



**CHAMBRE DES COMMUNES  
CANADA**

**LA PROTECTION DE LA VIE PRIVÉE DANS LE  
MONDE NUMÉRIQUE : ÉTUDE DES  
RÉPERCUSSIONS SUR LA VIE PRIVÉE DES  
SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE**

**Rapport du Comité permanent  
de l'accès à l'information, de la protection des  
renseignements personnels et de l'éthique**

**Le président**

**L' hon. Shawn Murphy, C.P., député**

**JANVIER 2011**

**40<sup>e</sup> LÉGISLATURE, 3<sup>e</sup> SESSION**

---

Publié en conformité de l'autorité du Président de la Chambre des communes

### **PERMISSION DU PRÉSIDENT**

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

On peut obtenir des copies supplémentaires en écrivant à :  
Les Éditions et Services de dépôt Travaux publics et Services gouvernementaux Canada  
Ottawa (Ontario) K1A 0S5  
Téléphone : 613-941-5995 ou 1-800-635-7943  
Télécopieur : 613-954-5779 ou 1-800-565-7757  
publications@tpsgc-pwgsc.gc.ca  
<http://publications.gc.ca>

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : <http://www.parl.gc.ca>

**LA PROTECTION DE LA VIE PRIVÉE DANS LE  
MONDE NUMÉRIQUE : ÉTUDE DES  
RÉPERCUSSIONS SUR LA VIE PRIVÉE DES  
SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE**

**Rapport du Comité permanent  
de l'accès à l'information, de la protection des  
renseignements personnels et de l'éthique**

**Le président**

**L' hon. Shawn Murphy, C.P., député**

**JANVIER 2011**

**40<sup>e</sup> LÉGISLATURE, 3<sup>e</sup> SESSION**



# **COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE**

## **PRÉSIDENT**

L'hon. Shawn Murphy

## **VICE-PRÉSIDENTS**

Patricia Davidson

Bill Siksay

## **MEMBRES**

Harold Albrecht

Kelly Block

L'hon. Wayne Easter

Pierre Poilievre

L'hon. Carolyn Bennett

Paul Calandra

Carole Freeman

Ève-Mary Thאי Thi Lac

## **AUTRES DÉPUTÉS QUI ONT PARTICIPÉ**

Bob Dechert

Jean Dorion

Judy Foote

Greg Rickford

Paul Szabo

Luc Desnoyers

Earl Dreeshen

Russ Hiebert

Michelle Simson

Boris Wrzesnewskyj

## **GREFFIER DU COMITÉ**

Chad Mariage

## **BIBLIOTHÈQUE DU PARLEMENT**

### **Service d'information et de recherche parlementaires**

Alysia Davies, analyste

Élise Hurtubise-Loranger, analyste

Dara Lithwick, analyste



# **LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE**

a l'honneur de présenter son

## **ONZIÈME RAPPORT**

Conformément au mandat que lui confère l'article 108(3)*h*(vi) du Règlement, le Comité a étudié la question des répercussions sur la vie privée des systèmes d'imagerie à l'échelle de la rue et a convenu de faire rapport de ce qui suit :





# TABLE DES MATIÈRES

---

LA PROTECTION DE LA VIE PRIVÉE DANS LE MONDE NUMÉRIQUE : ÉTUDE DES RÉPERCUSSIONS SUR LA VIE PRIVÉE DES SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE .....	1
CONTEXTE .....	1
A. L'étude du Comité .....	1
B. La protection des renseignements personnels au Canada .....	2
C. Street View de Google .....	3
1. Le service .....	3
2. Protection de la vie privée .....	5
3. Collecte, par Google, de données utiles dans des réseaux Wi-Fi non protégés et conclusions préliminaires du Commissariat à la protection de la vie privée .....	6
D. Scène de rues de Canpages.....	8
1. Le service .....	8
2. Politique de confidentialité.....	9
3. Canada Eye.....	10
CE QUE LE COMITÉ A ENTENDU : PREMIERS TÉMOIGNAGES — LES APPLICATIONS D'IMAGERIE À L'ÉCHELLE DE LA RUE DE GOOGLE ET DE CANPAGES.....	11
A. Google Canada .....	11
B. Canpages.....	13
C. Commissariat à la protection de la vie privée du Canada .....	14
CE QUE LE COMITÉ A ENTENDU : SUITE DES TÉMOIGNAGES — COLLECTE DE DONNÉES WI-FI PAR GOOGLE .....	16
A. Commissariat à la protection de la vie privée du Canada .....	16
B. Google Canada .....	20
1. Audition de Jacob Glick le 4 novembre 2010 .....	20
2. Audition de Jacob Glick et Alma Whitten le 25 novembre 2010 (par téléconférence) .....	22
C. Groupe Pages jaunes (Canpages).....	26
CONCLUSION.....	28
LISTE DES RECOMMANDATIONS.....	31
ANNEXE A — VOUS ÊTES PHOTOGRAPHIÉS .....	33

ANNEXE B — LETTRE DE CONCLUSIONS PRÉLIMINAIRE .....	37
ANNEXE C	
LISTE DES TÉMOINS, DEUXIÈME SESSION, 40 <sup>E</sup> LÉGISLATURE.....	51
LISTE DES TÉMOINS, TROISIÈME SESSION, 40 <sup>E</sup> LÉGISLATURE.....	51
ANNEXE D — LISTE DES MÉMOIRES, DEUXIÈME SESSION, 40 <sup>E</sup> LÉGISLATURE .	53
PROCÈS-VERBAUX.....	55

# LA PROTECTION DE LA VIE PRIVÉE DANS LE MONDE NUMÉRIQUE : ÉTUDE DES RÉPERCUSSIONS SUR LA VIE PRIVÉE DES SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE

---

## CONTEXTE

### A. L'étude du Comité

Le 27 avril 2009, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ci-après le Comité) a adopté la motion suivante :

Que, le comité étudie les répercussions qu'ont sur la vie privée les systèmes de caméras de surveillance comme les applications « Street View » de Google et Canpages et d'autres questions liées à la surveillance vidéo et que le comité demande à Eric Schmidt, président-directeur général de Google, ou à une personne le représentant au Canada, et à Olivier Vincent, président-directeur général de Canpages, ou à une personne le représentant, de témoigner à ce sujet devant ses membres.

L'étude du Comité a porté sur la technologie de l'imagerie à l'échelle de la rue, qui a recours à divers moyens pour photographier les paysages de rue. Généralement, on utilise une caméra montée sur un véhicule qui sillonne les rues des villes choisies. Les images peuvent ensuite être visionnées sur Internet.

Le Comité a recueilli les témoignages de Jonathan Lister, directeur général et chef de Google Canada, et d'Olivier Vincent, président-directeur général de Canpages, le 17 juin 2009, ainsi que d'Elizabeth Denham, commissaire adjointe fédérale à la protection de la vie privée, le 22 octobre 2009.

On a découvert en mai 2010 que des véhicules Street View de Google avaient recueilli des données utiles à partir de réseaux sans fil non protégés pendant leur collecte de données Wi-Fi. Au terme de l'enquête faite ultérieurement par le Commissariat à la protection de la vie privée sur les manquements aux règles de protection de la vie privée qu'a pu entraîner la collecte de données Wi-Fi, le Comité a entendu le témoignage du Commissariat le 28 octobre 2010 et celui de Jacob Glick, conseiller en matière de politique au Canada chez Google, le 4 novembre 2010. Le 25 novembre 2010, le Comité a de nouveau entendu M. Glick, ainsi que la nouvelle directrice de la protection de la vie privée chez Google, Alma Whitten, par téléconférence, de même que François D. Ramsay, premier vice-président, conseiller juridique principal, secrétaire et responsable du respect de la vie privée et Martin Aubut, premier directeur, Commerce social, tous deux du Groupe Pages jaunes (Canpages).

Bien que l'étude du Comité ait pour thème les répercussions des systèmes d'imagerie à l'échelle de la rue sur la vie privée, le cas des données Wi-Fi de Google

soulève des préoccupations nouvelles qui touchent la nécessité pour les concepteurs de technologies comme Google de prendre des mesures pour bien protéger la vie privée des citoyens dans l'élaboration de nouveaux produits.

## **B. La protection des renseignements personnels au Canada**

La collecte, l'usage et la communication de renseignements personnels par les entreprises au Canada sont régis par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cependant, dans les provinces qui ont adopté leur propre loi « essentiellement similaire » à la loi fédérale, les organismes régis par la loi provinciale sont soustraits à l'application de la loi fédérale. Ainsi, en Colombie-Britannique, ce genre d'activité est régi par la *Personal Information Protection Act*, en Alberta par la *Personal Information Protection Act*, et au Québec par la *Loi sur la protection des renseignements personnels dans le secteur privé*<sup>1</sup>.

En avril 2009, la commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, a envoyé au Comité une lettre accompagnée d'une fiche d'information produite par son bureau et intitulée « Vous êtes photographié — La technologie de l'imagerie à l'échelle de la rue, Internet et vous<sup>2</sup> » (annexe A). La fiche d'information fait part de certaines préoccupations en matière de protection de la vie privée soulevées par la commissaire et ses homologues provinciaux en ce qui concerne les applications de l'imagerie à l'échelle de la rue :

Les commissaires à la protection de la vie privée ont tenu des discussions avec diverses entreprises pour renforcer les mécanismes de protection des personnes dont la photo a été prise. Nous croyons que toutes les entreprises qui offrent de telles applications doivent prendre des mesures pour mieux protéger votre vie privée.

En plus de demander aux entreprises d'être plus proactives et originales dans leurs communications avec le public pour veiller à ce que les Canadiennes et les Canadiens soient informés du moment où leurs villes — et par conséquent eux-mêmes — pourraient être photographiées, nous croyons qu'elles devraient adopter une attitude plus sensible au respect de la vie privée lorsqu'elles choisissent les endroits à photographier. Les personnes qui pénètrent dans des lieux, comme des refuges ou des cliniques d'avortement, où la confidentialité est d'une importance capitale ou qui en sortent veulent vraisemblablement conserver l'anonymat pour des raisons liées à leur vie privée ou à leur sécurité.

Les entreprises devraient également utiliser des technologies de brouillage efficaces et éprouvées des visages et des numéros de plaques d'immatriculation de façon à ce que les personnes ne puissent être identifiées lorsque leurs photos sont affichées sur Internet. Dans ces cas, les entreprises devraient offrir des mécanismes rapides et réactifs qui permettent de bloquer ou de retirer les images.

---

1 En Ontario, la situation est quelque peu différente : dans cette province, la plupart des renseignements personnels détenus par des entreprises sont régis par la LPRPDE, mais les renseignements personnels liés à la santé relèvent d'une loi provinciale, soit la *Loi sur la protection des renseignements personnels sur la santé*.

2 Disponible aussi en ligne : [http://www.priv.gc.ca/fs-fi/02\\_05\\_d\\_39\\_prov\\_f.cfm](http://www.priv.gc.ca/fs-fi/02_05_d_39_prov_f.cfm).

Les entreprises qui offrent ces applications d'imagerie doivent également avoir une bonne raison pour conserver les images originales et non brouillées dans leurs bases de données. Si elles conservent des images non brouillées, elles doivent cependant limiter la période durant laquelle elles les gardent et les protéger avec des mesures de sécurité appropriées<sup>3</sup>.

## C. Street View de Google

### 1. Le service

Le service Street View est créé par Google inc., une entreprise offrant un moteur de recherche sur le Web, et offert dans le cadre de Google Maps. Il reproduit la vue de la rue qu'un utilisateur aurait s'il se promenait dans un lieu géographique donné quelque part dans le monde. L'utilisateur n'a qu'à cliquer sur une carte du service à <http://Maps.google.ca/streetview>, et faire une *promenade virtuelle* dans le quartier choisi, reconstruit en ligne au moyen d'images photographiques des environs.

Ces photographies sont prises par des photographes qui se déplacent dans des villes et d'autres sites cartographiés à bord de voitures identifiées surmontées de caméras. Les photographes ont commencé à visiter les villes canadiennes et à prendre des photos en 2007, mais ces images ont été entreposées pour usage futur<sup>4</sup>. Le lancement officiel des activités de cartographie photographique de Google au Canada a eu lieu en mars 2009, dans 11 villes canadiennes<sup>5</sup>, et le service lui-même a été lancé au Canada en octobre 2009. Les visites par les Canadiens sur le site ont plus que doublé après le lancement<sup>6</sup>.

La société Google a annoncé le 22 mars 2010 qu'elle passerait plusieurs mois à photographier les rues des villes, grandes et petites, de l'ensemble des provinces et des territoires du Canada. Quand tout sera terminé, le Canada, comme les États-Unis, le Royaume-Uni et la France, aura accès à un service Street View à l'échelle du pays. La société a également affirmé qu'elle retournerait à Windsor pour reprendre des photographies de la ville, car des conseillers municipaux se sont plaints des photos existantes, qui ont été réalisées au cours de la longue grève des travailleurs municipaux l'été précédent. Les photos prises au printemps montrent des rues négligées et des monceaux de déchets à de nombreux endroits<sup>7</sup>.

---

3 *Ibid.*

4 CBC News, « Google Alerts Canadians About Street View Filming », CBC News Online, 26 mars 2009, <http://www.cbc.ca/technology/story/2009/03/26/tech-090326-google-street-view.html>.

5 « Google Street View faces privacy roadblocks in Japan, Greece », CBC News Online, 13 mai 2009, <http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html>.

6 Vito Pilieci, « Canadian Street View snoopers pump up Google's hits; Privacy concerns remain as more than 28 million images viewed in one day », *Ottawa Citizen*, 10 octobre 2009.

7 CBC News, « Google Street View to expand in Canada », CBC News, 22 mars 2010, <http://www.cbc.ca/technology/story/2010/03/22/google-street-view-windsor-canada.html>.

L'application Street View peut maintenant être consultée pour la plupart des régions peuplées du Canada, comme le montre la carte du site Web de Google, [http://www.google.com/intl/fr\\_us/help/maps/streetview/where-is-street-view.html](http://www.google.com/intl/fr_us/help/maps/streetview/where-is-street-view.html), qui indique les régions du monde répertoriées. Ce site donne aussi un aperçu des zones où les véhicules de Google sont actuellement en activité.

Tout au long de 2009, la commissaire à la protection de la vie privée du Canada a mené des discussions avec Google inc. pour informer l'entreprise des dispositions législatives protégeant la vie privée au Canada et elle a fait part de ses inquiétudes concernant la surveillance caméra nécessaire pour offrir le service Street View. À la suite de consultations avec la commissaire, la société Google a accepté de brouiller les visages et les plaques d'immatriculation dans les images canadiennes du service Street View.

Le service de Google couvre déjà la majeure partie des États-Unis et a été lancé dans plus de 100 villes à l'échelle du monde. Il a généré une controverse considérable. Par exemple, en mai 2009, l'Agence de protection des données en Grèce a interdit à Google de prendre des photos Street View à Athènes, exigeant plus de garanties de la part de la société en matière de protection de la vie privée, comme des avis publics annonçant quand les véhicules de tournage circulent et l'amélioration de la protection des images stockées<sup>8</sup>. Au Japon, les plaintes de la population ont forcé Google à baisser ses caméras de 40 centimètres afin que les images soient prises au niveau des yeux et non par-dessus les clôtures, dans les cours intérieures<sup>9</sup>.

En février 2010, les organismes de réglementation de la protection des renseignements personnels de l'Union européenne ont demandé à Google d'informer la population avant d'envoyer des caméras dans les villes pour son service Street View. Ils ont aussi écrit à Google pour lui demander de raccourcir la durée de conservation des photos originales pour la ramener d'un an à six mois. Dans une déclaration tenant lieu de réponse, Google a affirmé que son besoin de conserver les images Street View pendant un an est légitime et justifié<sup>10</sup>.

