UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

October 27, 2010

Albert Gidari, Esq.
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, WA 98101-3099

Dear Mr. Gidari:

I am writing regarding your client Google's announcement about its collection of consumer data transmitted over unsecured wireless networks. According to Google's announcement, in 2007, the company installed software on its "Street View" cars[1] to collect data about consumers' wireless network access points for the purpose of improving its location-based services. Earlier this year, in response to a request from the data protection authority in Hamburg, Germany, Google discovered that the software on the Street View cars had also been collecting some "payload" data – contents of communications sent over unsecured wireless networks. The company stated that the collection of payload data was inadvertent and that the company did not use the payload data in any Google product or service.[2]

FTC staff has concerns about the internal policies and procedures that gave rise to this data collection. As noted above, the company did not discover that it had been collecting payload data until it responded to a request for information from a data protection authority. This indicates that Google's internal review processes – both prior to the initiation of the project to collect data about wireless access points and after its launch – were not adequate to discover that the software would be collecting payload data, which was not necessary to fulfill the project's business purpose. These review processes are necessary to identify risks to consumer privacy posed by the collection and use of information that is personally identifiable or reasonably linkable to a specific consumer. For *any* such information, Google should develop and implement reasonable procedures, including collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored.

---

[1] Google's Street View program provide street-level imagery of locations through the company's Google Maps product. The images are collected primarily by Street View cars, which include directional cameras to capture 360° views, a GPS unit for positioning and laser range scanners. *See* Google Maps with Street View, Behind the Scenes, *available at* http://maps.google.com/help/maps/streetview/behind-the-scenes.html#vehicles.

[2] *See* Official Google Blog, WiFi Data Collection: An Update (May 14, 2010), *available at* http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

Chairman Leibowitz highlighted some of these issues in his testimony before the Senate Commerce Committee on July 27, 2010.[3] As you know, the FTC has undertaken a project to re-examine its approach to consumer privacy in light of changing technologies and business practices.[4] During a series of public roundtables, panelists raised concerns about companies' collecting more consumer information than necessary to fulfill a legitimate business need. A related concern was that companies are storing consumer data for longer periods (at lower cost) and will find new uses for it that consumers may not have contemplated at the time of collection. Accordingly, panelists and commenters discussed the need for companies to build strong privacy protections into their products and business operations at the outset.

To this end, we note that Google has recently announced improvements to its internal processes to address some of the concerns raised above, including appointing a director of privacy for engineering and product management; adding core privacy training for key employees; and incorporating a formal privacy review process into the design phases of new initiatives. The company also publicly stated its intention to delete the inadvertently collected payload data as soon as possible.[5] Further, Google has made assurances to the FTC that the company has not used and will not use any of the payload data collected in any Google product or service, now or in the future. This assurance is critical to mitigate the potential harm to consumers from the collection of payload data.[6] Because of these commitments, we are ending our inquiry into this matter at this time.

We ask that the company continue its dialogue with the FTC about how best to protect consumer privacy as it develops its products and services.

Sincerely,

David Vladeck | KDR

David C. Vladeck

---

[3] *See* Prepared Statement of the Federal Trade Commission on Consumer Privacy before the Committee on Commerce, Science, and Transportation, United States Senate, at 22 (July 27, 2010), *available at* http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

[4] *See* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[5] *See* Official Google Blog, Creating Stronger Privacy Controls Inside Google (Oct. 22, 2010), *available at* http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

[6] *See id.*

Personal Data (Privacy) Ordinance ("the Ordinance")
Google Street View Cars Collecting Wi-Fi Payload Data in Hong Kong

Decision by the Privacy Commissioner for Personal Data ("the Commissioner")

Case No.: 201006847 **Date issued: 30 July 2010**

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

The Background

Google Inc. ("Google") announced on 14 May 2010 that it had mistakenly collected the unencrypted Wi-Fi payload[1] data while it should only have captured the Service Set Identifiers (SSIDs[2]) and the Media Access Control (MAC[3]) addresses of Wi-Fi routers for the purpose of its location-based services during the exercise of taking pictures by the Google Street View cars being driven around in Hong Kong during the period from December 2008 to October 2009. Google submitted that the equipment that had collected the payload data changed channels five times a second so the collected data would have been snippets of information.

2. As the Wi-Fi payload data might contain personal data of individuals collected without their knowledge, the matter raises personal data privacy concerns on compliance with the requirements of the Ordinance. Similar happenings had been reported in other parts of the world in which Google Street View cars operated and the matter had received international attention.

