HOUSE OF COMMONS
CANADA

MAPPING PRIVACY PROTECTION IN THE DIGITAL WORLD: STUDY OF THE PRIVACY IMPLICATIONS OF STREET-LEVEL IMAGING APPLICATIONS

Report of the Standing Committee on Access to Information, Privacy and Ethics

Hon. Shawn Murphy, P.C., MP
Chair

JANUARY 2011

40th PARLIAMENT, 3rd SESSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site
at the following address: http://www.parl.gc.ca

MAPPING PRIVACY PROTECTION IN THE DIGITAL WORLD: STUDY OF THE PRIVACY IMPLICATIONS OF STREET-LEVEL IMAGING APPLICATIONS

Report of the Standing Committee on Access to Information, Privacy and Ethics

Hon. Shawn Murphy, P.C., MP
Chair

JANUARY 2011

40th PARLIAMENT, 3rd SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Hon. Shawn Murphy

VICE-CHAIRS

Patricia Davidson

Bill Siksay

MEMBERS

Harold Albrecht
Hon. Carolyn Bennett
Kelly Block
Paul Calandra
Hon. Wayne Easter
Carole Freeman
Pierre Poilievre
Ève-Mary Thaï Thi Lac

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Bob Dechert
Luc Desnoyers
Jean Dorion
Earl Dreeshen
Judy Foote
Russ Hiebert
Greg Rickford
Michelle Simson
Paul Szabo
Boris Wrzesnewskyj

CLERK OF THE COMMITTEE

Chad Mariage

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Alysia Davies, Analyst
Élise Hurtubise-Loranger, Analyst
Dara Lithwick, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

ELEVENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*)(vi), the Committee has studied the subject of the privacy implications of street-level imaging applications and has agreed to report the following:

TABLE OF CONTENTS

MAPPING PRIVACY PROTECTION IN THE DIGITAL WORLD: THE STUDY OF THE PRIVACY IMPLICATIONS OF STREET-LEVEL IMAGING APPLICATIONS

BACKGROUND

A. The Committee Study

On April 27, 2009, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (hereafter the Committee) passed the following motion:

> That the Committee study the privacy implications of camera surveillance such as "Google's Street View" and "Canpages" and other issues related to video surveillance, and that the committee ask Eric Schmidt, the chairman and CEO of Google, or his Canadian representative, and Olivier Vincent, the chairman and CEO of Canpages, or his representative, to testify before the committee on this subject.

The Committee's study focused on street-level imaging applications, which use various means of photographing the streetscape. Typically, a camera is mounted on a vehicle that is driven up and down the streets of selected cities. The images can then be viewed on the Internet.

The Committee heard testimony from the Managing Director and Head of Google Canada, Jonathan Lister, and President and Chief Executive Officer of Canpages, Olivier Vincent, on June 17, 2009, as well as from the federal Assistant Privacy Commissioner, Elizabeth Denham, on October 22, 2009.

Following the discovery in May 2010 that Google Street View cars had been collecting payload data from unsecured wireless networks as part of its collection of Wi-Fi data, and the Office of the Privacy Commissioner's subsequent investigation into the possible privacy violations of the Wi-Fi data collection, the Committee heard testimony from the Office of the Privacy Commissioner on October 28, 2010 and from Jacob Glick, Canada Policy Counsel for Google, on November 4, 2010. The Committee heard further testimony from Mr. Glick, and Google's new Director of Privacy, Dr. Alma Whitten, via teleconference on November 25, 2010, as well as from François D. Ramsay, Senior Vice-President, General Counsel, Secretary and Responsible for Privacy, and Martin Aubut, Senior Manager, Social Commerce, at Yellow Pages Group (Canpages).

While the focus of the Committee's study has been on the privacy implications of street level imaging, the Google Wi-Fi issue has raised new concerns regarding the need for technology innovators, such as Google, to take measures to adequately incorporate the protection of individuals' privacy in the development of new products.

B. Protection of Personal Information in Canada

The collection, use and disclosure of personal information by commercial organizations in Canada is governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). However, where a province has introduced its own legislation on this subject that has been deemed "substantially similar" to PIPEDA, organizations covered by the provincial legislation are exempted from the application of the federal Act. Accordingly, in British Columbia, such activity would be governed by the *Personal Information Protection Act*; in Alberta, by the *Personal Information Protection Act*, and in Québec by the *Loi sur la protection des renseignements personnels dans le secteur privé*.[1]

In April 2009, the Privacy Commissioner of Canada, Jennifer Stoddart, sent a letter to the Committee enclosing a fact sheet from her office entitled "Captured on Camera: Street-level imaging technology, the Internet and you" (Appendix A).[2] The fact sheet notes the following privacy concerns raised by the Privacy Commissioner and her provincial counterparts regarding street-level imaging applications:

> Privacy Commissioners have had discussions with several companies to strengthen privacy protections for people whose images are captured. Our position is that all companies that offer such applications must take steps to better safeguard your privacy.
>
> In addition to companies being proactive and creative in their public communications to ensure that Canadians know when their cities—and, therefore, they themselves—may be photographed, we think these companies need to be more privacy sensitive in the areas they choose. They need to be mindful that people entering or leaving sensitive locations, such as shelters or abortion clinics, likely want to remain anonymous for privacy and safety reasons.
>
> They should also use proven and effective blurring technologies for faces and vehicle licence plates, so that people cannot be identified when their images are posted. Where individuals may be identifiable, companies must offer fast and responsive mechanisms to allow the images to be blocked or taken down.
>
> Companies offering these imaging applications must also have a good reason to keep the original, unblurred images in their databanks. If they do retain unblurred images, they must limit how long they keep them and protect them with appropriate security measures.[3]

---

1 In Ontario, there is a slightly anomalous situation—most personal information held by commercial organizations there is regulated under PIPEDA, but the specific category of personal health information is governed by the province's *Personal Health Information Protection Act* instead.

2 Also accessible online at: http://www.priv.gc.ca/fs-fi/02_05_d_39_prov_e.cfm.

3 Ibid.

C. Google Street View

1. The Service

Google Street View is a service created by the web engine company Google Inc. as part of Google Maps. It is intended to replicate the "street view" the user would experience if he or she was walking down the street in any given geographical location around the world. Users can click on a map in the service at: http://Maps.google.ca/streetview, and then take a virtual "walk" through their chosen neighbourhood, which has been reconstructed online using photographic images of the environs.

These photographic images are taken by photographers, who travel around cities and other mapped sites in marked cars with cameras mounted on top. While photographers visited some Canadian cities and began taking photographs in 2007, those images were stockpiled for future use.[4] The official rollout of Google's photographic mapping activities in Canada began in March 2009 in 11 Canadian cities,[5] and the service itself was launched in Canada in October 2009. Visits to the website by Canadians more than doubled following the launch.[6]

Google announced on March 22, 2010 that it would be spending a few months photographing streets in cities and towns in all provinces and territories across Canada. Once finished, Canada will join the United States, United Kingdom, and France in having nationwide Street View. The company also said that it was returning to Windsor, Ontario, to reshoot the city, after city officials complained about the existing photos, which were taken during the long municipal workers' strike last summer. The photos taken in the spring had shown unkempt streets and garbage piles in many locations.[7]

Google Street View is now available throughout most of populated Canada, as shown on a map on the Google website indicating where Street View is available: http://www.google.com/intl/en_us/help/maps/streetview/where-is-street-view.html. This website also shows a sample of the areas in which Google's cars are currently operating.

Throughout 2009, the Privacy Commissioner of Canada was in discussions with Google Inc. to ensure that they were aware of Canada's privacy laws, and she expressed concerns about the camera surveillance required to set up the service. Following consultation with the Privacy Commissioner, Google agreed to blur faces and license plates in its Canadian Street View images.

---

4 CBC News, "Google Alerts Canadians About Street View Filming," CBC News Online, March 26, 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, May 13, 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*, October 10, 2009.

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

The Google service already covers most of the United States, and has been introduced in more than 100 cities worldwide. The service has generated considerable controversy. For example, in May 2009, Greece's Data Protection Authority banned Google from taking Street View pictures in Athens until additional privacy safeguards, such as public notification of when the camera cars would be operating and additional storage security for the images had been implemented by the company.[8] In Japan, public complaints resulted in Google lowering its cameras by 40 centimetres to ensure that the images stay at eye level and do not peek over fences into private yards.[9]

In February 2010, European Union data privacy regulators issued a warning to Google that it must inform people before it sends cameras out into cities to take pictures for its Street View maps. The regulators also stated in a letter to Google that it should shorten the time it keeps its original photos from one year to six months. In a statement by way of response, Google said that its need to retain Street View images for one year is "legitimate and justified".[10]

In October 2010, Italy's privacy regulator announced restrictions on Google's Street View mapping service, echoing privacy concerns aired elsewhere in Europe. Google cars must now "be clearly identifiable by signs and stickers" indicating they will be taking pictures for Street View, the regulator said in a statement. Under the regulator's decision, Google must also publish on its website the names of the areas it intends to photograph three days ahead of time and publish the same information in at least two local newspapers and a radio station so residents can choose to avoid having their images collected. Google will be liable to fines of up to 180,000 euros for violating the new Italian rule, the regulator added.[11]

2. Privacy Protection

Google provides the following information regarding privacy protection to users on its website:

---

8 Derek Gatopoulos, "Google's Street View halted in Greece over privacy," *USA Today*, May 12, 2009, 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, May 13, 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, May 13, 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*, February 26, 2010, http://www.theglobeandmail.com/news/technology/google-warned-by-eu-over-street-view-map-photos/article1482311/.

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

Public access only

Street View contains imagery that is no different from what you might see driving or walking down the street. Imagery of this kind is available in a wide variety of formats for cities all around the world. In select cases, Google will partner with an organization such as Disneyland Paris to schedule imagery collection of their property.

Street View images are not real time

Our images show only what our vehicles were able to see on the day that they drove past the location. Afterward, it takes at least a few months to process the collected images before they appear online. This means that images you look at on Street View could be anywhere from a few months to a few years old.

Individuals and license plates are blurred

We have developed cutting-edge face and license plate blurring technology that is applied to all Street View images. This means that if one of our images contains an identifiable face (for example that of a passer-by on the sidewalk) or an identifiable license plate, our technology will automatically blur it out, meaning that the individual or the vehicle cannot be identified. If our detectors missed something, you can easily let us know.