En octobre 2010, l'organisme de protection de la vie privée de l'Italie a annoncé que des restrictions étaient imposées au service de cartographie de Street View, faisant ainsi écho aux préoccupations exprimées ailleurs en Europe. Il a précisé dans une déclaration que, dorénavant, les véhicules de Google devront être « clairement identifiés par des pancartes et des auto-collants » indiquant qu'ils sont en train de prendre des

---

8 Derek Gatopoulos, « Google's Street View halted in Greece over privacy », *USA Today*, 12 mai 2009, [http://www.usatoday.com/tech/news/2009-05-12-google-street-view\\_N.htm](http://www.usatoday.com/tech/news/2009-05-12-google-street-view_N.htm). « Google Street View faces privacy roadblocks in Japan, Greece », CBC News Online, 13 mai 2009, <http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html>.

9 « Google Street View faces privacy roadblocks in Japan, Greece », CBC News Online, 13 mai 2009, <http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html>.

10 Aoife White, « Google warned by EU over Street View map photos », *The Globe and Mail*, 26 février 2010, <http://www.theglobeandmail.com/news/technology/google-warned-by-eu-over-street-view-map-photos/article1482311/>.

photos pour Street View. De plus, la société Google devra publier trois jours à l'avance sur son site Web les noms des zones qu'elle entend photographier et communiquer la même information dans au moins une station radio et deux journaux locaux pour que les résidents puissent avoir le choix d'éviter de se faire photographier. Google sera passible d'amendes pouvant aller jusqu'à 180 000 euros pour avoir enfreint le nouveau règlement italien<sup>11</sup>.

## **2. Protection de la vie privée**

Google, sur son site Web, fournit aux utilisateurs les renseignements suivants concernant la protection de la vie privée :

### **Accès public uniquement**

La fonctionnalité Street View propose des photographies tout à fait semblables à ce que vous voyez lorsque vous vous promenez dans la rue, que ce soit en voiture ou à pied. Ces images sont aujourd'hui disponibles pour de nombreuses villes du monde. Dans certains cas, Google prévoit de conclure des partenariats, à l'instar de celui réalisé avec Disneyland Paris, pour planifier la prise de photos des lieux.

### **Les images Street View ne sont pas en temps réel**

Nos images affichent uniquement ce que nos véhicules ont pu voir le jour lorsqu'ils sont passés dans un lieu précis. Ensuite, plusieurs mois sont nécessaires pour traiter les images recueillies avant de les mettre en ligne. Les images que vous voyez dans Street View peuvent donc être datées de quelques mois à quelques années.

### **Les personnes et les plaques d'immatriculation sont rendues floues**

Nous avons mis au point une technologie très sophistiquée permettant de rendre flous des visages et des plaques d'immatriculation. Elle est utilisée dans toutes les images Street View. Par conséquent, si un visage reconnaissable (par exemple, celui d'un passant sur le trottoir) ou une plaque d'immatriculation lisible figure sur l'une de nos photos, [cette portion d'image] est automatiquement rendue floue par notre technologie, afin que la personne ou le véhicule en question ne puisse pas être identifié. Si nos détecteurs ont laissé passer quelque chose, n'hésitez pas à nous le faire savoir.

### **Vous pouvez demander le retrait d'une image**

Nous offrons des outils faciles d'accès afin de permettre à tout utilisateur de demander le retrait d'une image dont il juge le contenu inapproprié (en cas de nudité, par exemple) ou sur laquelle il se reconnaît lui-même, sa famille, sa voiture ou son domicile. La procédure permettant d'effectuer ce type de demande est décrite ci-dessous.

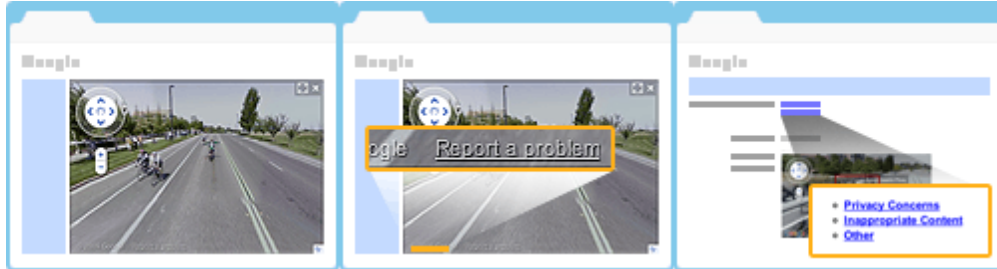
---

11 « Italy privacy regulator orders restrictions on Google's Street View », *International Business Times*, 26 octobre 2010, <http://www.ibtimes.com/articles/75777/20101026/google-street-view-italy.htm>.

## Comment signaler un problème

Si vous avez trouvé une image Street View que vous considérez comme inappropriée, procédez comme suit :

1. Localisez l'image dans Street View.
2. Cliquez sur « Signaler un problème » dans l'angle situé en bas à gauche de l'image.
3. Remplissez le formulaire, puis cliquez sur « Envoyer ».



C'est tout. Nous examinerons votre rapport très rapidement<sup>12</sup>.

### **3. Collecte, par Google, de données utiles dans des réseaux Wi-Fi non protégés et conclusions préliminaires du Commissariat à la protection de la vie privée**

Après que l'organisme allemand de protection des renseignements personnels situé à Hambourg lui eut demandé de vérifier les données Wi-Fi recueillies par ses véhicules Street View dans le cadre d'un projet de services géodépendants, Google a découvert en mai 2010 qu'elle avait recueilli des données utiles (le contenu de communications faites dans un réseau) transmises sur des réseaux sans fil non protégés pendant sa collecte de renseignements sur les points d'accès Wi-Fi à l'appui d'un projet de services géodépendants. Un service géodépendant est un service d'information et de divertissement accessible au moyen d'un appareil mobile dans le réseau mobile et qui tire parti de la capacité d'utiliser la position géographique de l'appareil<sup>13</sup>. De l'aveu même de Google, cette collecte accidentelle semble avoir été causée par l'intégration d'un code au logiciel élaboré pour capter les signaux Wi-Fi. Devant cette situation, la société a immobilisé ses véhicules Street View, arrêté de recueillir des données sur les réseaux Wi-Fi le 7 mai 2010 et isolé et stocké toutes les données déjà recueillies<sup>14</sup>.

---

12 <http://maps.google.ca/help/maps/streetview/privacy.html>.

13 « Location-Based Services », GSM Association, janvier 2003, <http://www.gsmworld.com/documents/se23.pdf>.

14 Commissariat à la protection de la vie privée du Canada, *Lettre de conclusions préliminaire*, 19 octobre 2010, [http://www.priv.gc.ca/media/nr-c/2010/let\\_101019\\_f.cfm](http://www.priv.gc.ca/media/nr-c/2010/let_101019_f.cfm).



Le 31 mai 2010, après avoir appris que des véhicules Street View avaient recueilli des données utiles transmises sur des réseaux Wi-Fi non cryptés pendant la collecte de signaux radio Wi-Fi diffusés publiquement, le Commissariat à la protection de la vie privée du Canada a déposé trois plaintes contre Google conformément au paragraphe 11(2) de la LPRPDE<sup>15</sup>.

Les trois plaintes sont les suivantes :

- a. Google aurait recueilli, utilisé ou communiqué des données utiles sans avis et consentement préalable;
- b. Google aurait recueilli des données utiles sans déterminer les fins de la collecte de renseignements personnels au préalable;
- c. Google aurait recueilli des données utiles au-delà de ce qui est nécessaire aux fins déterminées<sup>16</sup>.

Au terme de son enquête, la commissaire à la protection de la vie privée a, le 19 octobre 2010, publié une *Lettre de conclusions préliminaire*<sup>17</sup> (annexe B), où elle recommandait que Google instaure un modèle de gouvernance permettant de respecter les lois canadiennes sur la protection de la vie privée. Le modèle comprendrait des mesures de contrôle qui feraient en sorte que les procédures nécessaires au respect de la vie privée aient été suivies avant le lancement d'un produit.

La commissaire a aussi recommandé que Google améliore la formation offerte à tous ses employés au sujet du respect de la vie privée et désigne une ou des personnes responsables de la protection de la vie privée et du respect des obligations de leur entreprise à cet égard, ce qui est une exigence des lois canadiennes en la matière.

Elle a recommandé en outre que Google supprime les données utiles recueillies au Canada, dans la mesure où les lois canadiennes et américaines ne l'empêchent pas de le faire, ce qui pourrait être le cas par exemple pour préserver des éléments de preuve dans le cadre de poursuites judiciaires. Si les données utiles canadiennes ne pouvaient pas être supprimées sur-le-champ, il faudrait les conserver de manière sécuritaire et en restreindre l'accès .

La commissaire à la protection de la vie privée ne considérera l'affaire comme résolue que si Google lui remet au plus tard le 1<sup>er</sup> février 2011 la confirmation que les

---

15 Paragraphe 11(2) de la LPRPDE : « Le commissaire peut lui-même prendre l'initiative d'une plainte s'il a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question relative à l'application de la présente partie. »

16 Commissariat à la protection de la vie privée du Canada, *Lettre de conclusions préliminaire*, 19 octobre 2010, [http://www.priv.gc.ca/media/nr-c/2010/let\\_101019\\_f.cfm](http://www.priv.gc.ca/media/nr-c/2010/let_101019_f.cfm).

17 *Ibid.*

recommandations formulées ci-dessus ont été mises en œuvre; elle produira à ce moment-là son rapport final avec ses conclusions<sup>18</sup>.

Dans un article paru le 22 octobre 2010, le journaliste Michael Liedtke de l'*Associated Press* a signalé que Google « serre la vis à ses employés pour qu'ils n'empiètent pas sur la vie privée des gens pendant la collecte et le stockage de renseignements<sup>19</sup> ». Selon lui, « en plus de nommer une employée de longue date, Alma Whitten, directrice de la protection de la vie privée, Google a dit vendredi qu'elle obligera ses 23 000 employés à suivre une formation. La société est aussi en train d'implanter de nouvelles mesures de vérification pour que les travailleurs obéissent aux règles. L'adoption de mesures plus strictes semble faire suite aux manquements récents qui ont soulevé des doutes sur les contrôles et les politiques internes ». Lorsqu'il a témoigné devant le Comité le 4 novembre 2010, le conseiller en matière de politique au Canada de Google, Jacob Glick, a confirmé que son entreprise était en train de prendre ces mesures.

## D. Scène de rues de Canpages

### 1. Le service

Canpages, une entreprise canadienne offrant un annuaire en ligne pour les recherches d'entreprises, a lancé, en partenariat avec une société américaine appelée MapJack, un service qui fera concurrence à l'outil Street View de Google<sup>20</sup>. Tout comme l'outil Street View de Google Maps, le service Scène de rues de Canpages offre des images panoramiques des voies urbaines, ce qui permet aux utilisateurs d'explorer des quartiers entiers en quelques clics de souris. Toutefois, contrairement au service Street View de Google, le service Scène de rues de Canpages se concentre sur les commerces. Ainsi, comme l'indique un communiqué de presse :

Scène de rues fournit des vues panoramiques de 360 degrés des voies urbaines aux utilisateurs effectuant des recherches d'entreprises locales sur Canpages.ca. Cette technologie leur permet de cibler les résultats de recherche sur une carte géographique et d'en obtenir des images à haute résolution dans l'environnement local. Par exemple,

---

18 Ibid.

19 Michael Liedtke, « Google to impose tougher privacy measures after backlash to recent employee missteps, breaches », *Canadian Business Online*, 22 octobre 2010, [http://www.canadianbusiness.com/markets/headline\\_news/article.jsp?content=b4915117&page=2](http://www.canadianbusiness.com/markets/headline_news/article.jsp?content=b4915117&page=2).

20 Kris Abel, « Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca », CTV.ca, blogue de Kris Abel, 16 mars 2009, <http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx>. Canpages est la plus importante entreprise locale de recherches locales et le plus grand éditeur d'annuaires au Canada. Son site Web, Canpages.ca, offre des bases de données résidentielles et commerciales nationales et plus de 3,5 millions de visiteurs uniques visitent le site chaque mois pour y effectuer des demandes de recherches locales. Forte de 80 publications et comptant plus de 80 000 clients, Canpages rejoint plus de huit millions de foyers et d'entreprises d'un bout à l'autre du Canada. Le siège social est situé à Vancouver, et quelque 700 personnes sont à l'emploi de Canpages dans ses bureaux de l'Alberta, de la Colombie-Britannique, de l'Ontario et du Québec : [http://corporate.canpages.ca/about\\_us/company\\_profile/where\\_local\\_search\\_gets\\_done](http://corporate.canpages.ca/about_us/company_profile/where_local_search_gets_done).

les utilisateurs peuvent naviguer "virtuellement" dans les rues pour voir si un restaurant offre du stationnement ou pour jeter un coup d'œil à la vitrine d'un magasin en particulier<sup>21</sup>.

Le lancement de Scène de rues a eu lieu en mars 2009 et permettait de voir Vancouver, Squamish et Whistler en ligne<sup>22</sup>. En août 2009, Canpages a tourné des images des rues du centre-ville et des artères commerciales de Toronto<sup>23</sup> et de Montréal<sup>24</sup>, et ces deux villes sont maintenant visibles en ligne.

## 2. Politique de confidentialité

La politique de confidentialité de Canpages<sup>25</sup> donne les précisions suivantes concernant l'outil Scène de rues :

Dans son effort de fournir le Service Vue de la rue (Street Scene) [habituellement appelé Scène de rues] de Canpages, Canpages fait preuve de sensibilité pour éviter d'inclure des informations de nature photographique qui fourniraient de l'information personnelle au sujet de personnes identifiables. Nous sommes sensibles à l'égard des préoccupations relatives à la confidentialité que pourraient avoir certaines personnes ayant été photographiées lors de la préparation des données requises par le service Vue de la rue (Street Scene). Les photographies de personnes identifiables ne sont aucunement requises par le service. L'assemblage des données est conçu de manière à flouter consciemment les visages de toute personne pouvant être photographiée dans le cadre de cette démarche. Vous constaterez, par conséquent, que personne ne peut être identifié en utilisant le service Mapjack. Si vous souhaitez faire part d'une préoccupation concernant la confidentialité, veuillez cliquer sur « Faire part d'une préoccupation » sur l'une des pages du Service Vue de la rue.

La politique de confidentialité précise également ceci : « Nos politiques de confidentialité reposent sur les 10 principes d'équité dans le traitement des renseignements personnels tels que décrits par le Commissaire à la protection de la vie privée du Canada ». Les dix principes sont ensuite énumérés.

---

21 Canpages inc., « Canpages to Begin Street Scene Shooting in Toronto », 11 août 2010, <http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf>.

22 Kris Abel, « Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca », CTV.ca, blogue de Kris Abel, 16 mars 2009, <http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx>.

23 Canpages inc., « Canpages to Begin Street Scene Shooting in Toronto », 11 août 2009, <http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf>, et Kenyon Wallace, « Google Street View gets Canpages competition », *Toronto Star*, 11 août 2009, <http://www.thestar.com/business/companies/google/article/679194--google-street-view-gets-canpages-competition>.

24 Roberto Rocha, « Canpages Street Scene launches in Montreal », *Montreal Gazette*, 27 août 2009, <http://www.canada.com/montrealgazette/Canpages+Street+Scene+launches+Montreal/1936073/story.html>.

