place a link in the left-hand navigation menu of their account; publish stories in their News Feed and Mini-Feed; and place a link below the profile picture on any profile. The options are all pre-selected, though the user may de-select any of them. Failure to agree to the Application knowing who they are and accessing their information will, however, result in a notice that the Application is unable to be installed without this permission.

43 Facebook Application Terms of Use.

44 EPIC: Facebook Privacy .

45 Facebook Developer Terms of Service.

46 David George-Cosh (28 January 2009) We're Worried About Canadian Spammers: Q&A with Facebook's Privacy Chief Chris Kelly National Post.

47 Srarama Mitra (8 June 2008) Social Networking Without Boundaries: hi5 CEO Ramu Yalamanchi

48 Hi5 Timeline

49 Interview with Ramu Yalamanchi supra note 47

50 Interview with Ramu Yalamanchi supra note 47

51 Erick Schonfeld (10 December 2008) Hi5 Hopes to Make Real Coin with Virtual Gifts TechCrunch

52 Hi5 Advertise

53 Press Release (23 July 2008) Hi5 Is Fastest Growing Social Network in the World for the First Half of 2008

54 Hi5 Timeline supra note 48

55 Interview with Ramu Yalamanchi supra note 47

56 Social Media Statistics: Hi5

57 Quantcast: Hi5 Network

58 Site Analytics: Hi5.com

59 Traffic Rankings: Hi5.com

60 Hi5 FAQ: Advertising

61 Hi5 Advertise

62 Hi5 Privacy Policy

63 Hi5 Privacy Policy supra note 62

64 Hi5 Privacy Policy supra note 62

65 Hi5 Privacy Policy supra note 62

66 Hi5 Timeline supra note 48

67 Hi5 Terms of Service

68 Hi5 Developer Platform: Hi5 Platform Terms and Conditions

69 Hi5 Privacy Policy supra note 62

70 Hi5 Timeline supra note 48

71 LinkedIn User Agreement at cl. 3

72 CrunchBase LinkedIn.com Profile

73 LinkedIn Company History

74 LinkedIn Company History supra note 73

75 Alexa Traffic Rankings: LinkedIn.com

76 Site Analytics: LinkedIn.com

77 LinkedIn Demographic Data June 08

78 LinkedIn About Us

79 Joop Dorresteijn (16 July 2008) LinkedIn Introduces Targeted Advertising The Next Web.

80 The beta page for DirectAds can be found at https://www.linkedin.com/directads/start.

81 LinkedIn: Advertising: Precision Targeting

82 LinkedIn Privacy Policy

83 LinkedIn Privacy Policy supra note 82

84 LinkedIn Privacy Policy supra note 82

85 LiveJournal Our Company

86 LiveJournal Code

87 Robert Amsterdam (Dec 2007) SUP's Shenderovich Talks About LiveJournal Purchase
88 LiveJournal About Us supra note 85
89 Alexa Traffic Rankings: LiveJournal.com
90 LiveJournal Statistics
91 Quantcast Audience Profile: LiveJournal.com
92 LiveJournal FAQ #24
93 LiveJournal FAQ #262
94 Social Network Stats supra note 32
95 CrunchBase Profile: MySpace.com
96 Tom Anderson MySpace History FreeMySpace
97 MySpace Help: Is MySpace Free?
98 Erick Schonfeld (8 September 2008) TC50: MySpace CEO Chris DeWolfe Says 95% of Ad Revenues Comes From 9 Countries, Announces New Google Gears Project TechCrunch
99 Jordan McCollum (6 November 2008) MySpace Revenue Up, New Ads Up Even More Marketing Pilgrim
100 Alexa Traffic Details: MySpace.com
101 Site Analytics: MySpace.com
102 MySpace Canada Advertising
103 MySpace Termscl.1
104 MySpace FAQ: MyAds MySpace Online Advertising
105 MySpace Terms supra note 103
106 Associated Press (5 February 2008) MySpace Opens Up To Third Party Applications Marketing Mag.ca. See also Associated Press (5 February 2008) MySpace To Launch Third Party Applications CTV
107 Michael Arrington (14 September 2008) MySpace Music Already Has Revenue Locked, May Raise Outside Capital at $2 Billion Valuation TechCrunch
108 MySpace Terms supra note 103
109 MySpace Privacy Policy
110 Skyrock Terms of Service
111 Robert Andrews (26 October 2008) Skyrock.com's Sale Hampered By Crunch, Confident Will Survive "Dark Days" paidContent: UK
112 Skyrock Terms of Service supra note 110, s. 8 Legal Information
113 CrunchBase Company Profile: Skyrock.com
114 Skyrock Sale Hampered by Crunch supra note 111
115 AXA Private Equity: Investors Details Page: LBO SmallCap Investments: Skyrock