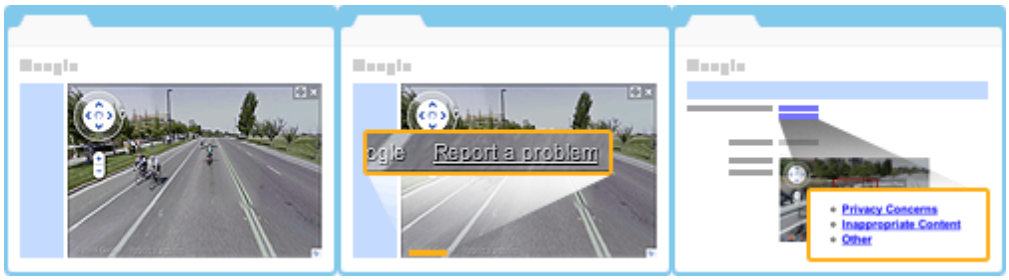
You can request removal of an image

We provide easily accessible tools allowing users to ask us to remove any images that feature inappropriate content (for example: nudity), or to remove any picture that features the user, their family, their car or their home. Below, you can review the steps to make a request.

How to Report a Concern

If you've found an image that you believe contains objectionable content, just follow these steps:

1. Locate the image in Street View.
2. Click "Report a problem" in the bottom-left of the image window.
3. Complete the form and click "Submit."



That's it. We'll review your report promptly.[12]

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

3. Google's Collection of Unsecured Wi-Fi Payload Data and the Office of the Privacy Commissioner's Preliminary Findings

Following a request from the German data protection authority in Hamburg to audit the Wi-Fi data collected by Google's Street View cars during a location-based project, Google discovered in May 2010 that it had been collecting payload data (the actual contents of transmissions made over a network) from unsecured wireless networks as part of its collection of information about Wi-Fi hot spots to support location-based services. A location-based service is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device.[13] By Google's own admission, it appears that this inadvertent collection was due to programming and code and software that it had developed with the purpose of collecting the Wi-Fi network data. As a result, Google halted the operation of its Street View cars, stopped the collection of Wi-Fi network data on May 7, 2010, and segregated and stored all of the data already collected.[14]

The Office of the Privacy Commissioner of Canada initiated three complaints against Google on May 31, 2010, pursuant to subsection 11(2) of PIPEDA,[15] after being made aware that Google Street View cars had been collecting payload data from unencrypted Wi-Fi networks during their collection of publicly broadcast Wi-Fi signals.

The three complaints are as follows:

a. Google's collection, use or disclosure of payload data was done without the individual's prior knowledge and consent;

b. Google's collection of payload data was done without prior identification of the purposes for which personal information (PI) was collected;

c. Google's collection of payload data was not limited to that which was necessary for the purposes identified.[16]

Following her investigation, on October 19, 2010 the Privacy Commissioner issued a *Preliminary Letter of Findings*[17] (Appendix B), which recommended that Google ensure it has a governance model in place to comply with Canadian privacy laws. The model

---

13 "Location-Based Services", GSM Association, January 2003, http://www.gsmworld.com/documents/se23.pdf.

14 Privacy Commissioner of Canada, *Preliminary Letter of Findings*, October 19, 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm.

15 Subsection 11(2) of PIPEDA states: "If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter."

16 Privacy Commissioner of Canada, *Preliminary Letter of Findings*, October 19, 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm.

17 Ibid.

should include controls to ensure that necessary procedures to protect individual privacy rights are duly followed before products are launched.

The Privacy Commissioner also recommended that Google enhance privacy training to foster compliance amongst all employees. As well, she called on Google to designate an individual or individuals responsible for privacy issues and for complying with the organization's privacy obligations—a requirement under Canadian privacy law.

She further recommended that Google delete the Canadian payload data it had collected, to the extent that the company does not have any outstanding obligations under Canadian and American laws preventing it from doing so, such as preserving evidence related to legal proceedings. If the Canadian payload data cannot immediately be deleted, the Privacy Commissioner recommended that it be secured and access to it be restricted.

The Privacy Commissioner will only consider the matter resolved upon receiving, either by or before February 1, 2011, confirmation of the implementation of the above recommendations, at which point she will issue her final report and conclusions.[18]

In an article dated October 22, 2010, *Associated Press* journalist Michael Liedtke reported that Google "is tightening its privacy leash on employees in an effort to ensure they don't intrude on people while the Internet search leader collects and stores information about its users."[19] According to Liedtke, "[b]esides promoting longtime employee Alma Whitten to be its director of privacy, Google said Friday that it will require all 23,000 of its employees to undergo privacy training. The company also is introducing more checks aimed at making sure workers are obeying the rules. Google's tougher privacy measures appear to be a response to recent breaches that have raised questions about the company's internal controls and policies." In his appearance before the Committee on November 4, 2010, Google Canada Policy Counsel Jacob Glick confirmed that these steps are being taken.

18 Ibid.

19 Michael Liedtke, "Google to impose tougher privacy measures after backlash to recent employee missteps, breaches," *Canadian Business Online*, October 22, 2010, http://www.canadianbusiness.com/markets/headline_news/article.jsp?content=b4915117&page=2.

D. Canpages' Street Scene

1. The Service

A competitive service to Google Street View was launched by a Canadian online business directory company called Canpages, in partnership with an American company called MapJack.[20] Similar to the Google Maps Street View feature, Canpages' Street Scene offers panoramic street-level images of city streets, allowing users to explore whole neighbourhoods with a few clicks of a mouse. However, unlike Google Street View, Canpages' Street Scene focuses on commercial offerings. Indeed, as noted in a press release:

> Street Scene provides 360-degree street-level views of the city for people conducting local business searches on Canpages.ca. The technology enables users to pinpoint their search results on a map as well as see high resolution images of the results in the context of the local environment. For example, users can take a virtual "drive" down a city street to find out whether a restaurant offers parking or to see what a particular storefront looks like. [21]

Street Scene was launched in March 2009 for viewing Vancouver, Squamish and Whistler online.[22] In August 2009 Canpages photographed the downtown cores and commercial arteries of Toronto[23] and Montreal,[24] and both cities are now online.

---

20 Kris Abel, "Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca," CTV.ca—Kris Abel's blog, March 16, 2009, http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx. Canpages is the largest independent local search and directories publisher in Canada. Its website, Canpages.ca features a national residential and business database and more than 3.5 million unique visitors come to visit it every month with their local search requests. With 80 publications and over 80,000 customers, Canpages reaches more than 8 million households and businesses across Canada. Headquartered in Vancouver, Canpages employs approximately 700 people and has offices in Alberta, British Columbia, Ontario and Quebec: http://corporate.canpages.ca/about_us/company_profile/where_local_search_gets_done.

21 Canpages Inc., "Canpages to Begin Street Scene Shooting in Toronto", August 11, 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—Kris Abel's blog, March 16, 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", August 11, 2009, http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf, and Kenyon Wallace, "Google Street View gets Canpages competition", *Toronto Star*, August 11, 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*, August 27, 2009, http://www.canada.com/montrealgazette/Canpages+Street+Scene+launches+Montreal/1936073/story.html.

2. Privacy Policy

Canpages' privacy policy[25] states the following regarding Street Scene:

> In providing Canpages Street Scene Service, Canpages has been sensitive to avoid including photographic information which would provide personal information about identifiable individuals. We are sensitive to the privacy concerns that might be raised by individuals who were photographed during the preparation of the data required by the Street Scene service. Photographs of identifiable individuals are in no way required by the service. The assembly of the data is designed to deliberately blur the faces of any individual who may be photographed in this process. You will notice as a result that no individual can be identified while using the Mapjack service. If you wish to report a privacy concern, please do so by clicking the "report a concern" on one the Street Scene Service Page.

The privacy policy also contains a statement specifying that "Our privacy policies follow the 10 principles of fair information practices as described by the Privacy Commissioner for Canada". The 10 principles are then listed:

> a. Accountability: An organization is responsible for personal information under its custody and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
>
> b. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
>
> c. Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
>
> d. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
>
> e. Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
>
> f. Accuracy: Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
>
> g. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
>
> h. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
>
> i. Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that

25 Accessible online at: http://www.canpages.ca/hm/privacy.jsp.

information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

j. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

3. Canada Eye

In March 2010, Canpages launched a free "augmented reality" iPhone application for local search called the Canada Eye. Canada Eye lets users search and view the direction and distance to all specific business locations in real-time overlaid on iPhone's screen. "Augmented reality" is the latest technology coined for applications that leverage the iPhone 3GS' compass, GPS and video camera simultaneously. As noted in a press release, "the Canpages application enables users to search for a specific business category-from local delis and mom and pop bakeries to Starbucks and Tim Hortons-and then shows the direction and distance to all of the businesses in the category in the local area. Essentially, Canada Eye is one application that allows users to locate businesses nearby as well as how to get to them in real time."[26]

In June 2010, Yellow Pages Group acquired Canpages for approximately C$225 million.[27]

WHAT THE COMMITTEE HEARD: INITIAL TESTIMONY ON GOOGLE AND CANPAGES' STREET-LEVEL IMAGING APPLICATIONS

A. Google Canada

Jonathan Lister, Managing Director and Head of Google Canada, appeared before the Committee on June 17, 2009. In his introductory remarks Mr. Lister emphasized how Google Street View "is a product that is changing the way people think about maps… The great innovation of Google Street View is the ability to marry street-level images with digital maps in order to provide a superior product for Internet users".[28]

With regard to the legal and privacy obligations incumbent upon Google as it operates in different countries, Mr. Lister stated the following:

---

26 "Canpages Brings 'Augmented Reality' Local Search to the iPhone 3GS", March 10, 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*, June 23, 2010, http://corporate.canpages.ca/media/Yellow%20Pages%20Group%20Finalizes%20Acquisition%20of%20Canpages.pdf.

28 Jonathan Lister, *Evidence*, Meeting No. 29, June 17, 2009, at 1550, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=E&Mode=1&Parl=40&Ses=2.