25 Accessible en ligne : <http://www.canpages.ca/hm/privacy.jsp?lang=1>.

- a. Responsabilité : une organisation est responsable des renseignements personnels qu'elle a en sa possession et doit charger une ou des personnes responsables de s'assurer de la conformité de ladite organisation aux principes suivants.
- b. Détermination des fins de la collecte de renseignements : les fins de la collecte de renseignements doivent être précisées par l'organisation avant la collecte ou au moment où elle a lieu.
- c. Consentement : la personne doit être informée et avoir donné son consentement pour que les renseignements personnels la concernant soient recueillis, utilisés ou communiqués, à moins qu'il ne soit pas approprié de le faire.
- d. Limitation des collectes : la collecte de renseignements personnels se limitera à ce qui est nécessaire aux fins précisées par l'organisation. Les renseignements seront recueillis à l'aide de moyens loyaux et licites.
- e. Limitation de l'utilisation, de la communication et de la conservation : les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'autorise. Vous ne devez conserver les renseignements personnels qu'aussi longtemps que nécessaire à la réalisation des finalités déterminées.
- f. Exactitude : les renseignements personnels doivent être aussi exacts, complets, et mis à jour que nécessaire aux fins pour lesquelles ils pourraient être utilisés.
- g. Mesures de sécurité : les renseignements personnels sont tenus d'être protégés par des mécanismes de sécurité adaptés à la sensibilité des informations.
- h. Transparence : une organisation doit rendre facilement accessibles à toute personne des renseignements précis sur ses politiques et pratiques en matière de gestion des renseignements personnels.
- i. Accès aux renseignements personnels : toute personne qui en fait la demande doit être informée du fait que vous possédez des renseignements personnels à son sujet, de l'usage que vous en faites ou entendez faire, ainsi que des tiers à qui ils sont communiqués, et doit se voir accorder le droit d'accéder à ces renseignements. Lorsqu'une personne démontre que des renseignements personnels la concernant sont inexacts et incomplets, vous devez apporter les corrections ou les modifications nécessaires.
- j. Possibilité de porter plainte contre le non-respect des principes : toute personne doit pouvoir contester la conformité aux principes susmentionnés auprès de la ou des personnes responsables chargées de s'assurer de la conformité de l'organisation.

### **3. Canada Eye**

En mars 2010, Canpages a lancé Canada Eye, application iPhone gratuite de « réalité augmentée ». Canada Eye permet de faire des recherches et de visualiser en temps réel sur l'écran iPhone la route à suivre vers n'importe quel commerce et la distance qui reste à parcourir. La « réalité augmentée » est une technologie de pointe intégrée aux applications qui font simultanément appel à la boussole 3GS, au GPS et à la caméra vidéo de l'iPhone. Comme le mentionne un communiqué de presse, « l'application de Canpages permet à l'utilisateur de chercher une certaine catégorie de commerces —

charcuterie locale, boulangerie du coin, Starbucks ou Tim Hortons —, et d'obtenir ensuite les indications à suivre et la distance vers toutes les entreprises de cette catégorie dans le voisinage. En fait, Canada Eye est une application qui repère les entreprises des environs et qui renseigne sur la façon de s'y rendre en temps réel<sup>26</sup>. »

En juin 2010, le Groupe Pages jaunes a fait l'acquisition de Canpages pour environ 225 millions de dollars canadiens<sup>27</sup>.

## **CE QUE LE COMITÉ A ENTENDU : PREMIERS TÉMOIGNAGES — LES APPLICATIONS D'IMAGERIE À L'ÉCHELLE DE LA RUE DE GOOGLE ET DE CANPAGES**

### **A. Google Canada**

Jonathan Lister, directeur général et chef de Google Canada, a comparu devant le Comité le 17 juin 2009. Dans ses observations préliminaires, M. Lister a souligné que Street View de Google « représente manifestement un produit qui change la façon dont les gens perçoivent les cartes [...] la grande innovation qu'offre l'outil Street View de Google est sa capacité de marier des images de la rue à des cartes numériques pour fournir un produit de qualité supérieure aux utilisateurs d'Internet<sup>28</sup> ».

En ce qui concerne les obligations juridiques et de protection de la vie privée qui incombent à Google dans divers pays, M. Lister a déclaré ce qui suit :

D'abord, Google respecte les lois de tous les pays dans lesquels Street View est implanté. Les images que nous mettons à la disposition du public montrent simplement ce que n'importe qui pourrait voir en s'engageant dans une rue publique. Les images auxquelles on a accès grâce à Street View représentent un instantané et ont souvent été prises au cours de la dernière année. Il ne s'agit pas d'images en temps réel. Même si nous recueillons des images prises uniquement dans des lieux publics, nous savons depuis toujours que des passants peuvent être inclus dans nos images par inadvertance. Ainsi Google a investi d'importantes ressources dans la mise au point d'un procédé d'identification et de brouillage de certaines caractéristiques d'une image — par exemple, les visages et les plaques d'immatriculation — qui est le plus avancé du monde [...].

Une autre composante clé des systèmes de protection de la vie privée que nous avons incorporés dans l'outil Street View est son système de demande de retrait d'images qui est facile à utiliser. Chaque image publiée dans Street View contient un lien « signaler un problème » qui renvoie les utilisateurs à une page où ils peuvent demander le retrait

---

26 « Canpages Brings "Augmented Reality" Local Search to the iPhone 3GS », 10 mars 2010, <http://www.benzinga.com/pressreleases/m166514/canpages-brings-augmented-reality-local-search-to-the-iphone-3gs>.

27 Yellow Media Inc., *Yellow Pages Group Finalizes Acquisition of Canpages*, 23 juin 2010, <http://corporate.canpages.ca/media/Yellow%20Pages%20Group%20Finalizes%20Acquisition%20of%20Canpages.pdf>.

28 Jonathan Lister, *Témoignages*, réunion n°29, 17 juin 2009, 1550, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=F&Mode=1&Parl=40&Ses=2>.

d'une image. Ainsi n'importe quel particulier peut demander à faire disparaître une image de lui-même, de membres de sa famille, de sa voiture ou de sa maison. Ce retrait est accordé même si ces éléments de l'image ont déjà été brouillés. Nous traitons des demandes de retrait tous les jours dans une multiplicité de langues différentes et le délai d'exécution de chaque demande est à la fois court et efficace.

Un autre aspect important des efforts que nous déployons afin de garantir la protection de la vie privée est notre engagement à travailler avec les intervenants clés dans chaque pays afin de recenser et de contacter des organismes locaux pertinents avant le lancement du service. Ainsi notre équipe peut travailler en collaboration avec les intervenants clés canadiens pour leur fournir tous les détails importants au sujet de l'outil Street View, y compris la procédure à suivre pour faire brouiller ou enlever l'image de leur organisme.

Nous sommes également en train de créer un système qui garantira que, le jour du lancement de Street View au Canada, nous aurons plus de personnel de disponible pour répondre aux demandes de retrait.

Permettez-moi donc de conclure en disant que, comme c'est le cas pour beaucoup de technologies de pointe, notre défi, en ce qui concerne Street View, consiste à établir le bon équilibre entre les fonctions d'un outil sophistiqué que nous voulons très utile et l'utilisation appropriée des données que nous réunissons pour nous permettre d'offrir de tels services<sup>29</sup>.

M. Lister a comparu devant le Comité avant le lancement de l'outil Street View au Canada en octobre 2009. À l'époque, il a informé le Comité que Google travaillait de près avec le Commissariat à la protection de la vie privée afin de s'acquitter de ses obligations juridiques et en matière de protection de la vie privée avant le lancement de Street View<sup>30</sup>. En réponse aux préoccupations concernant la possibilité que Street View viole la vie privée des particuliers à l'intérieur de leurs domiciles ou voie à l'intérieur de lieux sensibles comme des refuges pour femmes, M. Lister a signalé que les images Street View sont captées à l'extérieur de lieux publics : « [Street View] vise à améliorer la cartographie et à capter des images de bâtiments et de points de repère qui sont accessibles au public. Donc, il n'est pas nécessaire de voir l'intérieur; la définition même du produit n'inclut pas cet élément, et Google ne fait pas ce genre de chose<sup>31</sup>. »

S'agissant de politiques de conservation et d'élimination, les images de Google sont conservées dans des « fermes de serveur » sûres, dont la plupart semblent être situées aux États-Unis<sup>32</sup>. En ce qui concerne les images d'origine non brouillées, M. Lister signale que Google conserve les images claires en vue d'améliorer ses produits, c'est-à-dire pour améliorer les capacités de reconnaissance de la technologie de brouillage. Il a ajouté que Google a décidé de revoir sa politique de conservation des données afin de conserver les images non brouillées pendant « une période suffisante mais non

---

29 *Ibid.*

30 *Ibid.*, 1605, 1650.

31 *Ibid.*, 1630.

32 *Ibid.*, 1625.

excessive », après quoi ces images non brouillées seront floutées de façon permanente afin de les rendre complètement anonymes (au lieu de les éliminer<sup>33</sup>). En date de juin 2009, Google n'avait pas fixé de calendrier exact pour la conservation des images non brouillées<sup>34</sup>. M. Lister a signalé que Google informera le Comité du délai précis quand l'entreprise aura « une réponse exacte et raisonnable<sup>35</sup> ». Après la comparution de M. Lister devant le Comité, Google a convenu avec le Commissariat à la protection de la vie privée de conserver les images non brouillées pour une période d'un an<sup>36</sup>.

## B. Canpages

Lorsqu'il a comparu devant le Comité le 17 juin 2009, Olivier Vincent, président et chef de direction de Canpages, a expliqué la fonction de l'outil Scène de rues de Canpages qui vise principalement les zones commerciales : « Pleinement intégrée avec sa plate-forme de recherche Canpages.ca, l'application Scène de rues permet aux utilisateurs de consulter des photos panoramiques prises au niveau de la rue afin qu'ils puissent non seulement repérer les résultats de leur recherche sur une carte géographique, mais aussi voir les résultats de leur recherche à haute résolution dans un environnement local. Par exemple, les utilisateurs peuvent « marcher virtuellement » à travers les rues d'une ville et se rendre jusqu'à un restaurant local ou un hôtel particulier. Ils peuvent ainsi voir l'extérieur du restaurant recherché avant de faire la réservation, ou encore vérifier s'il est possible de stationner dans la rue ou dans un parc de stationnement disponible à proximité<sup>37</sup>. »

En ce qui concerne les préoccupations au sujet de la protection de la vie privée que soulève l'utilisation, par Scène de rues, d'images et de technologies de l'imagerie, M. Vincent a déclaré ce qui suit :

Canpages est d'avis que le respect de la vie privée est une priorité essentielle. Ainsi nous sommes sensibles aux préoccupations de certains concernant la possibilité que la vie privée de personnes photographiées pendant la préparation des données requises pour le service Scène de rue pourrait être atteinte. Canpages est résolu à garantir à tous que leur vie privée sera respectée et a d'ailleurs annoncé publiquement son engagement en ce sens par la publication de sa politique de protection de la vie privée relative au service Scène de rue.

Nous nous engageons donc à prévenir le public avant tout prochain tournage. Les visages des personnes et d'autres éléments reconnaissables, tels que les plaques

---

33 *Ibid.*, 1610.

34 *Ibid.*, 1650.

35 *Ibid.*, 1715.

36 Elizabeth Denham, *Témoignages*, réunion n° 32, 22 octobre 2009, 0930, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=F>.

37 Olivier Vincent, *Témoignages*, réunion n° 29, 17 juin 2009, 1555, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=F&Mode=1&Parl=40&Ses=2>.



d'immatriculation, seront brouillés sur les images originales avant qu'elles ne soient mises en ligne. Le procédé de brouillage que nous employons est une technologie que nous-mêmes avons mise au point et elle est irréversible par les utilisateurs. Les images originales sont détruites après avoir été brouillées et avant d'être mises en ligne. Il n'est donc pas possible de récupérer les images originales après coup.

Les utilisateurs peuvent aussi communiquer à tout moment leurs inquiétudes au sujet des images en cliquant sur le lien « signaler une préoccupation » qui se trouve sur toute image de l'application Scène de rue. À la demande d'un utilisateur, Canpages offrira de brouiller l'image d'une personne, d'un véhicule, d'une fenêtre, d'un édifice, d'un animal — il suffit d'en faire la demande. Bien que les lois visant à protéger la vie privée ne soient pas nécessairement adaptées aux nouvelles technologies, qui évoluent rapidement, Canpages désire adopter une approche proactive afin de répondre positivement à toute préoccupation qui pourrait être soulevée au sujet de ce service.

[...]

Canpages a ouvert un dialogue avec le public, les divers commissariats à la protection de la vie privée et avec M. Pierre Poilievre, le député qui a déposé une motion devant ce Comité pour que ce dernier examine la question de la protection de la vie privée.

En conclusion, Canpages s'engage à collaborer immédiatement et en permanence avec les différents acteurs afin de régler tout problème potentiel lié à la protection de la vie privée qui pourrait résulter de ses innovations dans le domaine de la recherche locale<sup>38</sup>.

Après ses observations préliminaires, M. Vincent a parlé, entre autres choses, de la technologie de brouillage employée par la société afin d'assurer l'anonymat des passants et des lieux sensibles. Il a précisé qu'avec les versions précédentes de la technologie de brouillage, il était plus facile de débrouiller l'image, mais la nouvelle version utilisée par la société est beaucoup plus puissante et le procédé de brouillage est irréversible. Il a aussi précisé que les versions d'origine de toute image qui doit être brouillée sont détruites et remplacées par la version floutée par application de la technologie<sup>39</sup>.

### **C. Commissariat à la protection de la vie privée du Canada**

Elizabeth Denham, commissaire adjointe au Commissariat à la protection de la vie privée du Canada, a comparu devant le Comité le 22 octobre 2009. M<sup>me</sup> Denham a informé le Comité que LPRPDE est une loi neutre sur le plan technologique qui est « un outil dynamique, moderne et efficace pour rehausser le droit à la vie privée des citoyens » qui a été conçu pour réagir à des situations comme « la collecte et [...] l'utilisation commerciales de renseignements personnels par la technologie de l'imagerie au niveau de la rue<sup>40</sup> ». Tout en sachant que de nombreux services utilisant l'imagerie au niveau de la rue sont très prisés de la population, le Commissariat à la protection de la vie privée

---

38 *Ibid.*

39 *Ibid.*, 1620, 1625 et 1720.

40 Elizabeth Denham, *Témoignages*, réunion n° 32, 22 octobre 2009, 0900, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=F>.



continue de tenir à assurer que l'utilisation commerciale de cette technologie garantit « la protection de la vie privée des citoyens en veillant à ce que la technologie respecte les exigences de la LPRPDE en matière de connaissance, de consentement, de mesures de sauvegarde et de conservation limitée des renseignements<sup>41</sup> ».

De l'avis du commissariat, les sociétés devraient informer les citoyens de leur intention de photographier dans la rue en leur indiquant où et quand elles le feront, en plus de leur expliquer comment ils peuvent demander le retrait de leurs images s'ils ne veulent pas qu'elles soient diffusées en ligne. Les visages et les plaques d'immatriculation doivent être brouillés de façon à ce que les personnes puissent rester anonymes ou du moins ne pas être identifiables. Les sociétés doivent se doter de moyens efficaces et rapides de retirer les images des citoyens l'ayant demandé. Les images non brouillées conservées à des fins commerciales légitimes devraient être protégées au moyen de mesures de sécurité appropriées, et les données brutes ne devraient pas être conservées indéfiniment<sup>42</sup>.

M<sup>me</sup> Denham a signalé que les fournisseurs de services qui ont comparu devant le Comité ont apporté des améliorations à ce chapitre. En août 2009, Google a convenu avec le Commissariat à la protection de la vie privée et d'autres commissaires à la protection des données en Europe qu'elle devait supprimer les images non brouillées au bout d'un an. Comme l'a dit M<sup>me</sup> Denham lors de son témoignage :

L'une des plus vives controverses que nous avons eues dans nos discussions avec Google et Canpages concernait ce que devient l'image brute, non brouillée, conservée dans des bases de données aux États-Unis. Au début, Google était réticente à fixer une période de conservation limitée. Ensuite, au mois d'août, la société est convenue avec nous et avec d'autres commissaires de protection des renseignements personnels en Europe que les images non brouillées devraient être supprimées au bout d'un an. Elle nous a donné des justifications pour vouloir les conserver pendant un an et nous les avons acceptées. Google s'est également engagée à nous permettre de visiter ses installations afin de voir comment se fait la suppression ou l'anonymisation permanente des données au bout d'un an. C'était l'une de nos principales préoccupations au sujet de ce service<sup>43</sup>.