Immediate Actions Taken by PCPD

3. In exercise of his regulatory functions to supervise and monitor compliance with the requirements of the Ordinance, the made a public announcement on 17 May 2010 to begin a compliance check against Google. Google's representative in Hong Kong was invited to attend before the Commissioner on 18 May 2010. During the meeting, Google's representative expressed deep regret to the Commissioner about the collection of personal data through the Wi-Fi network[4].

4. At the suggestion of the Commissioner that immediate remedial actions should be taken by Google, Google signed and gave an Undertaking[5] to the Commissioner on 7 June 2010 to the effect that :

(a) Google had ceased operating its Street View cars in Hong Kong;
(b) when Street View cars commence driving in Hong Kong again they would not collect Wi-Fi data;
(c) it would provide the Office of the Privacy Commissioner for Personal Data ("PCPD") access to the Wi-Fi payload data collected in Hong Kong ("the Data") and such assistance that

---

[1] The actual contents of Wi-Fi communications
[2] Names of Wi-Fi networks
[3] The unique number given to a device like a Wi-Fi router
[4] See media statement: http://www.pcpd.org.hk/english/infocentre/press_20100518.html
[5] See media statement: http://www.pcpd.org.hk/english/infocentre/press_20100608.html

might be required to facilitate PCPD's understanding of the collection and interpretation of the Data;

(d) it would securely store the Data and not to tamper with or subject the Data to any unauthorised uses or access which may contravene the laws of Hong Kong;

(e) it would completely delete the Data and provide PCPD with an independent third party's verification of such deletion;

(f) it would provide PCPD a copy of an analysis by an independent technical service firm which reviewed the source code involved in the payload data collection; and

(g) future Street View car operations carried out in Hong Kong would comply with the requirements of the Ordinance.

The Examination of Collected Payload Data

5. Since the Data could not be read and interpreted without a decoder developed by Google, Google was asked to provide the necessary technical assistance to enable examination and understanding of the Data by officers of PCPD. Google subsequently provided facilities to PCPD's officers to examine the Data on 23 and 24 June 2010 at its Hong Kong Office. As it was reasonable to suspect that the majority of the messages captured were in the Chinese language, Google was asked by PCPD to develop a Chinese decoder. With the development of the Chinese decoder a third examination was conducted by PCPD officers on 9 July 2010.

6. During the examination, Google showed PCPD the Data which comprised 364 files in 44 folders with a total size of 358MB (megabytes). As it was impractical to browse through all the contents manually, keyword-based searches were first conducted on the files and then all matches examined manually to determine the type of messages collected.

7. Using the above approach, the results of the examination showed that only a minimal amount of personal data, often fragmented pieces instead of a whole and complete content of the data were captured. As was suspected, the majority of the messages captured were in the Chinese language and consequently more data were found in the third examination with the assistance of the Chinese decoder which was developed for this purpose. Even then, my officers found that the amount of personal data such as email messages remained low. The type of messages seen were mainly :

(a) Small number of fragmented email messages containing names, business addresses, phone numbers and recipient email addresses;

(b) Instant messages such as MSNs;

(c) Social networking messages such as the 'Wall' messages in Facebook;
(d) Fragments of discussion forum postings;
(e) Fragments of web pages; and
(f) Fragments of downloading/sharing messages such as the headers of Foxy, BitTorrent (BT) downloads.

8. No sensitive personal data, such as passwords or contents of the whole of email messages, etc. were detected.

Further Evidence Obtained from Google

9. On 29 July 2010, Google provided an Affidavit ("the Affidavit") to the Commissioner confirming that :

(a) the Undertaking given by Google on 7 June 2010 remained effective, except to the extent its terms had already been satisfied;
(b) its senior management team had no actual knowledge that the Data were being collected in Hong Kong and stored;
(c) the equipment which collected the Data changed Wi-Fi channels five times a second thus only collected fragments of information;
(d) the Data had never been used by Google and had not been transferred before outside of Google; and
(e) Google has not accessed or converted the Data, except pursuant to the formal written requests by PCPD.

10. There exists no evidence upon which the Commissioner can rely to contradict the statements made in the Affidavit.

Matters Taken into Consideration

11. The Commissioner has considered all the circumstances of the case, in particular :

(a) The amount and extent of personal data captured which did not reveal any significant amount of personal data; a large proportion (over 90%) of the Data were examined and the amount of personal data collected was negligible and non-sensitive;
(b) The fact that Google had to develop and experiment with the Chinese decoder, as observed during its development stage,

suggests that Google had not itself studied the contents of the Data before;

(c) The immediate remedial measures taken by Google as set out in the Undertaking, especially its commitment not to collect Wi-Fi Data in its future Street View car operations;

(d) The Affidavit deposing to the lack of intention to collect the Data and the Commissioner did not have any reason to disbelieve this; and

(e) Google's Undertaking that its future operations of the Street View cars shall comply with the requirements of the Ordinance.