> First and foremost, Google is respectful of the laws of each country in which Street View operates. The imagery we make available shows no more than what any of you would see while travelling down a public street. The images in Street View are a snapshot in time, often several months to a year old. They aren't real time. While we only collect images from public places, we've always recognized that some passers-by may be inadvertently included in our pictures. As such, Google has invested significant resources into the development of a world-leading process for identifying and blurring certain features in an image, namely, identifiable faces and licence plates[...].
>
> Another key component to the privacy protections built into Street View is the easy-to-use, take-down request system. Every published Street View image includes a "report a problem" link, which takes users to a simple removals page. Any individual can ask to have an image entirely removed from the publication if it features themselves, their family, their car, or their home. This removal applies even if aspects of the image have already been blurred. We process removal requests every day in multiple languages and offer a fast and efficient turnaround time for each request.
>
> Another important aspect of our efforts to ensure privacy protection is our commitment to work with key stakeholders in every country in order to identify and contact relevant local organizations prior to launch. Our team will work to reach out to Canadian stakeholders and provide them with all the relevant details of Street View, including how to have their organization's image removed or blurred from the site.
>
> We're also putting in place a system that will ensure that on launch day for Street View in Canada, we will have additional staff on hand to handle take-down requests.
>
> Let me close by saying that as with many cutting-edge technologies, the challenge we face with Street View is striking the right balance between building a sophisticated and highly useful tool and ensuring that the data we collect to provide these services is used appropriately.[29]

Mr. Lister's June appearance before the Committee was prior to the Canadian launch of Street View in October 2009. At that time he informed the Committee that Google was working closely with the Privacy Commissioner's office in order to ensure that its privacy and legal obligations were met prior to Street View's launch.[30] In response to concerns about the capacity of Street View to invade the privacy of individuals within their homes or to see inside sensitive spaces such as women's shelters, Mr. Lister emphasized that Street View images are taken of the exterior of public places: "[T]he intended use [of Street View] is to improve mapping and capture the façades of publicly accessible, available buildings and landmarks. There is no need to see inside; it's not in the product definition to do that, and Google doesn't do it."[31]

With regard to the storage and disposal policies, Google images are held at secure "server farms," most of which appear to be in the United States.[32] With respect to the original unblurred images, Mr. Lister stated that Google retains non-blurred images for

29 Ibid.

30 Ibid. at 1605, 1650.

31 Ibid. at 1630.

32 Ibid. at 1625.

product enhancement, such as improving the blurring technology's recognition capacities. He added that Google had decided to revise its data retention policy to keep unblurred images for an "adequate but non-excessive period of time", after which non-blurred images would be permanently blurred and thus rendered anonymous (rather than disposed of).[33] As of June 2009, Google had not determined the exact timeframe for retention of the unblurred images.[34] He indicated that he would share this timeframe with the Committee once Google has a "reasonable and accurate answer".[35] Following Mr. Lister's appearance before the Committee, agreement was reached between Google and the Office of the Privacy Commissioner that Google would retain the unblurred images for the period of one year.[36]

B. Canpages

In his appearance before the Committee on June 17, 2009, Mr. Olivier Vincent, President and Chief Executive Officer of Canpages, explained the function of Canpages Street Scene, which focuses on commercial areas: "Fully integrated with Canpages' local search functionality, Street Scene provides panoramic street-level views of the city, so users can not only pinpoint their search results on a map, but also see high-resolution visuals of their search results in the context of the local environment. For example, users can take a virtual walk down the city streets to a local restaurant or hotel. They can see how it looks from the outside before they make a reservation, or they can assess where there is street parking or some other parking lot nearby."[37]

With regard to the privacy concerns raised by Street Scene's use of images and imaging technology, Mr. Vincent stated the following:

> Canpages considers respect of privacy as a key priority and is sensitive to the privacy concerns that might be raised by individuals who are photographed during the preparation of the data required by the Street Scene service. Canpages is committed to bringing every individual the assurance that it will respect their privacy, and has publicly stated its privacy policy regarding its Street Scene service.
>
> We will notify the public before we start shooting. Individual faces and other recognizable features like licence plates are blurred on the captured image prior to being posted online. The blurring process uses a proprietary technology that is irreversible by the users. All original non-blurred files are destroyed after blurring and before being posted online. There is no way to get back these original files later on.

---

33 Ibid. at 1610.

34 Ibid. at 1650.

35 Ibid. at 1715.

36 Elizabeth Denham, *Evidence*, Meeting No. 32, October 22, 2009, at 0930, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=E

37 Olivier Vincent, *Evidence*, Meeting No. 29, June 17, 2009, at 1555, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=E&Mode=1&Parl=40&Ses=2.

> Users can report any concern at any time using the "report a concern" feedback located on every image. Upon a specific request, Canpages will provide extra blurring for an entire person, a vehicle, a window, a building, a pet—you name it. While privacy laws are not necessarily reflective of the rapidly growing field of technology, we at Canpages want to take a proactive approach to all concerns that may be raised.
>
> [...]
>
> Canpages has engaged with the public, the privacy commissioners of Canada, and Mr. Pierre Poilievre, the MP who filed a motion before this committee to review privacy matters.
>
> In conclusion, Canpages is committed to working both immediately and as part of an ongoing process to address potential privacy issues that might arise as a result of its continuous innovation in the field of local search.[38]

Following his introductory remarks, Mr. Vincent discussed, among other topics, the company's blurring technology for protecting the anonymity of passers-by and sensitive places. He testified that while earlier versions of blurring technology were more easily reversed, the new version his company is using is much stronger and cannot be reversed. He also testified that the original versions of any images which require blurring are destroyed and replaced by the blurred version once the technology has been applied.[39]

C. Office of the Privacy Commissioner of Canada

Elizabeth Denham, Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada, appeared before the Committee on October 22, 2009. Ms. Denham informed the Committee that PIPEDA is a technology-neutral law that is a "dynamic, modern, and effective tool for strengthening the privacy rights of Canadians" that was designed to respond to such situations as the "commercial collection and use of personal information through street-level imaging technology".[40] While aware that the many services that use street-level imaging are very popular with the public, the Office of the Privacy Commissioner remains concerned about ensuring that the commercial use of the technology "protects the privacy of Canadians by meeting the requirements of PIPEDA, such as knowledge, consent, safeguards, and limited retention."[41]

The view of the Office of the Privacy Commissioner is that citizens should know in advance that street-level images are being taken, when, and why, and how they can have their image removed if they don't want it to appear online. Faces and license plates need to be blurred so that the individual is made anonymous or is at least not identifiable. Companies need an effective and quick take-down process whereby an individual can

---

38 Ibid.

39 Ibid., at 1620, 1625 and 1720.

40 Elizabeth Denham, *Evidence*, Meeting No. 32, October 22, 2009, at 0900, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=E.

41 Ibid.

have their image removed. Unblurred images retained for legitimate business purposes should be protected with appropriate security measures and the raw data should not be retained indefinitely.[42]

Ms. Denham observed that improvements have been made in these areas by the service providers who appeared before the Committee. In August 2009, Google agreed with the Office of the Privacy Commissioner and with other data protection commissioners in Europe that they needed to delete unblurred imagery after one year. As per her testimony:

> One of the most contentious issues that we had in our discussions with Google and Canpages is what happens to the raw imagery, the unblurred imagery that's stored in databases in the U.S. At first Google was very reluctant to set a retention period for how long they were going to keep that data. In August they agreed with us and they agreed with other data protection commissioners in Europe that indeed they needed to delete the unblurred imagery after one year. They gave us the business rationale as to why they needed to keep it for a year. We accepted that. We also have an undertaking from Google that we can visit their facilities and review how they are permanently deleting or permanently anonymizing the data after a year. That was one of our major concerns with the service.[43]

Ms. Denham also told the Committee that since the launch of Google Street View at the beginning of October 2009, the Office of the Privacy Commissioner had received fewer than a dozen inquiries from Canadians, and only one complaint, which was resolved. This complaint concerned an individual who felt that his image had been captured. The complaint was resolved during the investigation by Google agreeing to permanently delete the man's image from the database, so the Privacy Commissioner never issued a public recommendation. The Office of the Privacy Commissioner had not received any complaints regarding the effectiveness of Google's take-down procedure by the time of Ms. Denham's appearance before the Committee. The Office of the Privacy Commissioner had received calls from individuals asking how to remove their images from Street View. These individuals were referred to Google, and none of them has subsequently returned to the Office of the Privacy Commissioner with a full-scale complaint so far.[44]

In response to a question as to whether the Office of the Privacy Commissioner is satisfied that Google's blurring policy meets the standards found in Canadian commercial privacy laws, Ms. Denham replied that she believes that Google could do a better job with their blurring technology: "We were told by Google that their blurring technology was 98% effective; that was before the images went live. But we've seen for ourselves that there are many instances in which individual faces are not blurred. Google is committed to continuing to improve the blurring, which is one of the reasons they want to retain the

42 Ibid. at 0905.

43 Ibid. at 0930.

44 Ibid. at 0930, 1025.

images for one year. They're working on improving their blurring technology." The Privacy Commissioner is satisfied with the one year timeframe.[45]

WHAT THE COMMITTEE HEARD: FOLLOW-UP TESTIMONY ON GOOGLE'S COLLECTION OF WI-FI DATA

A. Office of the Privacy Commissioner of Canada

Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada, appeared before the Committee on October 28, 2010, to speak about the Office's investigation into Google's collection of Wi-Fi data that culminated in the Office's *Preliminary Letter of Findings* released on October 19, 2010.[46] She also provided updates regarding the privacy implications of street level imaging technology. She was accompanied by Daniel Caron, Legal Counsel (Legal Services, Policy and Parliamentary Affairs Branch), and Andrew Patrick, Information Technology Research Analyst.