M<sup>me</sup> Denham a également fait savoir au Comité que depuis le lancement de Street View de Google au début d'octobre 2009, le Commissariat à la protection de la vie privée a reçu seulement une dizaine de demandes d'information de la part de Canadiens et une seule plainte, laquelle a été réglée. La plainte provenait d'une personne qui estimait avoir été photographiée. Elle a été réglée lorsque Google a accepté de supprimer en permanence l'image de l'homme de la base de données, de sorte que le commissariat n'a jamais fait de recommandation publique. Le Commissariat à la protection de la vie privée n'avait pas reçu de plaintes concernant l'efficacité de la procédure de retrait de Google au

---

41 *Ibid.*

42 *Ibid.*, 0905.

43 *Ibid.*, 0930.

moment où M<sup>me</sup> Denham a comparu devant le Comité. Il a reçu des appels de la part de personnes souhaitant faire retirer leurs images de Street View, et celles-ci ont été renvoyées à Google et aucune, jusqu'à maintenant, n'est revenue au commissariat pour présenter une plainte officielle<sup>44</sup>.

Quand on lui a demandé si le Commissariat à la protection de la vie privée estime que la politique de brouillage de Google répond aux normes des lois sur la protection des renseignements personnels par les entreprises au Canada, M<sup>me</sup> Denham a affirmé que la technologie de brouillage de Google pourrait être meilleure : « Google nous a dit que sa technologie de brouillage est efficace à 98 p. 100. C'était avant la mise en marche du système. Nous avons constaté nous-mêmes que beaucoup de visages n'ont pas été brouillés. Google s'est engagé à améliorer le brouillage et c'est l'une des raisons pour lesquelles elle veut conserver les images pendant un an. Elle travaille sur l'amélioration de la technologie de brouillage. » La commissaire à la protection de la vie privée est satisfaite de ce délai d'un an<sup>45</sup>.

## **CE QUE LE COMITÉ A ENTENDU : SUITE DES TÉMOIGNAGES — COLLECTE DE DONNÉES WI-FI PAR GOOGLE**

### **A. Commissariat à la protection de la vie privée du Canada**

Patricia Kosseim, avocate générale au Commissariat à la protection de la vie privée du Canada, a comparu devant le Comité le 28 octobre 2010 pour parler de l'enquête effectuée sur la collecte par inadvertance de données Wi-Fi par Google et qui a débouché sur l'envoi de la *Lettre de conclusions préliminaire* le 19 octobre 2010<sup>46</sup>. Elle a aussi fait le point sur les conséquences de la technologie d'imagerie à l'échelle de la rue pour la vie privée. Elle était accompagnée de Daniel Caron, conseiller juridique, Direction des services juridiques, des politiques et des affaires parlementaires, et d'Andrew Patrick, analyste de recherche en technologie de l'information.

Dans ses observations préliminaires, M<sup>me</sup> Kosseim a résumé l'enquête du Commissariat sur la collecte accidentelle<sup>47</sup> de données utiles Wi-Fi non protégées par des véhicules Street View de Google. Elle a expliqué que les données utiles sont des renseignements sur les communications transmises dans les réseaux sans fil<sup>48</sup>. L'enquête a fait ressortir ce qui suit :

---

44 *Ibid.*, 0930, 1025.

45 *Ibid.*, 1025.

46 Commissariat à la protection de la vie privée du Canada, *Lettre de conclusions préliminaire*, 19 octobre 2010, [http://www.priv.gc.ca/media/nr-c/2010/let\\_101019\\_f.cfm](http://www.priv.gc.ca/media/nr-c/2010/let_101019_f.cfm).

47 Suivant les propres termes de Patricia Kosseim.

48 Patricia Kosseim, *Témoignages*, réunion n° 28, 28 octobre 2010, 1535, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=F&Mode=1&Parl=40&Ses=3>.

[...] Google avait recueilli des renseignements personnels de manière inappropriée à partir de réseaux sans fil non sécurisés. Dans certains cas, ces renseignements personnels étaient de nature très délicate, notamment des courriels au complet, des noms d'utilisateur et mots de passe, ainsi que des renseignements sur les troubles médicaux de personnes particulières. Malheureusement, cette collecte de données par inadvertance est le fruit d'une erreur qui aurait pu être facilement évitée si Google avait respecté ses propres procédures.

Essentiellement, ce qui est arrivé, c'est que l'ingénieur qui a élaboré le code en vue d'échantillonner des catégories de données Wi-Fi diffusées publiquement a inclus également un code permettant la collecte de données utiles, croyant que ce type de renseignements pourrait servir un jour à Google. L'ingénieur a déterminé des préoccupations à son avis « superficielles » en matière de vie privée, mais, contrairement à la procédure de la société, il a omis de porter ses préoccupations à l'attention du conseil juridique en matière de produits, dont la responsabilité aurait été de les traiter et de les résoudre avant le lancement du produit<sup>49</sup>.

Comme indiqué plus haut<sup>50</sup>, la commissaire a recommandé que Google réexamine et améliore la formation offerte à tous ses employés au sujet du respect de la vie privée et instaure un modèle global de gouvernance qui garantit que les procédures nécessaires au respect de la vie privée ont été suivies avant le lancement d'un produit. Elle a de plus recommandé que Google supprime les données utiles recueillies au Canada dans la mesure où les lois canadiennes et américaines l'autorisent à le faire<sup>51</sup>.

M<sup>me</sup> Kosseim a indiqué que la commissaire à la protection de la vie privée avait envoyé une « lettre de conclusions préliminaire » sur la collecte de données Wi-Fi. La commissaire veut des preuves que les recommandations ont été appliquées avant de mettre un terme à l'enquête et de « clore le dossier ». Autrement dit, elle veut une « mise en œuvre concrète, et pas de simples engagements<sup>52</sup> ».

M<sup>me</sup> Kosseim a ensuite précisé la façon dont le Commissariat à la protection de la vie privée avait été informé que Google recueillait des données utiles et des signaux Wi-Fi. Il avait reçu en avril 2010 un avis de Google l'informant que « l'entreprise avait l'intention de recueillir des signaux radio diffusés publiquement par des réseaux Wi-Fi et qu'elle le

---

49 Ibid.

50 Voir « Collecte, par Google, de données utiles dans des réseaux Wi-Fi non protégés et conclusions préliminaires du Commissariat à la protection de la vie privée ».

51 Patricia Kosseim, *Témoignages*, réunion n° 28, 28 octobre 2010, 1535, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=F&Mode=1&Parl=40&Ses=3..>

52 *Ibid.*, 1540.

faisait<sup>53</sup> ». Google a expliqué que son objectif était d'améliorer ses « services géodépendants<sup>54</sup> ».

M<sup>me</sup> Kosseim a poursuivi en disant que la collecte de signaux Wi-Fi n'était pas liée au produit Street View en soi, mais que, pour des raisons de commodité, Google se servait de ses véhicules Street View pour recueillir les données Wi-Fi. Google a dit au Commissariat à la protection de la vie privée en avril 2010 qu'elle était en train d'installer des antennes sur le toit des véhicules Street View pour recueillir et capter en même temps les signaux radio Wi-Fi des environs<sup>55</sup>.

C'est seulement en mai 2010, après avoir reçu des demandes d'information supplémentaires de la part de l'organisme allemand de protection des renseignements personnels, que Google s'est aperçue qu'elle recueillait sans le savoir des données utiles Wi-Fi<sup>56</sup>. Comme précisé dans la *Lettre de conclusions préliminaires*, Google a immobilisé ses véhicules Street View et arrêté de recueillir des données sur les réseaux Wi-Fi le 7 mai 2010 et a isolé et stocké toutes les données déjà recueillies.

D'après les résultats de son enquête, le commissariat n'avait pas de raison de croire que les données utiles Wi-Fi recueillies accidentellement par Google avaient été utilisées à des fins inappropriées<sup>57</sup>.

Le commissariat a cependant reconnu que la simple collecte de renseignements sur l'accès Wi-Fi peut en soi poser d'éventuelles difficultés sur le plan de la vie privée. Comme l'a mentionné Andrew Patrick : « Si l'information au sujet de la présence d'un point d'accès à un réseau Wi-Fi peut être liée à une personne, en soi ou en rapprochant cette information d'autres éléments d'information, alors cela pourrait devenir de l'information personnelle et pourrait donc être source de préoccupation pour nous<sup>58</sup>. » Le commissariat ne dispose pas de renseignements précis sur les services géodépendants que Google est en train de mettre au point grâce à la collecte de signaux radio Wi-Fi<sup>59</sup>.

M<sup>me</sup> Kosseim a dit dans l'ensemble qu'elle avait toutes les raisons de croire que Google appliquera les recommandations de la commissaire formulées dans la lettre de conclusions préliminaire :

---

53 *Ibid.*, 1555.

54 *Ibid.* Comme précisé plus haut, un « service géodépendant » est un service d'information et de divertissement accessible au moyen d'un appareil mobile dans le réseau mobile et qui tire parti de la capacité d'utiliser la position géographique de l'appareil.

55 *Ibid.*

56 *Ibid.*

57 *Ibid.*, 1605.

58 *Ibid.*

59 *Ibid.*, 1610.

Je pense que nous avons toutes les raisons de le croire. Même si Google ne nous a pas donné de réponses officielles, nous avons pris connaissance des réponses dans la presse, comme vous tous, réponses qui portaient sur les mesures concrètes que les gens de Google ont déjà prises. Dans le cadre de notre enquête, nous avons pris connaissance des mesures qui avaient déjà été prises pour entamer le processus de mise en place de structures de gouvernance adéquates au sein de l'organisation, qui est un géant mondial, comme vous le savez. La date du 1<sup>er</sup> février a été choisie avec soin, compte tenu du délai raisonnable non seulement pour apporter ces changements, mais également pour obtenir des preuves concrètes du fait qu'ils auront été apportés à l'échelle mondiale. C'est la raison pour laquelle cette date a été choisie. Nous avons très bon espoir d'obtenir une réponse positive plus tôt, et nous en serions très heureux. Nous sommes assez persuadés que tout cela va bien se terminer<sup>60</sup>.

M<sup>me</sup> Kosseim a aussi mentionné que, pour le moment, le Commissariat à la protection de la vie privée est satisfait des mesures de protection de la vie privée appliquées pour les technologies Street View de Google et Scène de rues de Canpages, abstraction faite de la collecte de données utiles Wi-Fi, qui est un cas distinct :

En ce qui concerne la technologie d'imagerie à l'échelle de la rue de Google et de Canpages, je veux simplement préciser que, dans un cas comme dans l'autre, les applications n'ont jamais fait l'objet d'une enquête de la commissaire [...] Cependant, d'après la correspondance et la réponse des organisations, les deux ont fait beaucoup de choses pour se plier aux recommandations de la commissaire ou pour poursuivre leurs activités en harmonie avec celles-ci, et elles ont notamment avisé les habitants des quartiers avant de les visiter, discuté avec les intervenants et les groupes vulnérables, mis au point des procédures de retrait des images ainsi que des mécanismes de conservation et de suppression et d'autres mécanismes de protection du genre. Ainsi, d'après cette correspondance, il se fait beaucoup de choses. Évidemment, les avis pourraient toujours être améliorés, comme la technologie qui permet de rendre les images floues peut toujours être améliorée, mais, jusqu'à maintenant, il y a eu énormément d'améliorations et de mesures qui ont été prises qui vont dans le sens de ce que la commissaire souhaitait<sup>61</sup>.

En conclusion, M<sup>me</sup> Kosseim a adressé une grande recommandation aux entreprises, comme Google, Canpages et Facebook, qui ont recours à de nouvelles technologies pour compiler, traiter et communiquer des renseignements, à savoir que ces entreprises doivent adopter le principe de la prudence face aux répercussions possibles sur la vie privée. Le Commissariat espère que les organisations qui conçoivent, élaborent et déploient des technologies de l'information dont tous les Canadiens bénéficient prendront « des mesures proactives dès le départ pour cerner les risques, les évaluer et les gérer avant le déploiement à grande échelle de ces technologies<sup>62</sup> ».

---

60 *Ibid.*

61 *Ibid.*, 1705.

62 *Ibid.*, 1705.

## B. Google Canada

### 1. Audition de Jacob Glick le 4 novembre 2010

Lorsqu'il a témoigné devant le Comité le 4 novembre 2010, Jacob Glick, conseiller en matière de politique au Canada pour Google, a parlé de l'outil Street View de Google et aussi de la collecte de données utiles Wi-Fi<sup>63</sup>.

Au sujet de Street View, M. Glick a mentionné que Google a « tenu compte de toutes les préoccupations que le comité et la commissaire à la protection de la vie privée ont cernées. Nous avons appliqué la technologie de brouillage la plus perfectionnée pour masquer les visages et les plaques minéralogiques sur toutes nos images. Tous peuvent demander à Google de retirer les images d'eux-mêmes, de leur maison, de leurs enfants ou de leur voiture dans Street View. Enfin, après un an, nous intégrons ce brouillage de façon permanente<sup>64</sup>. » Il a ajouté que les Canadiens sont de fervents utilisateurs de Street View. « En chiffres absolus, ils sont au troisième rang des plus grands utilisateurs de ce produit dans le monde, derrière les États-Unis et le Royaume-Uni. Depuis le lancement, les Canadiens de tout le territoire se servent de cette cartographie de nouvelle génération pour tracer le parcours à suivre pour aller au magasin, faire la promotion de leur entreprise locale, vendre leur maison et explorer leur pays en ligne<sup>65</sup>. »

En ce qui concerne la collecte de données utiles Wi-Fi, M. Glick a précisé qu'elle n'avait pas de lien avec le produit Street View, mais que les véhicules Street View servaient de moyens de collecte. Il a présenté ses excuses au nom de Google, mentionnant que « ce qui s'est passé n'est pas conciliable avec notre engagement de servir les usagers d'Internet<sup>66</sup> ». Il a signalé que Google n'a recueilli « aucune donnée utile transmise par réseau crypté. Google ne voulait utiliser les données d'aucune manière, et elles n'ont servi dans aucun de ses produits ou services. Aucune donnée utile canadienne n'a été cédée ni communiquée à des tiers. Les données ont été isolées et mises en sécurité<sup>67</sup>. »

Pour ce qui est de savoir comment des véhicules Street View de Google en sont venus à recueillir des données utiles Wi-Fi, M. Glick a dit qu'en 2007, à l'époque où Google se préparait à lancer Street View et déployait ses véhicules partout dans le monde pour appliquer la technologie de l'imagerie à l'échelle de la rue, un de ses ingénieurs a eu

---

63 Jacob Glick, *Témoignages*, réunion n° 30, 4 novembre 2010, 1530, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4764635&Mode=1&Parl=40&Ses=3&Language=F>.

64 *Ibid.*

65 *Ibid.*

66 *Ibid.*

67 *Ibid.*

l'idée d'utiliser les véhicules pour repérer les points d'accès Wi-Fi en vue des services géodépendants.