116 Robert Andrews (10 June 2008) Skyrock.com Seeking Sale To Big Telco Player, Talks Ongoing paidContent: UK
117 Alexa Traffic Details: Skyrock.com
118 Site Analytics: Skyrock.com
119 Jean Yves Chainon (20 February 2008) From Traditional to Digital: Skyrock Blogs Phenomenal Transition Editors Weblog.org
120 Skyrock Terms of Service supra note 110 at 1a.
121 From Traditional to Digital supra note 119
122 International Working Group on Data Protection in Telecommunications (3/4 March 2008) Report and Guidance on Privacy in Social Network Services (Rome (Italy) [Rome Memorandum]
123 Barnes supra note 19
124 CAPTCHA: Telling Humans and Computers Apart Automatically
125 European Network and Information Security Agency ENISA Position Paper No. 1 (2007) Security Issues and Recommendations for Online Social Networks ed. Giles Hogben [ENISA] Recc SN.5 p 4
126 Rome Memorandum supra note 122 at 5
127 UK Office of Communications (2008) Social Networking: A Quantitative and Qualitative Research Report Into Attitudes, Behaviours and Use at 55.
128 Anne Hewitt and Andrea Forte. (2006). Crossing Boundaries: Identity Management and Student/Faculty Relationships on the Facebook. Poster presented at CSCW, Banff, Alberta at 2.
129 Ralph Gross and Alessandro Acquisti supra note 8 at 7. See also W. MacKay Triggers and Barriers to Customizing Software In Proceedings of CHI 91 ACM Press 1991 153-160.
130 ENISA supra note 125 Recc. SN.8, p 5.
131 Harvey Jones and Jose Hiram Soltren. (2005). Facebook: Threats to Privacy. MIT 6.805/STS085 at 31.
132 ENISA supra note 125 Recc. SN.1. p 4.
133 Rome Memorandum supra note 122 at 5
134 Rome Memorandum supra note 122 at 6
135 Patricia G. Lange (2007). Publicly Private and Privately Public: Social Networking on YouTube. JCMC, 13 (1). [Special Issue of JCMC on Social Network Sites, Eds.: danah boyd and Nicole Ellison.] at 6.
136 boyd 2008 supra note 17 at 165
137 Rome Memorandum supra note 122 at 6
138 ENISA supra note 125 Recc. SN.12 at 5
139 Grimmelmann supra note 10 at 46
140 Jones & Soltren supra note 131 at 34
141 Joinson supra note 20 at 2
142 Sören Preibusch et al supra note 22 at 4
143 Rome Memorandum supra note 122 at 6.
144 Monica Chew, Dirk Balfanz, and Ben Laurie. (2008). (Under)mining Privacy in Social Networks. at 11
145 Chew et al supra note 144 at 3
146 Rome Memorandum supra note 122 at 6
147 boyd 2008 supra note 17 at 161
148 Rome Memorandum supra note 122 at 6
149 ENISA supra note 125 Recc. SN. 14 at 5
150 Matthew J. Hodge (2006). The Fourth Amendment and privacy issues on the "new" internet: Facebook.com and MySpace.com. Southern Illinois University Law Journal, 31 at 118.
151 Sören Preibusch et al supra note 22 at 2.
152 Jones & Soltren supra note 131 at 23
153 Rome Memorandum supra note 122 at 6
154 EPIC Social Networking Privacy p 6.
155 Rome Memorandum supra note 122 at 6
156 Grimmelmann supra note 10 at 46
157 Rupert Neate and Rowena Mason Networking Site Cashes In On Friends: Facebook founder finally finds a way to profit from its 150m members' private data. Telegraph newspaper 31 January 2009.

158 Grimmelmann supra note 10 at 35
159 Jones & Soltren supra note 131 at 23
160 Jones & Soltren supra note 131 at 21
161 Jones & Soltren supra note 131 at 24
162 Jones & Soltren supra note 131 at 26
163 Jennifer Barrigar, Jacquelyn Burkell, Ian Kerr. (2006) Let's Not Get Psyched out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information 44 C.B.L.J. 54.
164 EPIC supra note 154 at 5
165 Grimmelmann supra note 10 at 48
166 ENISA supra note 125 Recc SN.9 at 5
167 Joinson supra note 20 at 9
168 Adrienne Felt & David Evans (2008) Privacy Protection for Social Networking APIs W2SP '08. at 3
169 Felt & Evans supra note 168 at 3
170 Felt & Evans supra note 168 at1
171 Felt & Evans supra note 168 at 4
172 Rome Memorandum supra note 122 at 5
173 Grimmelmann supra note 10 at 46
174 Grimmelmann supra note 10 at 47
175 Nissenbaum supra note 11 at 137
176 Nissenbaum supra note 11 at 140
177 Nissenbaum supra note 11 at 141
178 Hodge supra note 150 at 121