In her opening statement, Ms. Kosseim summarized the office's investigation into Google's inadvertent[47] collection of unsecured Wi-Fi payload data with its Street View cars. As she explained, payload data is information about the communications that run through Wi-Fi networks.[48] The Privacy Commissioner's investigation found that:

> [...]Google had inappropriately collected personal information of Canadians from unsecured wireless networks. In some cases, that personal information was highly sensitive, including complete e-mails, user names and passwords, and even medical conditions of specified individuals. Unfortunately, this collection of data was due to an error that could have been easily avoided if Google's own procedures had been followed.
>
> Essentially what happened here was the engineer who developed the code to sample categories of publicly broadcast Wi-Fi data also included code allowing for the collection of payload data, thinking that this type of information might be useful to Google in the future. The engineer had identified what he believed to be "superficial" privacy concerns, but contrary to company procedure, failed to bring these concerns forward to product counsel, whose responsibility at Google would have been to address and resolve these concerns prior to product development.[49]

As noted earlier in the report[50], the Privacy Commissioner recommended that Google re-examine and improve the privacy training it provides to all its employees and

---

45 Ibid. at 1025.

46 Privacy Commissioner of Canada, *Preliminary Letter of Findings*, October 19, 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm.

47 As described by Patricia Kosseim.

48 Patricia Kosseim, *Evidence*, Meeting No. 28, October 28, 2010, at 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=E&Mode=1&Parl=40&Ses=3.

49 Ibid.

50 See "Google's Collection of Unsecured Wi-Fi Payload Data and the Office of the Privacy Commissioner's Preliminary Findings".

ensure that it has an overarching governance model in place that guarantees that procedures to protect privacy are followed prior to the launch of any product. Furthermore, the Privacy Commissioner called on Google to delete the Canadian payload data it collected to the extent that it is able to do so under Canadian and U.S. laws.[51]

Ms. Kosseim explained that the Privacy Commissioner issued a *Preliminary Letter of Findings* with regard to Google's collection of Wi-Fi data as she is seeking proof and evidence that the recommendations will actually be followed before she formally concludes, or "resolves", her investigation. In other words, the Privacy Commissioner is seeking "actual implementation and not just undertakings".[52]

Ms. Kosseim then detailed how the Office of the Privacy Commissioner initially became aware that Google was collecting Wi-Fi signal and payload data. She testified that the office had received notice from Google in April 2010 "that they had intended and they were collecting publicly broadcast Wi-Fi radio signals." [53] Google had explained that this was in order for the company to be able to enhance its offering of "location-based services". [54]

Ms. Kosseim further explained that while the collection of the Wi-Fi signals was not related to the Google Street View product itself, as a matter of practicality, Google used the Street View cars in order to collect the Wi-Fi data. Indeed, Google told the Office of the Privacy Commissioner in April 2010 that they were putting antennae on the roofs of the Street View cars to at the same time collect and capture the neighbouring Wi-Fi radio signals.[55]

Only in May 2010, after being prompted by requests for further information from German data protection authorities, did Google realize that it was unknowingly collecting Wi-Fi payload data.[56] As detailed in the *Preliminary Letter of Findings*, on May 7, 2010, Google grounded its Street View cars, stopped the collection of Wi-Fi network data, and segregated and stored all of the data already collected.

---

51 Patricia Kosseim, *Evidence*, Meeting No. 28, October 28, 2010, at 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=E&Mode=1&Parl=40&Ses=3.

52 Ibid. at 1540.

53 Ibid. at 1555.

54 Ibid. As described earlier in the report, a "location based service" is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device.

55 Ibid.

56 Ibid.

The Office of the Privacy Commissioner had no reason to believe, from the basis of the investigation, that there was anything untoward done with the Wi-Fi payload data that had been inadvertently collected by Google.[57]

Nonetheless, the Office of the Privacy Commissioner recognized that the mere collection of information about Wi-Fi access or location points can itself raise potential privacy concerns. As noted by Mr. Andrew Patrick: "[I]f information about the presence of a Wi-Fi access point can be at all linked to a particular individual, either individually or in combination with other bits of information, then it would be potentially personal information and therefore potentially something that we would be worried about."[58] The office does not have specific information about the actual location-based services that Google is developing with the collection of Wi-Fi radio signals.[59]

Overall, Patricia Kosseim expressed confidence that Google will implement the Privacy Commissioner's recommendations contained in the preliminary letter of findings:

> I think we have every indication to be confident. Again, there has been, not formal responses to us from Google, but responses in the press that we have heard, as all of you have, to indicate concrete steps that they have already taken and steps that we have learned of in the course of our investigation had already been undertaken to begin the process of putting in place appropriate governance structures within the organization which is a global giant as you can understand. The date of February 1 was deliberately chosen bearing in mind a reasonable amount of time that it will take not only to undertake to make these changes but to have concrete evidence that they've been made at a global scale. That's why the date was given. We have every hope that we will get a positive response earlier than that and we'd be delighted to do so. We are fairly confident that there will be a good ending to this.[60]

As well, Ms. Kosseim noted that at this time the Office of the Privacy Commissioner is satisfied with the privacy protections found in the Google Street View and Canpages Street Scene technologies, which are separate from the incident regarding the collection of Wi-Fi payload data:

> In respect of the Street View imaging technology by Google and Canpages, one point I just want to clarify is that those were never the subject of an investigation by the commissioner...on the basis of the correspondence and the response of the organizations, there has been a lot of movement on the part of both organizations to comply with or to move along in harmony with the recommendations that the commissioner has made including notification to neighbourhoods before they arrive, discussions with vulnerable stakeholders and groups, take down procedures, retention and deletion mechanisms and other such protections. So it's on the basis of that correspondence there's been a lot of movement. Of course there could always be improved notification, there could always be ongoing improvements to blurring

57 Ibid. at 1605.

58 Ibid.

59 Ibid. at 1610.

60 Ibid.

technology but so far there's been great improvement and movement towards the commissioner's wishes.[61]

In conclusion, Ms. Kosseim emphasized one over-arching recommendation to companies such as Google, Canpages and Facebook that use new technologies to compile, process and share information in various ways, namely that such organizations must adopt the precautionary principle with regard to the possible privacy implications of new technologies. It is the hope of the Office of the Privacy Commissioner that organizations, when conceiving, developing, and deploying information technologies of which Canadians all benefit "take the proactive measures up front to identify the risks, asses them, and manage them before deployment of these technologies on a widespread basis."[62]

B. Google Canada

1. Appearance of Jacob Glick on November 4, 2010

In his appearance before the Committee on November 4, 2010, Mr. Jacob Glick, Canada Policy Counsel for Google Inc., spoke both about Google Street View and about Google's collection of Wi-Fi payload data.[63]

With regard to Street View, Mr. Glick noted that Google has "addressed all of the concerns identified by this committee and by the Privacy Commissioner. We've implemented the most sophisticated blurring technology to blur faces and licence plates in all of our images. We've implemented a quick and easy take-down procedure. Anybody can request that Google remove pictures of themselves, their house, their kids, or their car, from Google Street View. Finally, we are permanently baking in this blurring after one year."[64] Mr. Glick noted that Canadians are avid users of Street View. Indeed, "in absolute numbers, Canadians are the third most active users of Street View in the world, behind only the U.S. and the U.K. Since its launch, Canadians from coast to coast to coast have used this next generation cartography to map their way to the store, promote their local business, sell their house, and explore our country online."[65]

With regard to Google's collection of Wi-Fi payload data, Mr. Glick clarified that it was not related to the Street View product, but that Street View vehicles were used as a platform for the collection. He apologized on behalf of Google for what had happened, noting that "what happened is not consistent with our commitment to serving Internet

---

61 Ibid. at 1705.

62 Ibid. at 1705.

63 Jacob Glick, *Evidence*, Meeting No. 30, November 4, 2010 at 1530, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4764635&Language=E&Mode=1&Parl=40&Ses=3.

64 Ibid.

65 Ibid.

users".[66] He emphasized that "no payload data transferred over encrypted networks was collected by Google. Google had no desire to use payload data in any way. No payload data has been used in any Google product or service, and none of the Canadian payload data has been given or disclosed to third parties; it has been segregated and secured."[67]

In terms of how Google Street View cars came to collect Wi-Fi payload data, Mr. Glick testified that at the time that Google was preparing to launch Street View and was deploying a fleet of vehicles around the world to collect street level imaging in 2007, a Google engineer had the idea of using Street View vehicles as a platform to detect Wi-Fi hot spots to support location-based services:

> Using publicly broadcast Wi-Fi hot spots as landmarks to help users identify where they are is common industry practice. The engineer designed software code to collect Wi-Fi network data, and unfortunately, also Wi-Fi payload data. Payload data refers to the contents of transmissions. Google did not want this payload data and does not believe that collecting such payload data is useful or appropriate. The engineer should have flagged, for Google's in-house lawyers, the plan to collect Wi-Fi payload data. He did not do so. If he had, this would have been an opportunity at the outset of the program for Google to identify the problem and stop it. As a result, the code was deployed on Street View vehicles. The software worked as it was programmed to do, collecting Wi-Fi network data and Wi-Fi payload data sent over un-encrypted networks.[68]

In April 2010, Google was asked by German authorities to audit the Wi-Fi data collected by Street View vehicles. This audit revealed that Google had been collecting Wi-Fi payload data in addition to the network data. According to Mr. Glick, "[b]efore announcing publicly what we discovered, I personally called Commissioner Stoddart and advised her of this issue. After that, Google made a public announcement and apologized for what had happened."[69] Street View vehicles were grounded, and data was segregated. According to Mr. Glick, "nobody has reviewed the Canadian payload data, other than the Privacy Commissioner's investigators and those who facilitated their investigation. It has not been disclosed to any third parties."[70] It was not clear from Mr. Glick's testimony whether the Wi-Fi data collection only began in April, or whether it began beforehand.

Mr. Glick confirmed that on October 22, 2010 Google made a number of significant changes to its privacy policies and controls. Mr. Glick indicated that he had spoken with Commissioner Stoddart prior to the public announcement of the following measures:

> [F]irst, Google appointed Dr. Alma Whitten as our director of privacy to ensure we build effective privacy controls into our products and internal practices. Dr. Whitten is an internationally recognized expert in the computer science field of privacy and security. Second, we are enhancing our core privacy training with a particular focus on the responsible collection, handling, and use of data. Finally, Google is adding new

66 Ibid.

67 Ibid.

68 Ibid.

69 Ibid.

70 Ibid.

> safeguards to our existing privacy-compliant system to include independent internal audits to ensure that user privacy is protected.[71]

Google is of the view that these changes will significantly improve its processes and controls to prevent something like the Wi-Fi incident from happening again.