C'est une pratique courante dans l'industrie que d'utiliser les points d'accès publics Wi-Fi comme points de repère pour renseigner les utilisateurs sur l'endroit où ils se trouvent. L'ingénieur a conçu le code du logiciel pour recueillir les données réseau Wi-Fi et, hélas, les données utiles également. Par données utiles, on veut désigner le contenu des transmissions. Google ne voulait pas de ces données utiles et croit qu'il ne sert à rien de les recueillir et qu'il est inacceptable de le faire. L'ingénieur aurait dû signaler aux avocats à l'interne, chez Google, ce plan de collecte des données utiles. Il ne l'a pas fait. S'il l'avait fait, Google aurait eu la possibilité de repérer et de régler le problème dès le début du programme. Le code a donc été déployé sur les véhicules de Street View. Le logiciel a fait ce qu'il était programmé pour faire et il a recueilli les données réseau et les données utiles Wi-Fi transmises sur des réseaux non cryptés<sup>68</sup>.

En avril 2010, les autorités allemandes ont demandé à Google de vérifier les données Wi-Fi recueillies par ses véhicules Street View. La vérification a révélé que Google avait recueilli des données utiles Wi-Fi en plus des données de réseau. Selon M. Glick, « [a]vant d'annoncer publiquement ce que nous avons découvert, j'ai appelé moi-même la commissaire Stoddart pour l'informer du problème. Ensuite, Google a fait une annonce publique et présenté des excuses pour l'incident<sup>69</sup>. » L'entreprise a immobilisé ses véhicules Street View et isolé les données. M. Glick a indiqué que « personne n'a examiné les données utiles provenant du Canada sinon les enquêteurs de la commissaire à la protection de la vie privée et ceux qui ont facilité leur travail. Elles n'ont été communiquées à aucune tierce partie<sup>70</sup>. » Le témoignage de M. Glick ne permet pas de déterminer clairement si la collecte de données Wi-Fi n'a commencé qu'en avril ou si elle avait commencé avant.

M. Glick a confirmé que, le 22 octobre 2010, Google a apporté des modifications importantes à ses politiques et mesures de contrôle concernant le respect de la vie privée. Il a dit avoir parlé à la commissaire, M<sup>me</sup> Stoddart, avant que les mesures suivantes soient annoncées publiquement :

D'abord, Google a nommé M<sup>me</sup> Alma Whitten au poste de directrice de la protection de la vie privée pour veiller à ce que nous intégrions à nos produits et à nos pratiques internes des contrôles efficaces pour protéger la vie privée. M<sup>me</sup> Whitten est une spécialiste internationalement reconnue dans les domaines de la protection de la vie privée et de la sécurité en sciences informatiques. Deuxièmement, nous améliorons notre formation de base en matière de protection de la vie privée en mettant un accent particulier sur la collecte, la manipulation et l'utilisation responsables des données. Enfin, Google ajoute de nouvelles garanties à son système actuel d'application de la protection des

---

68 *Ibid.*

69 *Ibid.*

70 *Ibid.*

renseignements en prévoyant des vérifications internes indépendantes pour protéger la vie privée des utilisateurs<sup>71</sup>.

Google est d'avis que les modifications apportées vont grandement améliorer ses mécanismes et contrôles et éviter ainsi que des incidents comme celui des données Wi-Fi se produisent à nouveau.

M. Glick s'est vu demander plusieurs fois en quoi consiste le poste de directeur de la protection de la vie privée chez Google et en quoi Alma Whitten est qualifiée pour ce poste<sup>72</sup>. Il n'a pas été en mesure de fournir une notice biographique de M<sup>me</sup> Whitten au cours de la réunion, mais il a signalé qu'elle travaille dans l'entreprise depuis des années, qu'elle a un doctorat en informatique et en sécurité et qu'elle a publié de nombreux articles sur les questions d'informatique, de sécurité et de respect de la vie privée. C'est une sommité mondiale dans le domaine du respect de la vie privée et de la sécurité depuis plusieurs années. Elle travaille à Londres, au bureau britannique de Google<sup>73</sup>.

D'après le témoignage de M. Glick, il semblerait que Google n'a pas encore supprimé les données utiles recueillies au Canada, car il n'a pas été dit clairement si elles devaient être conservées pour une raison ou une autre<sup>74</sup>. M. Glick a entrepris de vérifier si — et quand — les données utiles canadiennes seront supprimées<sup>75</sup> et si les lois américaines pourraient faire obstacle à leur élimination<sup>76</sup>.

## **2. Audition de Jacob Glick et Alma Whitten le 25 novembre 2010 (par téléconférence)**

Après avoir entendu M. Glick le 4 novembre 2010, le Comité a décidé d'entendre la nouvelle directrice de la protection de la vie privée chez Google, Alma Whitten, et d'interroger de nouveau M. Glick, le 25 novembre 2010, pour obtenir un complément d'information sur les mesures prises par Google à la suite de la collecte accidentelle de données Wi-Fi et en réponse à la *Lettre de conclusions préliminaire* de la commissaire à la protection de la vie privée parue le 19 octobre 2010. Les deux témoins ont comparu par voie de téléconférence, M<sup>me</sup> Whitten depuis Londres et M. Glick, depuis Toronto.

---

71 *Ibid.*

72 Voir, par exemple, 1550 et 1555.

73 *Ibid.*, 1550.

74 *Ibid.*, 1600.

75 *Ibid.*

76 *Ibid.*, 1635.



Préalablement à la comparution de M<sup>me</sup> Whitten, Google a envoyé au Comité la notice biographique suivante à son sujet<sup>77</sup> :

Alma Whitten a rejoint Google en 2003 et occupe actuellement le poste de directrice de la protection de la vie privée pour l'équipe d'ingénierie comme pour l'équipe de produit. À ce titre, elle est chargée de voir à ce que Google intègre à ses produits et ses pratiques internes des mesures de contrôle efficaces pour protéger la vie privée. Spécialiste de renommée internationale dans le domaine de la protection de la vie privée et de la sécurité, M<sup>me</sup> Whitten a témoigné devant le Congrès des États-Unis et a comparu devant le Groupe de travail « article 29 » de la Commission européenne.

M<sup>me</sup> Whitten a été auparavant responsable de la sécurité appliquée puis responsable des outils de protection de la vie privée, affectation durant laquelle elle a mis sur pied les équipes qui ont mis au point des outils comme le Dashboard de Google.

Avant d'entrer chez Google, M<sup>me</sup> Whitten a publié un document technique connu sur le problème du manque de convivialité des mesures de sécurité informatique intitulé « Why Johnny Can't Encrypt », un des documents fondateurs de la recherche sur la convivialité mesures de sécurité. Elle continue de faire de la recherche, de rédiger des textes et de donner des conférences sur les méthodes de sécurité et de protection de la vie privée axées sur le facteur humain dans le cadre de son travail chez Google. M<sup>me</sup> Whitten possède un doctorat en informatique de l'Université Carnegie Mellon.

Dans son témoignage, M<sup>me</sup> Whitten a dit au Comité qu'elle avait « consacré ma carrière, comme universitaire et maintenant comme directrice de la protection de la vie privée chez Google, à un seul grand objectif: permettre aux utilisateurs d'Internet d'assumer le contrôle de leur vie privée et de leur sécurité par des moyens intuitifs, simples et utiles »<sup>78</sup> et a évoqué le projet de Google de renforcer ses mesures internes en matière de sécurité et de protection des renseignements personnels :

Dans le cadre de mes responsabilités étendues, j'aurai la possibilité de superviser les équipes d'ingénierie et de produits et de collaborer avec elles pour veiller à ce que les considérations de sécurité et de protection de la vie privée soient intégrées dans la totalité de nos produits. Même si les fonctions qui correspondent à ce rôle sont lourdes, je suis sûre que je pourrai compter sur les ressources et le soutien interne nécessaires pour aider Google à faire mieux [...] Nous voulons être sûrs que chacun des nouveaux produits que nous mettons en service répond aux normes élevées de sécurité et de protection des renseignements personnels que nos utilisateurs attendent de nous<sup>79</sup>.

M<sup>me</sup> Whitten a expliqué que Google a l'intention d'offrir à ses employés une formation sur la protection de la vie privée adaptée aux responsabilités de chacun<sup>80</sup> qui

---

77 Lettre envoyée par courriel au greffier du Comité, 22 novembre 2010. On trouvera de plus amples informations sur Alma Whitten sur le site Web <http://www.google.com/research/pubs/author32149.html>. [traduction]

78 Alma Whitten, *Témoignages*, réunion n° 34, 25 novembre 2010, 1535, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Mode=1&Parl=40&Ses=3&Language=F>.

79 *Ibid.*, 1540.

80 *Ibid.*, 1600.

comprendra une formation générale sur la sécurité et la protection des renseignements personnels, une formation sur un code de conduite et une formation plus ciblée et plus approfondie portant spécifiquement sur divers types d'activités :

Le point le plus important sur lequel nous insisterons constamment dans le cadre de la formation, c'est que les ingénieurs ne doivent jamais faire eux-mêmes ce genre de jugement de valeur. Nous voulons les sensibiliser à l'environnement de la vie privée et aux préoccupations qu'elle soulève.

Nous sommes également déterminés à leur faire comprendre les principes Google de protection de la vie privée, qui sont fondés sur la transparence, le contrôle et l'administration responsable. Nous voulons surtout leur apprendre à ne jamais perdre de vue les processus améliorés que nous mettons en place pour nous assurer d'avoir des mesures à sécurité intégrée et des procédures d'examen réfléchies et pour veiller à ce que les ingénieurs n'essaient pas de se substituer aux avocats pour régler certaines questions.

[...]

Nous avons l'intention de faire suivre aux ingénieurs nouvellement engagés une session assez importante de formation en protection de la vie privée dans les deux premières semaines qu'ils passent chez Google, avant qu'ils ne soient chargés d'écrire des programmes ou de développer des produits. Grâce à cette formation initiale, nous espérons jeter les fondations nécessaires pour qu'ils apprennent à qui ils doivent s'adresser et où se trouvent les ressources internes pouvant les aider à comprendre la vie privée et les processus que nous avons mis en place dans ce domaine. Nous espérons leur donner ainsi les éléments de base pour qu'ils trouvent rapidement et facilement des personnes à qui parler en cas de besoin.

Pour ce qui est des autres ingénieurs qui ne seront pas passés par cette formation initiale donnée juste après l'embauche, nous organiserons une formation de suivi. Par-dessus tout, le processus que nous sommes en train d'améliorer et d'optimiser en ce moment permettra d'intégrer les deux volets de la formation pour qu'ils se renforcent mutuellement et fonctionnent bien ensemble.

Le processus obligera les ingénieurs à passer par la formation à différentes étapes du cycle de vie de leurs projets. Comme on s'attend à ce qu'ils participent au processus, la formation leur permettra de savoir comment faire et les aidera à agir. L'objectif consiste très certainement à faire en sorte que les deux volets se renforcent l'un l'autre pour rendre le processus aussi efficace que possible<sup>81</sup>.

M<sup>me</sup> Whitten a aussi expliqué comment Google se tient au fait des règles sur la protection de la vie privée en vigueur dans les divers pays où l'entreprise est active :

Nous avons des experts locaux sur le terrain dans autant de pays que possible... en fait, dans la plupart des pays. En réponse à une question posée plus tôt, j'ai parlé de la nécessité de recourir à toutes sortes d'experts juridiques, techniques, etc.

---

81 *Ibid.*, 1625.

Nous en sommes aussi très conscients sur le plan interculturel. Nous voulons donc que notre examen de vie privée nous donne des perspectives venant de tous les coins de la planète où nos produits sont vus et utilisés. C'est en partie la raison pour laquelle je suis maintenant basée en Europe: je peux ainsi veiller personnellement à apporter un petit peu plus d'équilibre grâce à l'expérience que j'ai acquise aux États-Unis.

Le Canada est certainement l'un des pays auxquels nous prêtons une très grande attention par suite des travaux de votre commissaire à la protection de la vie privée et de son influence sur la scène internationale. Nous comptons beaucoup sur les relations et les contacts étroits de Jacob avec le Commissariat. Nous faisons la même chose dans tous les pays où nous sommes présents<sup>82</sup>.

Dans son témoignage du 25 novembre 2010, M. Glick a confirmé que Google n'avait pas encore détruit les données Wi-Fi qu'elle avait recueillies et qu'elle attendait pour cela les résultats d'une analyse des questions qui pourraient éventuellement empêcher la suppression immédiate des données :

Nous faisons précisément ce que la commissaire a demandé. Nous avons entrepris une analyse de la législation tant canadienne qu'américaine liée au droit de la preuve et à d'autres questions pour déterminer la mesure dans laquelle les données peuvent être supprimées. Entre-temps, nous faisons exactement ce qu'elle a demandé en protégeant les données et en mettant en place les mesures de sécurité nécessaires<sup>83</sup>.

M. Glick a ajouté que, « [e]n fin de compte, notre objectif est de détruire toutes les données. Nous n'en voulions pas au départ et nous n'en voulons pas aujourd'hui. Toutefois, nous voulons éviter de les détruire prématurément en suscitant encore plus de problèmes<sup>84</sup>. » M. Glick s'est engagé à fournir au Comité une liste des pays où Google fait l'objet de poursuites pénales ou de sanctions administratives en raison de la collecte de données utiles Wi-Fi<sup>85</sup>.

Dans une lettre au Comité datée du 9 décembre 2010, M. Glick a fourni les réponses suivantes aux questions du Comité :

**1. Dans quels pays la société Google a-t-elle recueilli par erreur des données utiles provenant de réseaux Wi-Fi non protégés :**

États-Unis d'Amérique, Canada, une grande partie de l'Europe (Autriche, Belgique, République tchèque, Danemark, Finlande, France, Allemagne, Royaume-Uni, Grèce, Hongrie, Irlande, Italie, Luxembourg, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Espagne, Suède et Suisse), Australie, Hong Kong, Japon, Corée du Sud, Macao, Nouvelle-Zélande, Singapour, Taïwan, Brésil, Mexique et Afrique du Sud.

---

82 *Ibid.*, 1645.

83 Jacob Glick, *Témoignages*, réunion n° 34, 25 novembre 2010, 1605, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Mode=1&Parl=40&Ses=3&Language=F#Int-3580901>.

84 *Ibid.*, 1620.

85 *Ibid.*, 1715.

## **2. Où les données utiles ont-elles été stockées :**

Les données utiles recueillies n'importe où dans le monde avant mai 2010, moment où le problème a été découvert et où la collecte a cessé, ont été stockées aux États-Unis et y sont encore.

Les disques durs des véhicules Street View qui n'avaient pas été traités au moment de la découverte du problème ont été mis en sécurité sur une base régionale. Ceux de l'Amérique du Nord, de l'Amérique du Sud et de l'Asie sont aux États-Unis et ceux de l'Europe et de l'Afrique sont en Europe.

## **3. Quelles données utiles ont été détruites :**

Les données utiles désignées comme provenant des pays suivants avaient été détruites de façon sécuritaire à la date de la présente lettre : Irlande, Autriche, Danemark, Hong Kong et Royaume-Uni.

## **4. La société Google a-t-elle été soumise à des accusations au criminel ou à des sanctions ou pénalités administratives pour cette affaire quelque part dans le monde?**

Non<sup>86</sup>.

## **C. Groupe Pages jaunes (Canpages)**

Le 25 novembre 2010, le Comité a entendu aussi François D. Ramsay, premier vice-président, conseiller juridique principal, secrétaire et responsable du respect de la vie privée et Martin Aubut, premier directeur, Commerce social, pour se renseigner sur les améliorations apportées au produit Vue de la rue (Street Scene) de Canpages (Pages jaunes) et déterminer comment l'entreprise intègre la protection de la vie privée à l'élaboration de ses produits.

Dans sa déclaration préliminaire, M. Ramsay a brièvement décrit le Groupe Pages jaunes, qui a fait l'acquisition de Canpages en juin 2010. Il a précisé que le produit Vue de la rue obtient ses données cartographiques aux termes de contrats de licence conclus avec deux sociétés, MapJack et Google. Après que Google a découvert qu'elle avait recueilli des données utiles Wi-Fi, le Groupe Pages jaunes a obtenu confirmation de la part de MapJack que cette dernière n'avait jamais recueilli de données de réseau ou de données utiles Wi-Fi :

Selon l'endroit où on se trouve dans notre univers de sites Web [Yellow Média Inc., le réseau de sociétés qui comprend le Groupe Pages jaunes, la société Trader et Canpages], on utilisera la technologie Street View de Google et de Microsoft, à part celle de MapJack, fournisseur traditionnel de Canpages.