The Conclusion

12. While the Commissioner does not preclude the possibility that other data protection authorities may find that personally identifiable data had been collected in their jurisdictions, he is reasonably satisfied that in regard to the Wi-Fi data captured by Google in its Street View car operation in Hong Kong, they do not contain any meaningful details that can directly identify any one individual.

13. Furthermore, the Commissioner has no reason to disbelieve Google's assertion that Google had no intention to compile personal information through the Street View car operation in Hong Kong and that it had not accessed or used any of the Wi-Fi data captured in Hong Kong through the operation.

14. The Commissioner has decided not to carry out a formal investigation of the case since he cannot reasonably expect to obtain a more satisfactory result than that already achieved, i.e. the procurement of the Undertaking which sets out the remedial measures that Google will take in this incident.

15. The Commissioner has concluded this case on the bases mentioned above. Since no formal investigation will be carried out, there is no finding of a contravention. It is to be stressed that, the decision in this case is made without prejudice to the exercise by the Commissioner of his regulatory functions and powers in relation to any other matter or complaint concerning the future operation of the Street View cars.

Deletion of the Data

16. The Commissioner is conscious of the reality that even after a complex and contracted investigation he would still be left with the option to issue an enforcement notice requiring Google to erase the Data and to adopt the remedial measures contained in the Undertaking. That being the case, the

Commissioner has asked Google to completely and irreversibly erase all the Wi-Fi payload data collected in Hong Kong, and to provide to the Commissioner a third-party verification of such erasure.

Roderick B. WOO
Privacy Commissioner for Personal Data

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

專員用箋 From the desk of the Commissioner

Our Ref.: 201006847

(By Fax: 3923 5401 & By hand)

30 July 2010

Google Inc.
Suite 1706,
Tower 1, Times Square
1 Matheson Street
Causeway Bay
Hong Kong
(Attn: Mr. Ross LaJeunesse, Head of Government Affairs, Asia Pacific)

Dear Sirs,

Personal Data (Privacy) Ordinance (the "Ordinance")
Case No: 201006847

I am writing to inform you of the result of the compliance check carried out by the Office of the Privacy Commissioner for Personal Data ("**PCPD**") regarding the collection of Wi-Fi payload data in Hong Kong by the Street View cars operated by Google Inc. ("**Google**"),

2. After protracted enquiries I have decided not to carry out a formal investigation without a finding of any contravention by Google of the requirements of the Ordinance. The reasons are detailed in my Report which is attached.

3. In accordance with the Undertaking dated 7 June 2010 and the Affidavit dated 29 July 2010, both provided by Google, I hereby direct Google

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話Tel (852) 2877 7168 傳真Fax (852) 2877 7026
電郵 Email roderickbwoo@pcpd.org.hk 網址 Website www.pcpd.org.hk

to completely and irreversibly delete the payload data identified as coming from Hong Kong, and provide the Privacy Commissioner with an independent third-party verification of the deletion within 14 days.

4. I wish to stress that the decision in this case is made without prejudice to the exercise by the Privacy Commissioner of his regulatory functions and powers in relation to any other matter or complaint concerning the future operation of the Street View cars.

Yours faithfully,

Roderick B. WOO
Privacy Commissioner for Personal Data

c.c. Google Inc
(Attn: Mr. William FARRIS)
(Email address : wafarris@google.com)

Google Inc
(Attn: Ms. Nicole WONG)
(Email address : nicolew@google.com)

Statement

29 July 2010

Google – Assessment of WiFi data

A spokesperson for the Information Commissioner's Office (ICO) said:

"The ICO has visited Google's premises to assess samples of the 'pay-load' data it inadvertently collected. Whilst Google considered it unlikely that it had collected anything other than fragments of content, we wanted to make our own judgement as to the likelihood that significant personal data had been retained and, if so, the extent of any intrusion. The information we saw does not include meaningful personal details that could be linked to an identifiable person. As we have only seen samples of the records collected in the UK we recognise that other data protection authorities conducting a detailed analysis of all the payload data collected in their jurisdictions may nevertheless find samples of information which can be linked to identifiable individuals. However, on the basis of the samples we saw we are satisfied so far that it is unlikely that Google will have captured significant amounts of personal data. There is also no evidence as yet that the data captured by Google has caused or could cause any individual detriment. Nevertheless it was wrong to collect the information. We will be alerting Privacy International and others who have complained to us of our position. The Information Commissioner is taking a responsible and proportionate approach to this case. However, we remain vigilant and will be reviewing any relevant findings and evidence from our international counterparts' investigations."

For all media enquires, please contact the ICO press office on 0207 025 7580

For all general enquires, please contact the ICO customer service team on 08456 306060