Mr. Glick was asked numerous times about how the position of Director of Privacy will work at Google and about Dr. Alma Whitten's qualifications for the position.[72] While Mr. Glick was not able to provide a biography of Dr. Whitten at the time, he noted that she has been at Google for a number of years, that her doctorate is in the area of computer science and security, and that she has published numerous papers on computer science, security and privacy. She has been a leader in the area of privacy and security on a global basis for a number of years. She is based in the London, England office of Google.[73]

Based on Mr. Glick's testimony, it would appear that Google had not yet disposed of the Canadian payload data that it had collected, as it was unclear whether it had to be preserved for some reason.[74] Mr. Glick undertook to verify whether and when the Canadian payload data would be deleted,[75] and whether there might be any impediment under U.S. law with regard to the deletion of that information.[76]

2. Appearance of Jacob Glick and Alma Whitten on November 25, 2010 (via teleconference)

Following Mr. Glick's appearance on November 4, 2010, the Committee decided to hear from Google's new Director of Privacy, Dr. Alma Whitten, as well as Mr.Glick, on November 25, 2010, seeking further information on the initiatives being undertaken by Google following the Wi-Fi data incident, and in response to the Privacy Commissioner's *Preliminary Letter of Findings* released on November 19, 2010. Both witnesses appeared via teleconference, Dr. Whitten testifying from London, England, and Mr. Glick testifying from Toronto.

Prior to her appearance, Google sent the Committee the following biography of Dr. Whitten:

> Alma Whitten joined Google in 2003 and currently serves as the company's Director of Privacy for both the engineering and product teams. In this role, she will ensure Google builds effective privacy controls into user products and internal practices. An internationally-recognized expert in privacy and security, Alma has testified before the

71 Ibid.

72 See for example at 1550 and 1555.

73 Ibid. at 1550.

74 Ibid. at 1600.

75 Ibid.

76 Ibid. at 1635.

> U.S. Congress and has appeared before the European Commission's Article 29 Working Party.
>
> Previously, Alma served first as Lead for Google's Applied Security engineering team, and then as Google's Privacy Engineering Lead where she grew teams that developed tools like the Google Dashboard.
>
> Prior to joining Google, Alma was best known for her 1999 technical paper on usability as a primary issue for computer security, titled "Why Johnny Can't Encrypt," which is recognized as a founding paper for usability of security as a field of research. She continues to research, write, and speak on human-centered approaches to security and privacy as part of her work at Google. Alma holds a Ph.D. in Computer Science from Carnegie Mellon University.[77]

In her testimony to the Committee, Dr. Whitten noted that: "I've devoted my career both as an academic and now as Google's Director of Privacy to one primary goal: to make it intuitive, simple, and useful for Internet users to take control of their privacy and security,"[78] and she spoke about Google's plans to strengthen its internal privacy and security practices:

> With my expanded responsibilities, I will have the chance to oversee and work with both the engineering and the product teams to help ensure that privacy and security considerations are built into all of our products. While the duties that go with this role are big, I am confident that I will be supported with the resources and internal support needed to help Google do better... We want to make certain that each product we roll out meets the high privacy and security standards that our users expect of us.[79]

She explained that Google will be providing privacy training to its employees tailored to their various responsibilities[80], including broad security and privacy compliance training, code of conduct compliance training, and a more focused and deeper training specific to different kinds of job roles:

> A very important point we will be making over and over again in our training is that individual engineers should never be making these judgment calls by themselves. We want to educate them on the privacy landscape and privacy concerns.
>
> We want to very much educate them on Google's own articulated privacy principles of transparency, control, and responsible stewardship above all, but we also want to educate them very, very strongly and reinforce that education in many ways on the improved processes we are putting in place, to make sure that those fail-safes are there, that the thoughtful review is in place, and that individual engineers don't try to "lawyer" questions by themselves.

---

77 E-mail letter to the Clerk of the Committee, November 22, 2010. Further information on Dr. Alma Whitten can be accessed at: http://www.google.com/research/pubs/author32149.html.

78 Dr. Alma Whitten, *Evidence*, Meeting No. 34, November 25, 2010, at 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Language=E&Mode=1&Parl=40&Ses=3.

79 Ibid. at 1540.

80 Ibid. at 1600.

[...]

> For newly hired engineers, we expect to give them a significant session of privacy training within their first two weeks at the company, before they would be writing any code, before they would be starting on any product development. With that initial training, we expect to lay a lot of the seeds in place in putting the framework in place for them to know who they are supposed to talk to and when, to know where the resources are internally to help them understand privacy and to understand our privacy processes, and where those are quickly and easily found--all of those aspects of who they should talk to.
>
> For engineers going forward, for the people who aren't going to be hired next week or the week after that to come in through this initial training, we will be doing follow-up training. But above all, I think, the process, which we are enhancing and optimizing now, and the training have to really be two halves of the same coin that will reinforce each other and work closely together.
>
> The process will force engineers to engage with the training at various parts of their project's life cycle. As they are expected to engage with the process, then the training is there to tell them how to do so and to provide them help to enable them to do so. The goal is very, very much for those two aspects to strongly reinforce each other to make this as effective as possible.[81]

Dr. Whitten also explained how Google ensures that it has expertise in the privacy considerations of the various countries where it operates:

> We do have local expertise on the ground in as many countries as possible--in fact, in most countries. I spoke to the earlier question from the member about the need to bring in all of these different kinds of expertise across legal and engineering functions.
>
> We're also very conscious of that cross-culturally, and of the need for our privacy review to bring in perspectives from all of the different parts of the world where our products are going to be seen, used, and experienced. That's part of the reason why I am now based in Europe: to make sure that even in my own person I can bring in a little bit of extra balancing, having started out in the United States and then bringing that over there.
>
> Canada is certainly one of the countries where we pay very, very close attention to the work of your Privacy Commissioner and to her voice on the international stage. We rely very heavily on Jacob's relationship and close communications with her office. We do similar things in all of the countries where we're present.[82]

In his testimony before the Committee on November 25, 2010, Mr. Glick confirmed that Google had not yet deleted the Canadian Wi-Fi data that it had collected, pending analysis of any issues that may prevent the immediate deletion of the data:

> What we're doing is precisely what the Privacy Commissioner asked, which is undertaking an analysis of Canadian and U.S. law, both in terms of the laws of evidence and other applicable laws, to determine the extent to which it can be deleted. In the

81 Ibid. at 1625.

82 Ibid. at 1645.

> interim we're doing precisely what she asked, which is maintaining the safeguards around the data and the protections for it.[83]

Mr. Glick added that "ultimately our objective here is to, as I've said before, delete all of the data. We didn't want it in the first place, we don't want it now, but we don't want to prematurely delete it and cause more headaches."[84] He undertook to provide the Committee with a list of countries where Google has been subject to criminal charges or administrative penalties with respect to the collection of Wi-Fi payload data.[85]

In a letter to the Committee dated December 9, 2010, Mr. Glick provided the following responses to the Committee's questions:

> **1. In what countries was payload data from unencrypted Wi-Fi networks mistakenly collected by Google:**
>
> United States of America, Canada, much of Europe (Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Great Britain/UK, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden and Switzerland), Australia, Hong Kong, Japan, South Korea, Macau, New Zealand, Singapore, Taiwan, Brazil, Mexico and South Africa.
>
> **2. Where has the payload data been stored:**
>
> Payload data collected anywhere in the world prior to May 2010, when this problem was discovered and the payload collection ceased, was and is stored in the United States.
>
> Hard drives from street view vehicles that were not processed by the time we learned of the problem have been secured on a regional basis. Hard drives from North America, South America and Asia are in the United States. Hard drives from Europe and Africa are in Europe.
>
> **3. What payload data has been deleted:**
>
> Payload data identified as being from the following countries has been securely deleted as of the date of this letter: Ireland, Austria, Denmark, Hong Kong and the United Kingdom.
>
> **4. Has Google faced criminal charges or administrative penalties or sanctions related to this matter anywhere around the world?**
>
> No.[86]

---

83 Jacob Glick, *Evidence*, Meeting No. 34, November 25, 2010, at 1605, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Language=E&Mode=1&Parl=40&Ses=3.

84 Ibid. at 1620.

85 Ibid. at 1715.

86 E-mail letter from Jacob Glick to the Committee, December 9, 2010.

C. Yellow Pages Group (Canpages)

On November 25, 2010 the Committee also heard testimony from François D. Ramsay, Senior Vice-President, General Counsel, Secretary and Responsible for Privacy, and Martin Aubut, Senior Manager, Social Commerce, in order to learn about any updates regarding the Yellow Pages / Canpages Street Scene product, and to determine how the company incorporates privacy considerations into the development of its products.

In his opening statement, Mr. Ramsay provided a brief introduction of Yellow Pages Group, which acquired Canpages in June 2010. He clarified that the Street Scene product licenses its map data from two companies, MapJack and Google. Following Google's discovery regarding the collection of Wi-Fi payload data, Yellow Pages Group obtained confirmation from MapJack that it had never collected either Wi-Fi network or payload data:

> Depending on where you are within our universe of websites, [Yellow Media Inc., the network of companies that include Yellow Pages Group, Trader Corporation, and Canpages is] currently using Street View technology from Google and Microsoft, in addition to MapJack, the provider that Canpages has historically used.
>
> I am pleased to confirm to the committee that Canpages' supplier of the Street Scene service, MapJack, has not been used to collect either Wi-Fi network data or Wi-Fi payload data. Therefore, we have never been in possession of any such data.
>
> Yellow Media Inc., YPG, Trader, and Canpages are fully committed to abiding by the privacy legislation applicable to our business.[87]

Mr. Ramsay and Mr. Aubut indicated that they could provide the Committee with confirmation of the types of technology used by their contractors for Canpages products.[88]

With regard to privacy training provided for employees of Yellow Pages Group, Mr. Ramsay noted that until now no such training had existed. However, given his appearance before the Committee, and upon hearing the testimony of Google's Dr. Alma Whitten, he is going to look into how Yellow Pages Group can provide privacy training for its employees.[89]

As well, Mr. Ramsay noted that Yellow Pages Group has not historically had direct contact with the Privacy Commissioner of Canada to consult on potential privacy issues regarding products. This is something that he is interested in changing, as he testified, "I've determined with some of my colleagues that this is something that we'd be interested in exploring and being proactive about. We understand that as the world becomes more

---

87 François Ramsay, *Evidence*, Meeting No. 34, November 25, 2010, at 1530, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Language=E&Mode=1&Parl=40&Ses=3.