Je suis heureux de confirmer au comité que MapJack, fournisseur du service Street Scene/Scènes de rue de Canpages, n'a pas été utilisé pour recueillir des données

---

86 Lettre de Jacob Glick envoyée par courriel au greffier du Comité, 9 décembre 2010.

réseaux ou des données utiles Wi-Fi. Par conséquent, nous n'avons jamais été en possession de telles données.

Les sociétés Yellow Media Inc., GPJ, Trader et Canpages sont déterminées à se conformer à la législation de protection de la vie privée qui s'applique dans notre secteur<sup>87</sup>.

M. Ramsay et M. Aubut ont dit qu'ils pourraient fournir au Comité confirmation des technologies employées par leurs fournisseurs pour les produits Canpages<sup>88</sup>.

En ce qui concerne la formation des employés du Groupe Pages jaunes sur la protection de la vie privée, M. Ramsay a dit qu'il n'en existait pas encore, mais que sa comparution et le témoignage de M<sup>me</sup> Whitten de Google l'avaient convaincu de s'occuper de ce dossier<sup>89</sup>.

M. Ramsay a indiqué que le Groupe Pages jaunes n'avait jamais directement consulté le Commissariat à la protection de la vie privée au sujet des problèmes potentiels que pourraient présenter ses produits, mais qu'il souhaitait que cela change. Il a dit : « Je peux vous dire cependant que je suis déterminé, avec un certain nombre de mes collègues, à explorer ce domaine et à adopter une approche proactive. Nous comprenons qu'en présence d'un monde de plus en plus numérique, beaucoup de ces questions vont passer au premier plan. Il est donc important pour nous d'être bien préparés et de nous montrer sensibles aux préoccupations légitimes des institutions canadiennes au chapitre de la protection de la vie privée<sup>90</sup>. »

En ce qui concerne Canada Eye, un service reposant sur la géolocalisation lancé par Canpages en mars 2010, M. Ramsay a expliqué ce qui suit :

Je ne sais pas s'il y a des membres du comité qui ont sur eux un iPhone, mais il y a un bouton à pousser sur l'application Canpages. Je connais mieux l'application du GPJ, qui est un concurrent de Canpages. Il s'agit essentiellement de pointer la caméra de l'iPhone dans une certaine direction, ce qui permet d'afficher des noms d'entreprises au moyen du GPS de l'iPhone ou d'un autre téléphone intelligent [...] Je suppose que l'image est en quelque sorte un trucage, dans le sens que ce n'est pas vraiment ce que l'œil voit. C'est simplement que l'iPhone détecte la direction dans laquelle il est pointé et détermine en conséquence les commerces qui se trouvent dans cette direction.

---

87 François Ramsay, *Témoignages*, réunion n° 34, 25 novembre 2010, 1530, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Mode=1&Parl=40&Ses=3&Language=F>.

88 *Ibid.*, 1710.

89 *Ibid.*, 1630.

90 *Ibid.*, 1645.

Je confirme donc qu'à strictement parler, la caméra n'identifie pas vraiment un commerce. Celui-ci est simplement géocodé, ce qui permet au téléphone pointé dans la bonne direction de présenter un affichage correspondant<sup>91</sup>.

M. Ramsay a précisé que, à sa connaissance, les services pour téléphones intelligents comme Canada Eye sont conformes aux lois et politiques canadiennes en matière de protection de la vie privée. Il a signalé que « nous donnons aux gens des itinéraires à suivre en nous fondant, encore une fois, sur des services offerts par des sociétés telles que Google et Microsoft<sup>92</sup> ». Autrement dit, la technologie de géolocalisation n'a pas été mise au point à l'interne par le Groupe Pages jaunes.

## CONCLUSION

Après avoir entendu les témoignages de représentants de Google Canada, de Canpages et du Commissariat à la protection de la vie privée, le Comité est convaincu que toutes les parties concernées traitent avec sérieux les préoccupations de la population canadienne concernant la technologie de l'imagerie à l'échelle de la rue et la protection de la vie privée. Google et Canpages ont, de concert avec le commissariat à la protection de la vie privée, établi des pratiques exemplaires qui visent la communication d'avis aux résidents sur la période au cours de laquelle les véhicules passeront dans les rues, le brouillage obligatoire des visages et des signes distinctifs (comme les numéros des plaques d'immatriculation), la durée de conservation des images et les procédures d'élimination des images en cas de plainte. Le Commissariat a notamment assuré au Comité qu'il continuera de suivre l'évolution de la situation concernant la protection de la vie privée et l'imagerie à l'échelle de la rue pour assurer la conformité aux exigences des lois canadiennes en vigueur. Pour sa part, le Comité continuera de suivre l'évolution de la situation dans ce domaine, en y revenant au besoin.

Cependant, la collecte de données utiles Wi-Fi non protégées soulève une question plus générale : Dans quelle mesure le respect de la vie privée est-il pris en compte à l'étape de l'élaboration de nouvelles technologies? Comme l'a mentionné la commissaire, « la question, c'est pourquoi [Google] n'applique-t-elle pas les principes de protection des renseignements personnels dès le départ? Et pourquoi les contribuables canadiens ou les contribuables espagnols, etc., doivent-ils dépenser beaucoup de temps et d'efforts alors que ces entreprises devraient faire les choses correctement dès le début, avant de lancer leurs produits sur le marché<sup>93</sup>? »

Le Comité estime que les concepteurs de technologies doivent accorder une attention très particulière à la protection de la vie privée à l'étape de l'élaboration de leurs

---

91 *Ibid.*, 1705.

92 *Ibid.*

93 Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, *Témoignages*, réunion n° 25, 19 octobre 2010, 1615, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4702609&Mode=1&Parl=40&Ses=3&Language=F>.

nouveaux projets. Il leur faut cerner les risques éventuels pour la vie privée et les supprimer ou les réduire dès le début des nouveaux projets, au lieu de les affronter après coup à grands frais. Pour ce qui est de l'incident qui a impliqué Google, le Comité fait preuve d'un optimisme prudent, ayant bon espoir que l'entreprise progresse dans la bonne direction par sa décision de nommer Alma Whitten directrice de la protection de la vie privée, de donner de la formation sur la vie privée à ses employés et d'instaurer plus de mesures de contrôle de la vie privée en milieu de travail, comme la vérification de projets en cours d'élaboration. Le Comité compte bien que Google mettra en œuvre les recommandations de la commissaire à la protection de la vie privée sur la collecte de données Wi-Fi formulées dans la *Lettre de conclusions préliminaire* de celle-ci, et ce, d'ici l'échéance du 1<sup>er</sup> février 2011 fixée par la commissaire.

Le Comité note par ailleurs que son étude a permis de sensibiliser le Groupe Pages jaunes à l'importance de la protection de la vie privée et que celui-ci envisage maintenant de former ses employés à ce sujet et de consulter le Commissariat à la protection de la vie privée lors de la conception de ses produits.

Le Comité félicite la commissaire à la protection de la vie privée pour son apport dans ce dossier et pour son travail avec ses homologues étrangers en vue de l'intégration des principes de la « protection intégrée de la vie privée »<sup>94</sup> à la conception des nouveaux produits de l'ère numérique.

---

94 La « protection intégrée de la vie privée » est un concept élaboré par Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario, pour désigner l'intégration, par défaut, des considérations en matière de protection de la vie privée dans la technologie même : <http://www.privacybydesign.ca/about/>. À la 32<sup>e</sup> Conférence internationale des commissaires à la protection des données et de la vie privée tenue à Jérusalem, en Israël, du 27 au 29 octobre 2010, les commissaires ont approuvé la résolution sur la protection intégrée de la vie privée présentée par M<sup>me</sup> Cavoukian et coparrainée par la commissaire à la protection de la vie privée du Canada, ainsi que par des commissaires d'autres pays : <http://www.ipc.on.ca/french/resources/news-releases/news-releases-summary/default.aspx?id=992>.





# LISTE DES RECOMMANDATIONS

---

## RECOMMANDATIONS

1. Compte tenu des profondes transformations qui touchent les médias sociaux et Internet en général, le Comité recommande que le Commissariat à la protection de la vie privée continue de faire preuve de vigilance pour bien protéger la vie privée des Canadiens dans ce contexte et se tenir au courant des questions qui préoccupent les Canadiens à ce sujet.
2. Le Comité soutient les recommandations présentées par la commissaire à la protection de la vie privée dans sa *Lettre de conclusions préliminaire* au sujet de la collecte de données Wi-Fi par Google et demande à Google d'appliquer ces recommandations dès que possible et d'ici l'échéance du 1<sup>er</sup> février 2011 fixée par la commissaire à la protection de la vie privée. Le Comité recommande que la commissaire à la protection de la vie privée communique avec lui dès qu'il aura reçu confirmation que Google s'est conformée aux recommandations précitées.
3. Le Comité recommande aussi que la commissaire à la protection de la vie privée l'avise de toute préoccupation qui pourrait être soulevée au sujet de la mise en application de ses recommandations par Google.
4. Le Comité recommande que la commissaire à la protection de la vie privée précise aux fournisseurs de technologie, comme ceux dont il a entendu le témoignage, l'importance d'avoir des programmes en bonne et due forme de formation sur la protection de la vie privée à l'intention de leurs employés.
5. Le Comité recommande que le Commissariat à la protection de la vie privée poursuive ses activités de sensibilisation – comme la publication de la fiche d'information *Vous êtes photographiés* — La technologie de l'imagerie à l'échelle de la rue, Internet et vous – pour informer le grand public sur ses droits en matière de protection de la vie privée et sur les risques que présentent les nouvelles technologies et les médias sociaux.
6. Enfin, le Comité reprend la recommandation formulée par la commissaire à la protection de la vie privée elle-même, à savoir que les innovateurs comme Google doivent intégrer les principes de la protection de la vie privée à la conception des nouveaux produits et consulter la commissaire, ainsi que, au besoin, ses homologues étrangers, de façon à garantir la protection de la vie privée dans le monde numérique.





## ***VOUS ÊTES PHOTOGRAPHIÉS*** **LA TECHNOLOGIE DE L'IMAGERIE À L'ÉCHELLE DE LA RUE, INTERNET ET VOUS**

De nombreuses entreprises ont commencé à recueillir des images de lieux publics canadiens qui peuvent ensuite être vues sur Internet ou par d'autres moyens. Des personnes peuvent être captées sur ces images, parfois de façon non intentionnelle. Une des applications les plus connues est Street View de Google qui permet à ses utilisateurs d'effectuer des « visites virtuelles » de villes comme Paris, Londres, New York et, un jour, de grands centres urbains du Canada. En outre, Canpages fournit des images fixes provenant de caméras de circulation routière locale. D'autres applications ont également été élaborées pour des domaines comme la géomatique, l'arpentage, la cartographie et l'urbanisme.

Au Canada, les lois sur la protection des renseignements personnels dans le secteur privé visent ces applications de l'imagerie à l'échelle de la rue quand elles recueillent des images de personnes identifiables. Bien que les commissaires à la protection de la vie privée du Canada, de la Colombie-Britannique, de l'Alberta et du Québec reconnaissent la popularité de ces applications, ils ont également exprimé des réserves au fait que cette technologie permet non seulement de saisir des images d'endroits, mais également des images des personnes qui s'y trouvent.

Les commissaires croient que les Canadiennes et les Canadiens doivent être conscients des enjeux de protection de la vie privée que ces applications peuvent soulever.

### **LES PERSONNES DANS LES LIEUX PUBLICS**

On croit souvent à tort qu'une entreprise n'a pas besoin de votre autorisation pour vous prendre en photo dans un lieu public.

En fait, la législation canadienne sur la protection des renseignements personnels prévoit, notamment, que vous devez être au courant lorsqu'on vous photographie à des fins commerciales et connaître l'utilisation qui sera faite de votre image. On doit également obtenir votre consentement<sup>1</sup>. Il y a des exceptions à cette règle, mais elles sont très limitées et précises<sup>2</sup>.

Toutefois, dans le cas de certaines des nouvelles applications de l'imagerie à l'échelle de la rue, vous ne savez pas toujours quand votre photo est prise. C'est la raison pour laquelle nous croyons que les entreprises qui s'adonnent à ce type d'activité doivent déployer davantage d'efforts pour faire savoir aux citoyens qu'elles vont photographier les rues de leur ville, le moment où cela se produira, la raison de cette activité et le moyen par lequel ils peuvent demander à ce que leur photo ne soit pas versée dans la banque de données. Par exemple, les véhicules utilisés pour enregistrer l'information pourraient porter des marques visibles, et l'on pourrait utiliser une vaste gamme de moyens (communiqué de presse, médias régionaux, site Web du service) pour diffuser les renseignements sur les dates et emplacements de tournage, la raison pour laquelle on procède à ce dernier et la manière dont on peut communiquer avec l'entreprise pour obtenir davantage de renseignements. La plupart des gens ne s'attendent probablement pas à ce que leur photo soit prise par une entreprise dans le cours de leurs activités quotidiennes, mais cela peut les déranger moins s'ils ont le choix de planifier leur journée en conséquence.

## **LA DIMENSION DE LA PROTECTION DE LA VIE PRIVÉE ET VOTRE IMAGE EN LIGNE**

Les applications de l'imagerie à l'échelle de la rue utilisent divers moyens pour photographier le paysage urbain. De façon générale, une caméra est montée sur un véhicule qui parcourt les rues de villes choisies. Les images peuvent ensuite être visualisées sur Internet.

Les commissaires à la protection de la vie privée ont tenu des discussions avec diverses entreprises pour renforcer les mécanismes de protection des personnes dont la photo a été prise. Nous croyons que toutes les entreprises qui offrent de telles applications doivent prendre des mesures pour mieux protéger votre vie privée.

En plus de demander aux entreprises d'être plus proactives et originales dans leurs communications avec le public pour veiller à ce que les Canadiennes et les Canadiens soient informés du moment où leurs villes — et par conséquent eux-mêmes — pourraient être photographiées, nous croyons qu'elles devraient adopter une attitude plus sensible au respect de la vie privée lorsqu'elles choisissent les endroits à photographier. Les personnes qui pénètrent dans des lieux, comme des refuges ou des cliniques d'avortement, où la confidentialité est d'une importance capitale ou qui en sortent veulent vraisemblablement conserver l'anonymat pour des raisons liées à leur vie privée ou à leur sécurité.

Les entreprises devraient également utiliser des technologies de brouillage efficaces et éprouvées des visages et des numéros de plaques d'immatriculation de façon à ce que les personnes ne puissent être identifiées lorsque leurs photos sont affichées sur Internet. Dans ces cas, les entreprises devraient offrir des mécanismes rapides et réactifs qui permettent de bloquer ou de retirer les images.

Les entreprises qui offrent ces applications d'imagerie doivent également avoir une bonne raison pour conserver les images originales et non brouillées dans leurs bases de

données. Si elles conservent des images non brouillées, elles doivent cependant limiter la période durant laquelle elles les gardent et les protéger avec des mesures de sécurité appropriées.

## LE FACTEUR DÉCISIF

La technologie de l'imagerie à l'échelle de la rue peut comporter des avantages, mais ceux-ci ne doivent pas l'emporter sur votre vie privée.

C'est la raison pour laquelle nous encourageons les entreprises de technologie à prendre les moyens nécessaires pour que vous puissiez continuer à profiter de vos droits en matière de protection de la vie privée, même lorsque vous êtes simplement au parc, que vous promenez votre chien ou que vous profitez du soleil dans votre cour.

