Google Australia Pty Ltd
Level 5, Workplace 6
48 Pirrama Road
Pyrmont NSW 2009

Main 61 2 9374 4000
Fax 61 2 9374 4001
www.google.com.au

19 May 2010

Geordie Guy
Vice-Chair, EFA
gguy@efa.org.au

Dan Svantesson
Vice-Chair, APF, and Chair APF Internet SubCommittee
vicechair2@privacy.org.au

Dear Geordie and Dan,

Thanks for your recent letter about the collection and use of WiFi-related Information.

Firstly, I'm sure you have seen our recent blog post (enclosed) about WiFi data collection. In that post we stated that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, though we never used that data in any Google products. As soon as we became aware of this problem, we grounded our Street View cars and segregated the data on our network; we then disconnected it to make it inaccessible to anyone other than the specific engineers with responsibility for deleting the data.

Maintaining people's trust is crucial to everything we do, and in this case we fell short. So we will be asking a third party to review the software at issue, and internally reviewing our procedures to ensure that our controls are sufficiently robust to address these kinds of problems in the future. In addition, given the concerns raised, we have decided that it's best to stop our Street View cars collecting WiFi network data entirely.

We are aware of the views expressed by privacy regulators regarding our collection of WiFi-related information and we plan to work with the authorities in the relevant countries to answer their questions and appropriately delete the WiFi payload data as quickly as possible.

In response to the specific questions you raise in your letter about our collection of WiFi data

1. What type of wireless network information is Google collecting (i.e. what beyond the SSID and MAC address is being recorded)?

As announced in our 14 May blog post we have decided to stop our Street View cars collecting WiFi network data entirely. Up to that time our Street View cars had been collecting publicly broadcast information sent over WiFi networks. This includes SSID information, MAC addresses,

and, mistakenly, samples of payload data from open (i.e. non-password-protected) WiFi networks.

2. What is the purpose of collecting this data?

We collected publicly broadcast WiFi data like geo codes and MAC addresses to improve our location-based services. GPS is not always available (it is unreliable indoors), while cell tower data is often insufficiently accurate. By treating WiFi access points as "beacons," smart phones are able to fix their general location quickly in a power-efficient way.

3. Beyond the purposes that led to its collection, how does Google intend to use, store and make available this information?

We have no plans to use any payload information or make it available at all. Indeed, we plan to delete the payload data as quickly as possible. The payload information on our network has been segregated and made inaccessible except for the specific engineers designated with responsibility for deleting the data. The SSID and Mac addresses previously collected were used as described in our answer to Question 2 above.

4. What other information, beyond that mentioned in the blog post, does Google collect as part of its provision of the Street View product, beyond the recently revealed wireless network information, and self evident information such as visual depictions of streets?

In addition to the now-ceased collection of WiFi data and photos, our Street View cars also collect 3-D building imagery. We collect 3D geometry data with low power lasers (similar to those used in retail scanners) which we can use for Google Maps and Google Earth. With this data, we can build rich 3D models to add to the immersive experience of Google Earth and we can build improved navigation features for Street View

I trust this letter answers the questions you have raised.

Yours sincerely

Iarla Flynn
Head of Public Policy & Government Affairs

WiFi data collection: An update

5/14/2010 01:44:00 PM

Update May 17, 2010:

On Friday May 14 the Irish Data Protection Authority asked us to delete the payload data we collected in error in Ireland. We can confirm that all data identified as being from Ireland was deleted over the weekend in the presence of an independent third party. We are reaching out to Data Protection Authorities in the other relevant countries about how to dispose of the remaining data as quickly as possible.

You can read the letter from the independent third party, confirming deletion, here.

[original post]

Nine days ago the data protection authority (DPA) in Hamburg, Germany asked to audit the WiFi data that our Street View cars collect for use in location-based products like Google Maps for mobile, which enables people to find local restaurants or get directions. His request prompted us to re-examine everything we have been collecting, and during our review we discovered that a statement made in a blog post on April 27 was incorrect.

In that blog post, and in a technical note sent to data protection authorities the same day, we said that while Google did collect publicly broadcast SSID information (the WiFi network name) and MAC addresses (the unique number given to a device like a WiFi router) using Street View cars, we did not collect payload data (information sent over the network). But it's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products.

However, we will typically have collected only fragments of payload data because: our cars are on the move; someone would need to be using the network as a car passed by; and our in-car WiFi equipment automatically changes channels roughly five times a second. In addition, we did not collect information traveling over secure, password-protected WiFi networks.

So how did this happen? Quite simply, it was a mistake. In 2006 an engineer working on an experimental WiFi project wrote a piece of code that sampled all categories of publicly broadcast WiFi data. A year later, when our mobile team started a project to collect basic WiFi network data like SSID information and MAC addresses using Google's Street View cars, they included that code in their software—although the project leaders did not want, and had no intention of using, payload data.

As soon as we became aware of this problem, we grounded our Street View cars and segregated the data on our network, which we then disconnected to make it inaccessible. We want to delete this data as soon as possible, and are currently reaching out to regulators in the relevant countries about how to quickly dispose of it.

Maintaining people's trust is crucial to everything we do, and in this case we fell short. So we will be:

- Asking a third party to review the software at issue, how it worked and what data it gathered, as well as to confirm that we deleted the data appropriately; and
- Internally reviewing our procedures to ensure that our controls are sufficiently robust to address these kinds of problems in the future.

In addition, given the concerns raised, we have decided that it's best to stop our Street View cars collecting WiFi network data entirely.

This incident highlights just how publicly accessible open, non-password-protected WiFi networks are today. Earlier this year, we encrypted Gmail for all our users, and next week we will start offering an encrypted version of Google Search. For other services users can check that pages are encrypted by looking to see whether the URL begins with "https", rather than just "http"; browsers will generally show a lock icon when the connection is secure. For more information about how to password-protect your network, read this.

The engineering team at Google works hard to earn your trust—and we are acutely aware that we failed badly here. We are profoundly sorry for this error and are determined to learn all the lessons we can from our mistake.

Posted by Alan Eustace, Senior VP, Engineering & Research