88 Ibid. at 1710.

89 Ibid. at 1630.

digital, obviously, many of these issues will come to the forefront. It's important for us to be on top of these matters and to be responsive and proactive on legitimate privacy concerns that Canadian institutions have."[90]

With regard to Canada Eye, a geolocation based service launched by Canpages in March 2010, Mr. Ramsay explained the following:

> I don't know if some of the members here have iPhones, but there is a button on the Canpages application that you can use. I'm more familiar with another one from a competitor of Canpages, YPG. Basically, you use the camera feature of your iPhone, pointing in a direction, and listings are pushed using the GPS features of the iPhone or the smartphone that you're using. [...] The image is a bit of a gimmick, I guess, in the sense that it's not really the eye that is seeing. It's just that the iPhone understands in which direction it is pointing and therefore understands which businesses are located in the direction in which you are pointing.
>
> So just to confirm, it's not strictly speaking the fact that the camera sees a business that it identifies it. It's just that it's geo-coded. The businesses are geo-coded, and the phones pointing in that direction push the listing that is being provided.[91]

To the best of Mr. Ramsay's knowledge, smartphone services such as Canada Eye are consistent with Canadian privacy legislation and policies. He noted that "the service we're using to provide directions for people is, again, with services that are provided by the likes of Google and Microsoft."[92] In other words, it does not seem that the geolocation technology was developed in-house by Yellow Pages Group.

CONCLUSION

The Committee, after hearing evidence from Google Canada, Canpages, and from the Office of the Privacy Commissioner of Canada, is satisfied that the privacy concerns of Canadians with regard to street level imaging technology are being taken seriously by all parties involved. Best practices have been developed by Google and Canpages, in consultation with the Office of the Privacy Commissioner, with regard to the notification of residents as to when street level images are being taken, the requirement to blur faces and distinguishing information such as licence plate numbers, the length of time that images can be retained, and the procedures to remove images in the case of complaints. In particular, the Committee is assured that the Office of the Privacy Commissioner is, and will continue to monitor developments regarding privacy and street-level imaging to ensure compliance with current Canadian law. For its part, the Committee will also continue to monitor developments in this area and revisit the matter if and when necessary.

However, the emergence of Google's collection of unsecured Wi-Fi payload data raises a broader question about the extent to which privacy concerns are addressed at the development stage of new technologies. As noted by Privacy Commissioner Stoddart, "the

90 Ibid. at 1645.

91 Ibid. at 1705.

92 Ibid.

question is, why aren't they starting with privacy principles at the beginning? And why are Canadian taxpayers or Spanish taxpayers and so on spending a lot of time and effort when these companies should get it right from the beginning before they launch their products?"[93]

The Committee is mindful that technology innovators need to ensure that privacy protection is a core consideration at the development stage of any new project. Potential privacy risks should be identified and eliminated or reduced at the onset of new projects and not be left to be addressed as costly afterthoughts. With respect to the specific incident pertaining to Google, the Committee is cautiously optimistic that the company is moving in the right direction by appointing Dr. Alma Whitten as company Director of Privacy, mandating privacy training for its employees, and incorporating more privacy controls, such as audits of projects under development, into the workplace. The Committee looks forward to receiving confirmation that Google has implemented the recommendations made by the Privacy Commissioner in her *Preliminary Letter of Findings* regarding Google's collection of Wi-Fi data by the deadline of February 1, 2011 set by the Privacy Commissioner.

As well, the Committee notes that this study has raised awareness of the importance of privacy protection at Yellow Pages Group, which is now considering how to implement privacy training for employees and consultation with the Privacy Commissioner on product development at Yellow Pages Group.

The Committee commends the Privacy Commissioner of Canada for her work on this file and her work with privacy commissioners internationally on the importance of implementing "privacy by design"[94] into the development of new products in the digital realm.

---

93 Jennifer Stoddart, *Evidence*, Meeting No. 25, October 19, 2010 at 1615, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4702609&Language=E&Mode=1&Parl=40&Ses=3.

94 "Privacy by design" is a concept developed by Ann Cavoukian, PhD, Information and Privacy Commissioner of Ontario, to describe the philosophy of embedding privacy proactively into technology itself—making it the default: http://www.privacybydesign.ca/about/. At the 32nd International Conference of Data Protection and Privacy Commissioners held in Jerusalem, Israel, from October 27-29, 2010, commissioners approved the Privacy by Design Resolution proposed by Dr. Cavoukian and co-sponsored by the Privacy Commissioner of Canada, as well as a number of international privacy commissioners: http://www.ipc.on.ca/english/Resources/News-Releases/News-Releases-Summary/?id=992.

LIST OF RECOMMENDATIONS

RECOMMENDATIONS

1. **Given the tremendous changes happening in social media and throughout the Internet, the Committee recommends that the Privacy Commissioner continue to be vigilant in protecting and keeping abreast of the privacy concerns of all Canadians.**
2. **The Committee supports the recommendations made by the Privacy Commissioner in her *Preliminary Letter of Findings* regarding Google's collection of Wi-Fi data and calls on Google to implement the Privacy Commissioner's recommendations as soon as possible, and by the deadline of February 1, 2011 as set by the Privacy Commissioner. The Committee recommends that the Privacy Commissioner communicate with the Committee upon receiving confirmation of Google's compliance with her recommendations.**
3. **The Committee further recommends that the Privacy Commissioner alert the Committee to any concerns that might arise with respect to Google's compliance with her recommendations.**
4. **The Committee recommends that the Privacy Commissioner clarify with technology providers, such as those seen by the Committee, the importance of having in place explicit privacy training regimes for their employees.**
5. **The Committee recommends that the Privacy Commissioner continue her outreach activities, such as through the fact sheet prepared for the public titled "*Captured on Camera*—Street-level imaging technology, the Internet and you", to educate the public about their privacy rights and the risks and implications of new technology and social media.**
6. **Finally, the Committee reiterates the recommendation made by the Privacy Commissioner herself, that technological innovators such as Google should implement "privacy by design" into the development of new products, and consult with the Privacy Commissioner, as well as her international counterparts as appropriate, to ensure that the privacy rights of the public continue to be protected in the digital world.**

APPENDIX A

CAPTURED ON CAMERA
STREET-LEVEL IMAGING TECHNOLOGY, THE INTERNET AND YOU

A number of companies have begun collecting images of public places in Canada, which may then be made available over the Internet or through other means. Individuals may be captured in these images, perhaps incidentally. One of the most widely known is Google's Street View application, which allows computer users to make "virtual visits" to cities such as Paris, London, New York and, eventually, major Canadian centres. Canpages is another company that provides street images on the Internet. Other applications have also been developed for fields such as geomatics, surveying, mapping and urban planning.

In Canada, there is private-sector privacy legislation that applies to these street-level imaging applications if they are collecting images of identifiable people. And, while the Privacy Commissioners of Canada, British Columbia, Alberta and Quebec recognize the popularity of these applications, they have also expressed reservations because the technology captures images not just of places, but of people as well.

The Commissioners believe Canadians should be aware of the privacy issues that can arise.

PEOPLE IN PUBLIC PLACES

A common misconception is that a company doesn't need your permission to take your photograph in a public place.

In fact, one of your key protections under Canadian privacy law is that you should know when your picture is being taken for commercial reasons, and what your image will be used for. Your consent is also needed[1]. There are exceptions to this rule but they are very limited and specific[2].

However, with some of the new street-level imaging applications, you don't always know if your image is being captured. This is why we think companies that engage in this activity have to let citizens know that they are going to be photographing the streets of their city, when this will happen, why, and how they can have their image removed if they don't want it in a database. For example, this could include visible marking on the vehicles that are used to capture the information, and notification using a variety of media (press release, local media outlets, service web site) outlining dates and locations for filming, the purpose for filming and how people can contact them with questions. Most people

probably don't expect their images to be captured by a company as they go about their business, but they may mind less if they have a choice to plan their day accordingly.

THE PRIVACY DIMENSION AND YOUR IMAGE ONLINE

Street-level imaging applications use various means of photographing the streetscape. Typically, a camera is mounted on a vehicle that is driven up and down the streets of selected cities. The images can then be viewed on the Internet.

Privacy Commissioners have had discussions with several companies to strengthen privacy protections for people whose images are captured. Our position is that all companies that offer such applications must take steps to better safeguard your privacy.

In addition to companies being proactive and creative in their public communications to ensure that Canadians know when their cities -- and, therefore, they themselves -- may be photographed, we think these companies need to be more privacy sensitive in the areas they choose. They need to be mindful that people entering or leaving sensitive locations, such as shelters or abortion clinics, likely want to remain anonymous for privacy and safety reasons.

They should also use proven and effective blurring technologies for faces and vehicle licence plates, so that people cannot be identified when their images are posted. Where individuals may be identifiable, companies must offer fast and responsive mechanisms to allow the images to be blocked or taken down.

Companies offering these imaging applications must also have a good reason to keep the original, unblurred images in their databanks. If they do retain unblurred images, they must limit how long they keep them and protect them with appropriate security measures.

THE BOTTOM LINE

Street-level imaging technology may offer benefits, but these should not come at the cost of your privacy.

That is why we encourage technology companies to ensure that you continue to enjoy your right to privacy, even when you're simply out in the park, walking your dog, or sunning yourself in your backyard.

Federal

Office of the Privacy Commissioner of Canada
www.priv.gc.ca

Provincial

Information and Privacy Commissioner of Alberta www.oipc.ab.ca

Information and Privacy Commissioner for British Columbia www.oipc.bc.ca

Commission d'accès à l'information du Québec www.cai.gouv.qc.ca

[1] Consent may be express or implied.

[2] In general, under Canadian private-sector privacy legislation, knowledge and consent are not required for journalistic, artistic or literary purposes. There are other exceptions and these can be found in the four applicable private-sector privacy laws: *Personal Information Protection and Electronic Documents Act*; *Personal Information Protection Act* (British Columbia); *Personal Information Protection Act* (Alberta); *La Loi sur la protection des renseignements personnels dans le secteur privé*.