### Fédéral

Commissariat à la protection de la vie privée du Canada  
[www.priv.gc.ca](http://www.priv.gc.ca)

### Provincial

Information and Privacy Commissioner of Alberta  
[www.oipc.ab.ca](http://www.oipc.ab.ca)

Information and Privacy Commissioner for British Columbia  
[www.oipc.bc.ca](http://www.oipc.bc.ca)

Commission d'accès à l'information du Québec  
[www.cai.gouv.qc.ca](http://www.cai.gouv.qc.ca)

<sup>1</sup> Le consentement peut être explicite ou implicite.

<sup>2</sup> En général, selon les lois visant la protection de la vie privée dans le secteur privé, l'information et le consentement ne sont pas nécessaires aux fins journalistiques, artistiques ou littéraires. D'autres exceptions figurent dans les quatre lois sur la protection de la vie privée pertinentes, soit la [\*Loi sur la protection des renseignements personnels et les documents électroniques\*](#), la [\*Personal Information Protection Act\*](#) (Colombie-Britannique), la [\*Personal Information Protection Act\*](#) (Alberta) et la [\*Loi sur la protection des renseignements personnels dans le secteur privé\*](#).



### LETTRE DE CONCLUSIONS PRÉLIMINAIRE

#### **Plaintes déposées en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (la Loi)**

- 1) Après avoir appris que les voitures de Google Street View avaient recueilli des données utiles transmises par des réseaux Wi-Fi non cryptés dans le cadre de la collecte de signaux Wi-Fi publics (des renseignements sur les identificateurs d'ensemble de services et des adresses MAC), le Commissariat à la protection de la vie privée du Canada a déposé trois plaintes contre Google inc. (Google) le 31 mai 2010, conformément au paragraphe 11(2) de la Loi.
- 2) Les trois plaintes sont les suivantes:
  - i. Google aurait recueilli, utilisé ou communiqué des données utiles sans avis et consentement préalable ;
  - ii. Google aurait recueilli des données utiles sans déterminer les fins de la collecte de renseignements personnels au préalable ;
  - iii. Google aurait recueilli des données utiles au-delà de ce qui est nécessaire aux fins déterminées.

#### **Résumé de l'enquête**

- 3) Après que l'autorité allemande de protection des données à Hambourg a demandé de soumettre à une vérification les données Wi-Fi recueillies par les voitures de Google Street View au cours d'un projet fondé sur la localisation, Google a découvert en mai 2010 qu'elle avait recueilli des données utiles transmises sur des réseaux sans fil non protégés dans le cadre de ses activités de collecte de données Wi-Fi. Selon l'entreprise elle-même, cette collecte accidentelle semble avoir été causée par l'intégration d'un code élaboré en 2006 au logiciel utilisé pour capter les signaux Wi-Fi. Devant cette situation, Google a immobilisé ses voitures Street View, arrêté de recueillir des données sur les réseaux Wi-Fi le 7 mai 2010, et isolé et stocké toutes les données déjà recueillies.
- 4) Le 1<sup>er</sup> juin 2010, le Commissariat a écrit à Google pour aviser l'entreprise qu'il lançait une enquête concernant cette collecte de données utiles. Google a répondu le 29 juin 2010.

- 5) Le 28 juin 2010, conformément au paragraphe 11(2) de la *Loi*, le Commissariat a demandé de visiter les locaux de Google à Mountain View (Californie). La visite sur place avait un double objectif : 1) examiner les données utiles recueillies par Google et 2) poser des questions précises aux représentants de l'entreprise, par exemple sur les circonstances de l'incident, l'isolement et le stockage des données utiles et les mesures d'atténuation et de prévention que Google prévoit mettre en œuvre.
- 6) Google a accepté une visite sur les lieux. Deux représentants spécialisés du Commissariat se sont ensuite rendus dans les locaux de Mountain View, le 19 juillet 2010. Bien que nos spécialistes aient passé en revue les données utiles, aucun représentant de Google n'était disponible pour répondre à nos questions à Mountain View. Google a plutôt répondu à nos questions générales en remplissant un questionnaire que nous lui avons transmis le 12 juillet 2010.
- 7) Le 18 août 2010, une téléconférence a eu lieu entre un avocat de Google et le Commissariat pour répondre à des questions supplémentaires.
- 8) Les résultats de notre enquête sur les trois plaintes déposées contre Google sont résumés dans les sections suivantes:
  - A. La participation du conseiller juridique en matière de produits de Google à l'examen des produits;
  - B. Les circonstances entourant la collecte de données utiles et les essais techniques;
  - C. La collecte de renseignements personnels;
  - D. L'isolement et le stockage des données utiles;
  - E. Les plans d'avenir de Google concernant ses services géodépendants;
  - F. Les répercussions des plans d'avenir sur la vie privée et les mesures d'atténuation et de prévention que Google prévoit prendre pour éviter une récurrence.

**A. La participation du conseiller juridique en matière de produits de Google à l'examen des produits**
- 9) Google a expliqué qu'elle dispose d'un processus d'examen officiel pour chaque lancement de produit externe (c'est-à-dire un produit offert aux consommateurs). Ce processus prévoit qu'un conseiller juridique en matière de produits doit évaluer notamment les répercussions du produit sur la vie privée.



- 10) Google considère que le code qui a finalement servi à relever toutes les catégories de données Wi-Fi publiques n'est pas un produit externe. Le processus d'examen officiel ne s'est donc pas appliqué.
- 11) Cependant, notre enquête a dévoilé que la procédure d'élaboration de code de Google comprend un modèle et un processus selon lesquels le conseiller juridique en matière de produits doit examiner le code avant que celui-ci ne soit utilisé ou intégré à un autre produit de Google. Le modèle — un document qui explique la méthodologie — est pour ainsi dire obligatoire et constitue la première étape de la procédure d'élaboration d'un code.
- 12) L'enquête a aussi révélé que, dans le document établissant la procédure d'élaboration du code qui allait servir à capter les signaux Wi-Fi, l'ingénieur a cerné une ou plusieurs préoccupations relatives à la collecte. Ces préoccupations étaient liées au fait que Google pourrait obtenir suffisamment de données pour trianguler avec précision l'emplacement d'un utilisateur à un certain moment.
- 13) L'ingénieur a affirmé que ses préoccupations avaient des répercussions superficielles sur la vie privée. Il n'a pas envoyé ses documents sur l'élaboration du code au conseiller juridique en matière de produits aux fins d'examen - ce qui contrevient à la procédure de l'entreprise. Les facteurs relatifs à la vie privée du code n'ont donc jamais été évalués.
- 14) Nous avons aussi appris que les membres du service juridique en matière de produits de Google étaient des avocats qui avaient des antécédents professionnels dans divers secteurs du droit. Google soutient que ces juristes ont généralement une certaine expérience des questions liées à la protection des renseignements personnels dans le secteur privé.
- 15) Selon Google, les membres du service juridique en matière de produits assistent à la même séance de formation de base que tous les nouveaux employés de l'entreprise. En outre, ils participent à des réunions hebdomadaires sur des enjeux liés à la protection de la vie privée et à la sécurité. Google affirme également que la formation juridique continue obligatoire pour les conseillers juridiques de Google comprend la protection de la vie privée

## **B. Les circonstances entourant la collecte de données utiles et les essais techniques**

- 16) Google permet à ses ingénieurs de consacrer 20 % de leur temps à des projets qui les intéressent. En 2006, un des ingénieurs a consacré ce temps à la création d'un code visant à prélever des échantillons de toutes les catégories de données Wi-Fi publiques.

- 17) L'ingénieur en question a ajouté des lignes de code permettant de recueillir des données utiles. Il a pensé que cela pourrait éventuellement servir à Google et qu'une telle collecte serait appropriée.
- 18) Google a utilisé ce code lorsqu'elle a décidé de lancer un certain service géodépendant qui se basait sur divers signaux (comme les GPS et l'emplacement de stations de base et de points d'accès Wi-Fi) pour indiquer un endroit à un utilisateur. Elle a installé des antennes et les logiciels requis (dont Kismet, une application libre) à bord de ses voitures Street View afin de capter les signaux Wi-Fi publics à portée de ces véhicules pendant que ceux-ci circulent dans un quartier. Les signaux étaient ensuite traités pour identifier les réseaux Wi-Fi (à l'aide de leur adresse MAC) et cerner leur emplacement approximatif (à l'aide des coordonnées fournies par le GPS au moment où le signal était reçu). Les renseignements sur l'identité des réseaux Wi-Fi et leur emplacement approximatif alimentent ensuite la base de données des services géodépendants de Google.
- 19) Dans ses observations présentées au Commissariat, Google a fourni des renseignements techniques sur sa façon d'utiliser les données transmises par les réseaux Wi-Fi pour les services géodépendants. Elle a mentionné que son logiciel n'enregistre pas les données utiles transmises par des réseaux cryptés, mais que les données utiles diffusées sur des réseaux Wi-Fi non cryptés sont recueillies et enregistrées sur un disque en format brut.
- 20) Toutefois, selon Google, les renseignements ainsi recueillis seraient fragmentés puisque les voitures sont en mouvement au moment de la collecte et que l'équipement servant à recueillir les signaux Wi-Fi automatiquement change de fréquence cinq fois par seconde.
- 21) Au cours de notre enquête, Google a reconnu avoir erré en insérant un code permettant de recueillir des données utiles dans le logiciel de collecte de renseignement sur les réseaux Wi-Fi. Elle soutient que le code a surtout été conçu pour un logiciel de collecte de données, et que cet objectif avait préséance sur son utilisation ultime dans le cadre de la collecte de renseignements sur les réseaux Wi-Fi pour des services géodépendants. Google affirme qu'elle n'était pas consciente de la présence de ce code lorsqu'elle a commencé à utiliser le logiciel pour son projet de géolocalisation.
- 22) Selon Google, quand l'entreprise a décidé d'utiliser le logiciel pour recueillir des renseignements publics sur les réseaux Wi-Fi, le code a été examiné pour découvrir les bogues, puis validé par un deuxième ingénieur avant d'être installé à bord des voitures Street View. Cette opération visait à s'assurer que le code ne nuirait pas aux opérations habituelles de Street View. Aucune vérification approfondie n'a été effectuée pour vérifier le

genre de données obtenues au moyen de la réception de signaux publics sur des réseaux Wi-Fi.

- 23) Google a admis que, puisqu'elle n'avait pas l'intention de recueillir des données utiles et qu'elle n'a jamais voulu inclure de telles données dans l'un ou l'autre de ses produits, elle ne pouvait ni indiquer la fin de la collecte ni obtenir le consentement des personnes touchées. Elle a également avoué qu'elle n'avait pas avisé les personnes concernées par la collecte de données utiles puisque les employés n'étaient pas conscients qu'ils en avaient recueillies avant mai 2010.
- 24) Google a invoqué trois raisons expliquant pourquoi la collecte de données utiles n'a pas été découverte plus tôt:
  - i. Hormis l'ingénieur qui a élaboré le code, aucun employé n'était intéressé à examiner ce programme : personne ne croyait que les données utiles pourraient servir et personne n'avait l'intention d'utiliser ces données.
  - ii. Étant donné que les données utiles formaient une infime partie de l'ensemble des données recueillies, leur collecte n'était guère préoccupante et il n'y avait aucune raison de les examiner.
  - iii. L'ingénieur n'a pas anticipé les conséquences de l'inclusion de ce code et n'a donc pas abordé la question avec son gestionnaire.
- 25) Google a aussi affirmé que, puisque la collecte de données utiles ne présente aucun intérêt, rien ne justifie de les conserver. Par conséquent, Google prévoit les détruire de façon sécuritaire aussitôt que possible, et elle demande l'autorisation du Commissariat pour s'exécuter.
- 26) Notre enquête a révélé que Google a recueilli des données Wi-Fi au Canada du 30 mars 2009 au 7 mai 2010 et que les voitures Street View ont sillonné la plupart des régions urbaines et des routes principales.
- 27) Google souligne qu'elle ne peut distinguer précisément les réseaux Wi-Fi des appareils sans fil. Elle peut toutefois cerner le numéro unique des identificateurs d'ensemble de services de base (IDESB), qui identifient généralement un point d'accès Wi-Fi unique. Les IDESB permettent d'identifier un point d'accès, mais ils n'indiquent pas combien d'appareils ou de réseaux s'y connectent.
- 28) Google estime avoir recueilli plus de 6 millions d'IDESB pendant que ses voitures Street View parcouraient le Canada.

### **C. La collecte de renseignements personnels**

- 29) Les deux spécialistes du Commissariat ont visité les bureaux de Google à Mountain View (Californie) les 19 et 20 juillet 2010. L'objectif de cette visite était d'examiner les données recueillies pour les services géodépendants par les voitures de Google Street View afin d'en déterminer la nature et la quantité. L'examen visait principalement à trouver des exemples de renseignements personnels dans les données utiles tirées des réseaux Wi-Fi du Canada.
- 30) Nos spécialistes ont effectué des recherches dans les données utiles pour trouver tout ce qui pourrait constituer un renseignement personnel (p. ex. des courriels, des noms d'utilisateur, des mots de passe et des numéros de téléphone). Ils ont fait un décompte approximatif des renseignements personnels au moyen d'une recherche automatisée. Pour donner un ordre de grandeur, le décompte comprenait 787 en-têtes de courriel et 678 numéros de téléphone. Cependant, ces recherches peuvent comprendre des résultats non pertinents ou passer outre certains éléments.
- 31) Pour compléter la recherche automatisée, nos spécialistes ont vérifié manuellement cinq occurrences de chaque type de renseignement personnel. L'objectif était de prouver l'existence de chacun de ces types de données sans envahir indûment la vie privée des personnes concernées.
- 32) Nos spécialistes ont découvert au moins cinq courriels dont ils ont vu les adresses, les en-têtes complets, les adresses IP, les noms d'hôte des appareils et le contenu des messages. Les cinq messages étaient tronqués, mais les spécialistes ont trouvé des courriels complets en vérifiant manuellement d'autres éléments (comme des numéros de téléphone).
- 33) Cinq noms d'utilisateur ont aussi été découverts. Ils se trouvaient dans les témoins de connexion, les messages transmis par MSN et les séances de clavardage. Les spécialistes ont aussi trouvé un cas où un mot de passe et un mot d'utilisateur étaient compris dans un courriel destiné à expliquer à des gens comment se connecter à un serveur.
- 34) Nos spécialistes ont aussi trouvé cinq noms de personnes véritables, cinq adresses résidentielles et cinq autres adresses d'entreprises. Ils ont remarqué que, contrairement aux adresses résidentielles, les adresses d'entreprises étaient très répandues.
- 35) Ils ont aussi trouvé cinq messages instantanés et cinq numéros de téléphone -tant d'entreprises et que de résidences. Tout comme les adresses, les numéros de téléphone des entreprises étaient plus faciles à trouver que les numéros personnels.

- 36) Les recherches de numéros à 9 ou à 16 chiffres, qui auraient pu être des numéros d'assurance sociale (NAS) ou de carte de crédit, n'ont donné aucun résultat puisqu'il y avait trop de numéros non pertinents ou semblables dans l'ensemble des données. Par conséquent, bien que nous n'ayons pas trouvé la preuve que des numéros d'assurance sociale ou de carte de crédit étaient recueillis, la possibilité ne peut être exclue.
- 37) Nos spécialistes ont aussi découvert des éléments sensibles, comme une liste de noms, de numéros de téléphone, d'adresses et de problèmes de santé liés à des personnes précises. Ils ont aussi trouvé une allusion à une personne arrêtée pour excès de vitesse, avec son adresse.
- 38) Les spécialistes ont vu de nombreux témoins transmis par des ordinateurs clients à des serveurs Web. Ces témoins n'étaient pas cryptés et certains d'entre eux comprenaient des renseignements personnels comme des adresses IP, des noms d'utilisateur et des adresses postales. Les enquêteurs ont été surpris du nombre de témoins non cryptés qui comprenaient des renseignements personnels.
- 39) Bref, nos spécialistes ont trouvé de nombreux renseignements personnels dans l'échantillon prélevé des données utiles recueillies au Canada par Google.

#### **D. L'isolement et le stockage des données utiles**

- 40) Les données Wi-Fi ont été captées au moyen d'antennes installées sur le toit des voitures Street View. Cette antenne recevait passivement les signaux radio publics à portée de la voiture à l'aide du logiciel libre Kismet. Les données étaient ensuite transmises à l'application « gStumbler », créée par Google, et à son programme exécutable « gslite », qui traitait les données en vue du stockage. Les données étaient ensuite enregistrées sur des disques durs physiques placés dans chaque voiture Street View, puis transférées sur les serveurs de Google.
- 41) Google affirme avoir interrompu les activités de ses voitures Street View et isolé les données utiles dans une zone d'accès restreint de son réseau dès qu'elle a pris conscience que l'application gStumbler recueillait les données utiles des réseaux Wi-Fi non cryptés.
- 42) Par la suite, un administrateur système de Google a copié sur un total de quatre disques les fichiers comprenant les données utiles recueillies dans tous les pays touchés. Cette opération s'est déroulée du 9 au 13 mai 2010. Les disques contenaient deux copies des données : la première a été obtenue après le classement par catégorie et l'étiquetage des dossiers de données par pays, et la seconde, avant le classement des données.

- 43) Le 15 mai 2010, l'administrateur système a réuni les données utiles sur un disque dur crypté et les a divisées par pays. Une copie de sauvegarde du disque dur crypté a été enregistrée. Les quatre premiers disques ont été détruits dans un outil de déformation physique.
- 44) Un employé de Google a livré en main propre un disque dur crypté à un autre bureau de l'entreprise aux fins de sauvegarde; l'administrateur système a conservé l'autre disque en lieu sûr. Lorsque l'employé de Google est arrivé à destination, l'administrateur système a détruit définitivement le disque dur crypté de sauvegarde. Les données américaines ont été isolées sur un disque crypté distinct alors que les données du reste du monde sont demeurées sur le disque crypté d'origine.

#### **E. Les plans d'avenir de Google concernant ses services géodépendants**

- 45) Google a toujours l'intention d'offrir des services géodépendants, mais ne prévoit pas reprendre la collecte de données Wi-Fi au moyen de voitures Street View. Cette collecte est interrompue et Google ne prévoit pas la reprendre.
- 46) Google n'a pas l'intention d'impartir à une tierce partie la cueillette des données Wi-Fi.
- 47) L'entreprise pense plutôt se servir des appareils portables de ses utilisateurs pour recueillir les renseignements sur l'emplacement des réseaux Wi-Fi dont elle a besoin pour sa base de données sur les services géodépendants. L'amélioration des téléphones intelligents au cours des dernières années a permis à Google de recueillir les données requises à cette fin à partir des appareils portables eux-mêmes.
- 48) Bien qu'elle ne dispose d'aucun outil pour faire le suivi des déplacements d'un consommateur (et elle n'a pas l'intention d'en créer un), Google convient qu'elle doit examiner les problèmes que pourrait poser cette méthode de collecte relativement à la vie privée.

#### **F. Les répercussions des plans d'avenir sur la protection de la vie privée et les mesures d'atténuation et de prévention**

- 49) Google fait valoir qu'elle tente d'intégrer des mesures de protection des renseignements personnels dans tous ses produits et services. Elle affirme que ses employés reçoivent une séance de formation initiale et une formation sur le code de déontologie qui comprennent une partie sur la protection des renseignements personnels et la sécurité des données. Cependant, la responsabilité d'harmoniser tous les projets de Google avec les principes et les politiques de l'entreprise en matière de protection

de la vie privée incombe à toutes les équipes de production et de conception.

- 50) Google soutient également que, lorsque les produits sont approuvés ou que les ressources et le personnel leur sont attribués, ils sont confiés à un conseiller juridique en matière de produits de l'entreprise. Il a une responsabilité de premier niveau pour ce qui est de cerner les préoccupations liées à la protection de la vie privée liées à un produit.
- 51) Pour éviter qu'un autre produit ait des répercussions néfastes sur la vie privée, Google dit examiner ses procédures liées au lancement de produits et à l'examen de code, ainsi que sa politique qui consiste à laisser ses employés décider de 20 % de leur emploi du temps. Ces mesures feraient en sorte que les contrôles internes seraient suffisamment efficaces pour aborder adéquatement les futurs enjeux. Au moment de la diffusion du présent rapport, l'examen de Google sur ses politiques et procédures n'était pas encore terminé.

### **Application**

- 52) Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.1 et 4.1.2 de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Selon le principe 4.1.1, il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes, même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidien des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées. Selon le principe 4.1.2, il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.
- 53) Nous avons également appliqué le principe 4.2, qui précise que les fins pour lesquelles les renseignements personnels sont recueillis doivent être établies par l'organisation avant ou pendant la collecte.
- 54) Le principe 4.3 stipule que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
- 55) Enfin, le principe 4.4 indique que l'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées par l'organisation.

### **Conclusions**

- 56) Le 15 septembre 2010, j'ai transmis à Google une version préalable du présent rapport et invité l'organisme à formuler une réponse. J'ai révisé la

présente lettre de conclusions préliminaire en tenant compte de la réponse de Google. Les paragraphes qui suivent sont un résumé de nos conclusions et de nos recommandations.

### **Collecte de renseignements personnels**

- 57) Au cours de leur visite sur les lieux, nos spécialistes ont découvert une quantité substantielle de renseignements personnels sous la forme de contenu de courriels (p. ex des adresses courriel, IP et postales) parmi les données utiles recueillies par Google au Canada.
- 58) Google a avoué au Commissariat qu'elle avait recueilli des données utiles, mais sans avoir l'intention de les utiliser dans l'un ou l'autre de ses produits. Elle affirme avoir tout simplement recueilli les données par erreur et n'a pas demandé le consentement des personnes touchées. Le principe 4.3 de la *Loi* exige que la personne concernée consente à la collecte, à l'utilisation et à la communication de renseignements personnels.
- 59) Google déclare aussi que la collecte de données utiles n'avait aucun objectif. Or, le principe 4.2 stipule que l'objectif doit être établi avant la collecte ou au moment de celle-ci. En outre, le principe 4.4 précise que seuls les renseignements personnels nécessaires aux fins déterminées doivent être recueillis. Étant donné qu'aucune fin n'a été établie, la collecte de données ne pouvait évidemment pas être limitée par un objectif précis, ce qui est contraire au principe 4.4.

### **La participation du conseiller juridique en matière de produits de Google à l'examen des produits**

- 60) Puisque l'ingénieur a omis de transférer son document de conception au conseiller juridique en matière de produits, ce dernier n'a pas pu évaluer les répercussions sur la vie privée du code visant à recueillir les données Wi-Fi. Je considère que cette négligence est très grave puisque l'examen des documents de conception par un conseiller juridique en matière de produits (et l'utilisation d'un modèle) est manifestement une étape obligatoire prévue dans la procédure d'élaboration de code de Google.
- 61) Le code non étudié a plus tard servi à recueillir des données comprenant des renseignements personnels. Si le conseiller juridique en matière de produits avait été mis à contribution comme il aurait dû l'être, Google aurait peut-être découvert le risque d'une collecte excessive et remédié à la situation avant que des données ne soient recueillies. Les répercussions négatives sur la vie privée des citoyens et sur la réputation de Google auraient facilement pu être évitées.



- 62) Google a indiqué au Commissariat qu'il incombe aux équipes de l'ingénierie et de l'élaboration de produits de respecter les politiques et les principes en matière de protection de la vie privée de l'entreprise. Google a ensuite déclaré qu'elle déploie des efforts en vue d'améliorer les processus d'examen des codes et des produits, ainsi que les mécanismes de responsabilisation, que doivent suivre le personnel de l'ingénierie et de la gestion de produits afin de les sensibiliser davantage aux enjeux de vie privée à toutes les étapes d'élaboration de produits et de codes. Une équipe juridique travaille avec les directeurs de l'ingénierie pour s'assurer qu'un examen exhaustif des codes est effectué afin de déterminer si ces derniers pourraient soulever des questions liées à la vie privée. Google estime que l'examen des politiques et des procédures qu'elle a entrepris fera en sorte que la situation ne se reproduira plus. Google a déclaré qu'elle tiendra le Commissariat au courant de la progression de l'examen.

### **Examen et essai du code**

- 63) Google soutient que l'ingénieur qui a élaboré les lignes de code ne se doutait pas que leur utilisation aboutirait à la collecte d'une vaste gamme de données transmises par des réseaux sans fil. Notre enquête n'a pas permis de déterminer s'il s'agissait d'une erreur ponctuelle d'une seule personne ou si c'était le signe que les employés en général ne sont pas suffisamment sensibilisés aux répercussions des nouveaux produits sur la vie privée. Chez Google, ces conséquences devraient être bien comprises par les conseillers juridiques en matière de produits, mais aussi par les professionnels qui mettent au point ces produits.
- 64) Dans le présent cas, l'examen et l'essai du produit contenant le code n'ont pas permis d'évaluer l'incidence sur la vie privée. Il semble que l'examen visait seulement à s'assurer que le produit ne nuirait pas à une deuxième application — celle qui a servi à prendre des images des rues où circulaient les véhicules Street View.
- 65) Notre enquête a démontré que l'examen n'a pas suffi à évaluer toutes les capacités du produit — y compris celle de recueillir des données qui ne sont pas nécessaires au projet de géolocalisation.

### **Mesures prises pour protéger les données utiles**

- 66) Lorsque Google a remarqué que ses voitures Street View recueillaient plus de données transmises par les réseaux sans fil que prévu, elle a exprimé du regret quant à la collecte par inadvertance des données diffusées publiquement. Elle a immédiatement immobilisé ses véhicules et pris des mesures pour protéger les données utiles et les isoler par pays d'origine.

- 67) La démarche de Google était justifiée, appropriée et suffisante pour protéger les données utiles recueillies au Canada. Je crois que l'entreprise a respecté les clauses pertinentes de la *Loi*.
- 68) Pour ce qui est des données que Google a recueillies, l'entreprise a affirmé qu'elle n'avait aucunement l'intention d'utiliser les données utiles canadiennes de quelque façon que ce soit, et qu'elle continuera de garder les données en toute sécurité et d'en restreindre activement l'accès d'ici à ce que ces données soient supprimées.
- 69) Je tiens à ajouter ici que l'on doit tenir compte non seulement des lois sur la protection des renseignements personnels, mais aussi d'autres lois canadiennes et américaines, y compris les règles de droit sur la preuve, afin de déterminer le moment opportun pour supprimer les données utiles canadiennes recueillies.

### **Plans d'avenir**

- 70) Le fait que Google n'a pas l'intention de reprendre la collecte de données Wi-Fi à l'aide de ses voitures Street View élimine le risque d'une nouvelle collecte de renseignements personnels inappropriée au moyen de l'outil conçu par l'ingénieur.
- 71) Cependant, Google prévoit recueillir des renseignements à partir des appareils portables des utilisateurs pour alimenter sa base de données sur les services géodépendants. Cette nouvelle méthode pourrait aussi mener à la collecte et à la conservation inappropriées de renseignements personnels si Google ne prenait pas les mesures de protection qui s'imposent.

### **Recommandations**

- 72) Je partage l'objectif de Google visant à éviter que des atteintes similaires à la vie privée des personnes se reproduisent. Bien que je sois heureuse de constater que Google a entrepris l'examen des processus et des procédures pouvant avoir une incidence sur la protection de la vie privée, je souhaite néanmoins que l'organisation complète ces mesures de contrôle par un modèle de gouvernance global qui tient compte de toutes les questions liées à la protection de la vie privée associées à la conception de produits et de services internes et externes. J'aimerais également que Google respecte des échéanciers raisonnables pour la mise en œuvre tant du modèle de gouvernance que des procédures et des processus révisés. C'est dans cette optique et à la lumière des renseignements supplémentaires que Google a présentés au Commissariat que j'é mets les recommandations suivantes :

- i. Que Google réexamine et améliore la formation offerte à tous les employés au sujet du respect de la vie privée, dans le but d'améliorer la conscientisation et la connaissance des employés quant aux obligations de Google en vertu des lois sur la protection des renseignements personnels.
  - ii. Que Google instaure un modèle de gouvernance qui comprenne :
    - des mesures de contrôle efficaces visant à faire en sorte que toutes les procédures nécessaires au respect de la vie privée ont bel et bien été suivies avant le lancement de tout produit;
    - la désignation et l'identification claires de personnes responsables du respect des obligations de Google en vertu des lois sur la protection des renseignements personnels.
  - iii. Que Google supprime les données utiles canadiennes recueillies, dans la mesure où elle est habilitée à le faire aux termes des lois canadiennes et américaines. Si les données utiles canadiennes ne pouvaient pas être supprimées sur le champ, elles devraient être conservées de manière sécuritaire et l'accès à ces données devrait être restreint.
- 73) À l'heure actuelle, j'estime que la plainte est **fondée** et demeure **non résolue**. Le Commissariat ne considérera l'affaire résolue que si Google lui remet au plus tard le 1er février 2011 la confirmation que les recommandations formulées ci-dessus ont été mises en œuvre; j'émettrai à ce moment mes conclusions et mon rapport finaux.



## ANNEXE C

# LISTE DES TÉMOINS DEUXIÈME SESSION, 40<sup>e</sup> LÉGISLATURE

Organisations et individus	Date	Réunion
<p><b>Canpages inc.</b> Olivier Vincent, président et chef de direction</p>	2009/06/17	29
<p><b>Google inc.</b> Jonathan Lister, directeur général et chef de Google Canada</p>		
<p><b>Commissariat à la protection de la vie privée du Canada</b> Carman Baggaley, conseiller en politiques stratégiques Daniel Caron, conseiller juridique, Direction des services juridiques, des politiques et des affaires parlementaires Elizabeth Denham, commissaire adjointe à la protection de la vie privée</p>	2009/10/22	32

# TROISIÈME SESSION, 40<sup>e</sup> LÉGISLATURE

Organisations et individus	Date	Réunion
<p><b>Commissariat à la protection de la vie privée du Canada</b> Daniel Caron, conseiller juridique, Direction des services juridiques, des politiques et des affaires parlementaires Patricia Kosseim, avocate générale Andrew Patrick, analyste de recherche en technologie de l'information</p>	2010/10/28	28
<p><b>Google inc.</b> Jacob Glick, conseiller en matière de politique au Canada</p>	2010/11/04	30
<p><b>Google inc.</b> Jacob Glick, conseiller en matière de politique au Canada Alma Whitten, chef technique à la protection de la vie privée</p>	2010/11/25	34

## **Groupe Pages Jaunes Cie**

Martin Aubut, premier directeur,  
Commerce social

François D. Ramsay, premier vice-président, conseiller  
juridique principal, secrétaire et responsable du respect de la  
vie privée

## **ANNEXE D**

# **LISTE DES MÉMOIRES DEUXIÈME SESSION, 40<sup>E</sup> LÉGISLATURE**

---

### **Organisations et individus**

---

**Google inc.**





# PROCÈS-VERBAUX

Un exemplaire des procès-verbaux pertinents ([40<sup>e</sup> législature, 3<sup>e</sup> session : séances n<sup>os</sup> 28, 30, 32, 34, 37 et 39](#)) et ([40<sup>e</sup> législature 2<sup>e</sup> session : séances n<sup>os</sup> 29 et 32](#)) est déposé.

Respectueusement soumis,

Le président,

L'hon. Shawn Murphy, C.P., député