APPENDIX B

PRELIMINARY LETTER OF FINDINGS

Complaints under the Personal Information Protection and Electronic Documents Act (the Act)

1) The Office of the Privacy Commissioner of Canada initiated three complaints against Google Inc. (Google) on May 31, 2010, pursuant to subsection 11(2) of the *Act*, after being made aware that Google Street View cars had been collecting payload data from unencrypted WiFi networks during their collection of publicly broadcast WiFi signals (service set identifiers [SSID] information and Media Access Control ("MAC") addresses.

2) The three complaints are as follows:

   i. Google's collection, use or disclosure of payload data was done without the individual's prior knowledge and consent;

   ii. Google's collection of payload data was done without prior identification of the purposes for which personal information (PI) was collected;

   iii. Google's collection of payload data was not limited to that which was necessary for the purposes identified.

Summary of Investigation

3) Following a request from the German data protection authority in Hamburg to audit the WiFi data collected by Google's Street View cars during a location-based project, Google discovered in May 2010 that it had been collecting payload data from unsecured wireless networks as part of its collection of WiFi data. By Google's own admission, it appears that this inadvertent collection was due to the integration of the code developed in 2006 with the software used to collect WiFi signals. As a result, Google grounded its Street View cars, stopped the collection of WiFi network data on May 7, 2010, and segregated and stored all of the data already collected.

4) On June 1, 2010, our Office sent a letter to Google stating that she was launching an investigation with regard to its collection of payload data. Google responded on June 29, 2010.

5) On June 28, 2010, pursuant to subsection 11(2) of the *Act*, this Office requested to undertake a site visit to Google's facility in Mountain View,

California. The purpose of this site visit was twofold: 1) to allow the review of the payload data gathered by Google, and 2) to ask specific questions of Google's representatives, such as the circumstances surrounding this incident, the segregation and storage of the payload data, and the mitigation and prevention measures Google intended to implement.

6) Google agreed to a site visit. Two technical representatives from this Office then went to the Mountain View facility on July 19, 2010. Although our technicians reviewed the payload data, no Google representatives were available in Mountain View to answer our questions. Instead, by letter dated July 16, 2010, Google answered general questions we posed in a questionnaire we sent on July 12, 2010.

7) On August 18, 2010, a videoconference was held between Google's counsel and this Office in order to answer supplementary questions.

8) The results of our investigation into the three complaints against Google are summarized below in the following sections:

A. Google's Product Counsel's involvement in product review;

B. Circumstances surrounding the collection of payload data and technical testing;

C. Personal information collected;

D. Segregation and storage of the payload data;

E. Google's future plans for its location-based services; and

F. Privacy implications of future plans, and mitigation and prevention measures that Google intends to implement to prevent a recurrence.

A. Google's Product Counsel's involvement in product review

9) Google advised that it has a formal review process for each external product launch. ("External product" denotes a product to be offered to consumers.) This process requires that a Product Counsel assess, among other things, the privacy implications of the product.

10) Since the code ultimately used to sample all categories of publicly broadcast WiFi data is not considered by Google to be an external product, the formal review process did not apply.

11) However, our investigation learned that Google's code design procedure includes a template and process by which the code must be reviewed by Product Counsel before being used or integrated with another Google

product. The template—a methodology document—is in fact mandatory and is the first step in the code design procedure.

12) Our investigation also learned that in the code design-procedure document for the particular code later to be used for the collection of WiFi signals, the engineer did identify one or more privacy concerns about the information collection. These relate to the fact that Google could obtain sufficient data to precisely triangulate a user's position at a given time.

13) The engineer qualified his concerns as being "superficial privacy implications". He did not forward his code design documents to Product Counsel for review—contrary to company procedure. Thus, the code's privacy implications were never assessed.

14) We were also informed that Google's Product Counsel Members consist of practising lawyers with various legal backgrounds. Google claims that they usually have some private-sector experience in privacy issues.

15) According to Google, Product Counsel Members attend the same introductory training session available to all new Google employees. As well, Product Counsel Members participate in weekly privacy- and security-issue meetings. Google also claims that "Privacy is part of the ongoing CLE [Continuing Legal Education] obligations of Google counsel."

B. Circumstances surrounding the collection of payload data and technical testing

16) Google allows its engineers to use 20% of their time to work on projects of interest to them. When using this time in 2006, a Google engineer developed code to sample all categories of publicly broadcast WiFi data.

17) The engineer involved included lines to the code that allowed for the collection of payload data. He thought it might be useful to Google in the future and that this type of collection would be appropriate.

18) This code was later used by Google when it decided to launch a particular location-based service. The service relies on a variety of signals (such as GPS, the location of cell towers and the location of WiFi access points) to provide the user with a location. Google installed antennas and appropriate software (including Kismet, an open-source application) on its Google Street View cars in order to collect publicly broadcast WiFi radio signals within the range of the cars while they travelled through an area. These signals are then processed to identify the WiFi networks (using their MAC address) and to map their approximate location (using the GPS co-ordinates of the car when the signal was received). This information on the identity of WiFi networks and their approximate location then populates the Google location-based services database.

19) In its representations to this Office, Google provided technical information on how it uses WiFi network data for location-based services. Google stated that its software does not store payload transmissions from encrypted networks, but that payload data sent over *unencrypted* WiFi networks is collected and "dumped" on a disk in raw format.

20) However, according to Google, the information thus collected would be fragmented because its cars are on the move when collection occurs and the equipment it uses to collect WiFi signals automatically changes channels five times per second.

21) To our investigation, Google acknowledged that it erred in including in the WiFi-network information-collecting software any code allowing the collection of payload data. Google contends that the code was primarily designed for data-collection software and that this purpose preceded its ultimate application in the collection of WiFi network information for location-based services. Google claims that it did not realize the presence of this code when it began using the software for its geo-location project.

22) It claims that when the decision was made to use the software for collecting publicly broadcast WiFi information, the code was reviewed for bugs and validated by a second engineer before being integrated with, and installed on, Street View cars. The purpose of this review was to ensure the code did not interfere with normal Street View operations. The code was not further examined to verify what kind of data was actually being obtained through the collection of WiFi publicly broadcast signals.

23) Google admitted that since it was not its intention to collect payload data and it never intended to use payload data in any of its products, it was not in a position to identify any purposes for the collection of these data or seek consent from affected individuals. Google also admitted that it did not inform any affected individuals of the fact that it was collecting payload data since its employees did not realize they were doing so until May 2010.

24) Google provided three reasons to explain why the collection of payload data was not discovered earlier:

    i. No one other than the engineer who developed the code was interested in looking at this program. No one thought payload data would be useful and no one had planned to use this data.

    ii. Payload data comprised a minuscule amount of the total data collected. Its collection was thus of minimal concern and no one had any reason to examine it.

iii. The engineer had not seen the ramifications of including this code and, consequently, had not spoken of it with his manager.

25) Google also asserted that since it had no purpose for the collection of payload data, there cannot be any justification for its retention. Consequently, Google is anticipating its secure destruction as soon as possible and is seeking this Office's authorization to do so.

26) Our investigation revealed that Google collected WiFi data in Canada from March 30, 2009 to May 7, 2010, and that its Street View cars have driven most urban areas and major roads.

27) Google stated that it cannot accurately distinguish between WiFi networks and wireless devices. It can, however, identify the unique number of basic service set identifiers (a.k.a. BSSIDs), which generally identify a single WiFi access point. Although the BSSID does identify an access point, it does not indicate how many devices or networks connect through the access point.

28) Google estimates that it collected over 6 million BSSIDs over the period its Street View cars drove throughout Canada.

C. Personal information collected

29) Our two technical experts visited Google's offices in Mountain View, California on July 19 and 20, 2010. The purpose of this site visit was for them to examine the data that had been collected by Google's Street View cars for Google's location-based services so as to determine its nature and the quantity involved. Their examination focussed on finding examples of personal information within the WiFi payload data collected in Canada.

30) Our technical experts searched the payload data to find anything that could constitute personal information (e.g., examples of e-mail, usernames, passwords and phone numbers). They produced an approximate count of possible personal information through an automated search. For example, the count included 787 e-mail headers and 678 phone numbers. However, a match does not mean a perfect identification. The searches may have included irrelevant items, or missed some items.

31) To complement the automated search, our experts performed a manual verification for five instances of each type of personal information. This was to demonstrate the existence of each data type, while preventing our experts from intruding too deeply into any individual's personal information.

32) Our technical experts found at least five instances of e-mails where they noted the presence of e-mail addresses, complete e-mail headers, IP addresses, machine hostnames, and contents of messages. The messages were truncated in the five instances of e-mails they found, but when performing a manual verification for other items (e.g., phone numbers), they observed complete e-mail messages.

33) They also found five instances of usernames. These could be seen in cookies, MSN messages and chat sessions. They also found one instance where a password and username were included in an e-mail message that a person was sharing with others to tell them how to log in to a server.

34) Our experts also found at least five instances of real names of individuals, five instances of residential addresses and five more of business addresses. They noted that, unlike the residential addresses, the business addresses were very common.

35) They also found five instances of instant messenger headers and five instances of phone numbers—both business and personal phone numbers. Like business addresses, business phone numbers were easier to find than personal ones.

36) A search for nine-digit or sixteen-digit numbers, which could have been Social Insurance Numbers (SIN) or credit card numbers, did not turn up anything due to there being too many other instances of irrelevant or similar numbers in the dataset. Therefore, although we found no evidence of SIN or credit cards numbers being collected, we still cannot entirely rule out the possibility that they were.

37) Our technical experts also noticed sensitive items during their searches. For example, they found a list of names, phone numbers, addresses and medical conditions for specified individuals. They also found a reference to someone stopped for a speeding violation, along with address information.

38) Our experts often saw cookies being passed from client machines to Web servers. These cookies were unencrypted and some contained personal information, including IP addresses, user names and postal addresses. They were surprised by the frequency of unencrypted cookies containing personal information.

39) In summary, our experts found many instances of personal information in the sample they took of the payload data collected in Canada by Google.

D. Segregation and the storage of the payload data

40) The WiFi data was collected through WiFi antennas attached to the roof of Street View cars. This WiFi antenna passively received the publicly

broadcast radio signals within range of the car using open-source Kismet software. The data was then relayed to a Google-developed application called “gStumbler” and its executable program “gslite”, which processed the data for storage. The data was then saved to hard drives physically located in each Street View car and then subsequently transferred to Google’s servers.

41) Google alleges it grounded its Street View cars and segregated the payload data on a restricted area of its network as soon as it became aware that its gStumbler application was collecting payload data from unencrypted WiFi networks.

42) As a follow up step, a Google system administrator copied onto a total of four disks the files containing the payload data collected in all affected countries. This was done from May 9, 2010, to May 13, 2010. These disks contained two copies of the data: one copy obtained after categorizing and labelling the data files by country, and one copy of the data before categorizing.

43) On May 15, 2010, the system administrator consolidated the payload data onto an encrypted hard drive, segregated by country. A second copy of the encrypted hard drive was made for security and backup preservation. The four original disks were then destroyed in a disk deformer.

44) A Google employee personally delivered one encrypted hard drive to another Google location for safekeeping, while the system administrator kept the other one in a secure location. Once the Google employee arrived at the destination, the system administrator permanently destroyed the backup, encrypted hard drive. The US data was then segregated onto a separate encrypted drive, while the data from the rest of the world remained on the initial encrypted drive.

E. Google’s future plans for its location-based services

45) Google still intends to offer location-based services, but does not intend to resume collection of WiFi data through its Street View cars. Collection is discontinued and Google has no plans to resume it.

46) Google does not intend to contract out to a third party the collection of WiFi data.

47) Google intends to rely on its users’ handsets to collect the information on the location of WiFi networks that it needs for its location-based services database. The improvements in smart-phone technology in the past few years have allowed Google to obtain the data it needs for this purpose from the handsets themselves.

48) Although it has no tracking tool to keep records of a customer's locations (and does not intend to create one), Google acknowledges that it does need to examine the potential privacy concerns of this method of collection.

F. Privacy implications of future plans, and mitigation and prevention measures

49) Google submits that it is striving to design privacy protections into all its products and services. It states that its employees receive orientation and code-of-conduct training that includes a privacy and data-security component. However, the responsibility of aligning Google's projects with its Privacy Principles and Privacy Policy lies with each of its product and engineering teams.

50) Google also states that as products are chartered or otherwise provided with resources and staffing, they are assigned to a Product Counsel in Google's legal department. This individual has a first-level responsibility for identifying privacy issues in a product.

51) In order to avoid a recurrence of a product design having a negative impact on privacy, Google claimed to be reviewing its product launch procedures, code review procedures and 20% time policy. In so doing, it would ensure that its internal controls are robust enough to adequately address future issues. As of the issue date of this report, Google's review of its procedures/policies has not yet been completed.

Application

52) In making our determinations, we applied Principles 4.1.1 and 4.1.2 of the *Personal Information Protection and Electronic Documents Act*. Principle 4.1.1 stipulates that accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s). Principle 4.1.2 continues that the identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

53) We also applied Principle 4.2, which states that the purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

54) Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate

55) Lastly, Principle 4.4 states that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.

Findings

56) On September 15, 2010, I shared an earlier version of this report with Google and invited their response. Taking into consideration their response, I have revised my preliminary letter of findings. What follows is a summary of our findings and recommendations.

Collection of personal information

57) During their site visit, our technical experts uncovered substantial amounts of personal information in the form of e-mail message content (e.g., e-mail, IP and postal addresses), captured in Google's collection of payload data in Canada.

58) Google acknowledged to this Office that it did collect payload data, but not with the intent of using it in any of its products. According to Google, it was "simply mistaken" in collecting the data and did not seek consent from the affected individuals. Principle 4.3 of the *Act* requires that the knowledge and consent of the individual be obtained for the collection, use or disclosure of their personal information.

59) Google also stated that it had not identified any purposes for the collection of the payload data. Principle 4.2 requires that such a purpose be identified at or before the time of collection. Further, Principle 4.4 stipulates that the collection of personal information be limited to that which is necessary for the purposes identified. Since no purpose could be identified, it follows that the collection in this case clearly could not be limited to any specific purpose. This is in violation of Principle. 4.4.

Google's Product Counsel's involvement

60) Due to the engineer's failure to forward his design document to the Product Counsel, the Counsel was unable to assess the privacy implications of the code designed to collect WiFi data. This is a careless error that I take very seriously since a review of design documents by a Product Counsel (and the use of a template) is clearly a mandatory step in Google's code design procedure.

61) As a result, the un-scrutinized code was later used to collect data containing personal information. If the Product Counsel had been involved when and as it should have been, Google may have discovered the risk of data over-collection and would have been in a position to remedy the situation before any collection took place. The ensuing negative effects on citizens' privacy and Google's reputation could easily have been avoided.

62) Google informed our Office that engineering and product teams are accountable for complying with Google's privacy policies and principles. Google then stated that it is working towards improving its code-and-product review processes, as well as accountability mechanisms, for engineering and product management personnel in order to improve their sensitivity to privacy issues at all stages of product and code development. A legal team is working with engineering directors to ensure a comprehensive review of codes for any privacy issues. Google believes that the review of its policies and procedures that it has undertaken will ensure no recurrences. Google stated that it will keep this Office informed as Google completes its review.

Code review and testing

63) Google asserted that the engineer who developed the lines of code did not see its ramifications of ultimately allowing the collection of a broader range of data from wireless networks. Our investigation was not able to determine with certainty if this was a one-time error committed by one individual or, perhaps, a sign of a more generalized lack of awareness among employees with regards to privacy implications of new products. At Google, the effects of new products on privacy should be well understood not only by the Product Counsel but also by the professionals who develop these products.

64) In this case, the review and testing of the product containing the code were insufficient to assess privacy impact. It would appear that the review consisted merely of ensuring that the product did not interfere with a second application—that used to collect pictures of the streets navigated by Street View vehicles.

65) As our investigation revealed, the review was not able to assess the extended capabilities of the product—including its ability to collect more information than necessary for the location-based project.

Steps taken to protect payload data

66) Once Google realized its Street View cars were collecting more data from wireless networks than anticipated, Google expressed regret in inadvertently collecting the publicly broadcast data. It immediately

grounded its vehicles and took measures to safeguard the collected payload data and segregate it by country of origin.

67) Google's actions were justified, appropriate and sufficient to safeguard the payload data collected in Canada. In my view, Google upheld the related safeguard provisions under the *Act*.

68) Concerning the data that Google collected, it affirmed that it has no desire to use the Canadian payload data in any manner and will continue to secure the data with strenuous access restrictions until it is deleted.

69) To this, I would like to add that not only privacy laws, but other applicable laws in the U.S. and in Canada, including laws of evidence, must also be taken into account in determining when to delete the Canadian payload data collected.

Future plans

70) The fact that Google does not intend to resume collection of WiFi data with its Street View cars eliminates the possibility of further inappropriate collection of personal information through the tool developed by its engineer.

71) However, from users' handsets, Google intends to obtain the information needed to populate its location-based services database. This alternative method of collection could also lead to inappropriate collection and retention of personal information if Google does not put in place appropriate safeguard measures.

Recommendations

72) I share Google's goal to avoid recurrences of any similar violations of individuals' privacy. While I am pleased that Google has taken under review its processes and procedures that could impact privacy, I would nonetheless like the organization to ensure that these controls are complemented by an overarching governance model embodying all privacy issues pertaining to the design of internal/external products and services. I would also like Google to respect reasonable timelines to implement both the governance model and the revised processes and procedures. With this view, and after reviewing the additional information Google provided this Office, I am making the following recommendations:

i. That Google re-examine and improve the privacy training it provides all its employees, with the goal of increasing staff awareness and understanding of Google's obligations under privacy laws.

ii. That Google ensure it has a governance model in place that includes:

- effective controls to ensure that all necessary procedures to protect privacy have been duly followed prior to the launch of any product;

- clearly designated and identified individuals actively involved in the process and accountable for compliance with Google's obligations under privacy laws.

iii. That Google delete the Canadian payload data it collected, to the extent that Google is allowed to do so under Canadian and U.S. laws. If the Canadian payload data cannot immediately be deleted, the data needs to be properly safeguarded and access thereto is to be restricted.

73) At this time, I consider the matter to be **well-founded** and still **unresolved**. My Office will only consider the matter resolved upon receiving either by or before February 1, 2011, confirmation of the implementation of the above recommendations, at which point I will issue my final report and conclusions.

APPENDIX C

LIST OF WITNESSES
SECOND SESSION, 40TH PARLIAMENT

Organizations and Individuals	Date	Meeting
Canpages Inc.	2009/06/17	29
Olivier Vincent, President and Chief Executive Officer		
Google Inc.		
Jonathan Lister, Managing Director and Head of Google Canada		
Office of the Privacy Commissioner of Canada	2009/10/22	32
Carman Baggaley, Strategic Policy Advisor		
Daniel Caron, Legal Counsel, Legal Services, Policy and Parliamentary Affairs Branch		
Elizabeth Denham, Assistant Privacy Commissioner		

THIRD SESSION, 40TH PARLIAMENT

Organizations and Individuals	Date	Meeting
Office of the Privacy Commissioner of Canada	2010/10/28	28
Daniel Caron, Legal Counsel, Legal Services, Policy and Parliamentary Affairs Branch		
Patricia Kosseim, General Counsel		
Andrew Patrick, Information Technology Research Analyst		
Google Inc.	2010/11/04	30
Jacob Glick, Canada Policy Counsel		
Google Inc.	2010/11/25	34
Jacob Glick, Canada Policy Counsel		
Alma Whitten, Engineering Lead for Privacy		
Yellow Pages Group Co.		
Martin Aubut, Senior Manager, Social Commerce		
François D. Ramsay, Senior Vice-President, General Counsel, Secretary and Responsible for Privacy		

APPENDIX D

LIST OF BRIEFS
SECOND SESSION, 40TH PARLIAMENT

Organizations and individuals
Google Inc.

MINUTES OF PROCEEDINGS

A copy of the relevant Minutes of Proceedings (40th Parliament, 3rd Session: Meetings Nos. 28, 30, 32, 34, 37 and 39) and (40th Parliament, 2nd Session: Meetings Nos. 29 and 32) is tabled.

Respectfully submitted,

Hon. Shawn Murphy, P.C., MP
Chair