

Google Inc
1600 Amphitheatre Parkway
Mountain View, CA 94043

c/o Peter Fleischer
Global Privacy Counsel
Google France
38 avenue de l'Opéra
75002 Paris
France

3 November 2010

Dear Mr Fleischer

Re: Google Street View (GSV) collection of payload data

In May 2010, Google announced that payload data from unencrypted wi-fi networks had been mistakenly collected by specially adapted vehicles which formed part of the GSV fleet.

It is understood that Google installed antennae and appropriate software on its GSV cars in order to collect publicly available wi-fi radio signals whilst the vehicles travelled through an area. The purpose was to identify wi-fi networks and to map their approximate location using the GPS co-ordinates of the GSV car when the radio signal was received. The aim was to build and improve the geo-location database for location-based mobile applications.

Google suggested that the payload data collected was likely to be fragmentary and also that it had not been analysed by Google. It was therefore not possible for Google to say whether or not any data which formed part of the payload data collected was personal information about any identifiable individual.

Staff from my office visited your premises and viewed a sample of the payload data which had been collected from the UK. They agreed that the data was fragmentary and was unlikely to constitute personal data.

On the 22nd October 2010 Alan Eustace, Senior VP, Engineering and Research posted further information about the collection of payload data on the Official Google Blog. Mr. Eustace, in the final paragraph of the blog wrote the following:

Finally, I would like to take this opportunity to update one point in my May blog post. When I wrote it no one inside Google had analyzed in detail the data we had collected, so we did not know for sure what the disks contained. Since then a number of external regulators have inspected the data as part of their investigations (seven of which have now been concluded). It's clear from those inspections that whilst most of the data is fragmentary, in some instances entire emails and URLs were captured, as well as passwords.

My office now understands that GSV cars driving in the UK before May 2010 were equipped with the same equipment as the GSV cars in countries where regulators found some instances where entire emails and URLs were captured, as well as passwords. As such, my office believes that while most of the payload data gathered from the UK is fragmentary, in some instances it is possible that entire emails and URLs were captured, as well as passwords. It is my view that the collection of this information is a serious breach of the first data protection principle:

Personal data shall be processed fairly and lawfully and in particular shall not be processed unless:

- *At least one of the conditions in Schedule 2 is met; and*
- *In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

Schedule 2 Conditions for processing.

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):

- *The data subject has given his consent to the processing.*
- *The processing is necessary:*

(a) for the performance of a contract to which the data subject is a party,

(b) for the taking of steps at the request of the data subject with a view to entering into a contract

- *The processing is necessary to comply with any legal obligations to which the data controller is subject, other than an obligation imposed by contract.*
- *The processing is necessary in order to protect the vital interests of the data subject.*

The payload data was collected without the consent of the data subjects.

It is my view that regulatory action is appropriate in this case in order to ensure that effective privacy controls are built into Google products and services, and in order to ensure that an incident such as the collection of payload data by GSV cars is not repeated. It is my view that as an alternative to the issuance of an Enforcement Notice under section 40 of the Data Protection Act 1998, that the data controller should sign an undertaking.

To ensure that GSV complies with the first principle of the Data Protection Act 1998 the undertaking will require Google in the UK to take the following steps:

- To continue and update orientation programs designed to provide Google employees with training on Google's privacy principles and the requirements of UK data protection law.
- To institute a policy that requires Google employees to be trained on Google's code of conduct, which includes sections on privacy and the protection of user data and the legal requirements applying to the protection of personal data in the UK.
- To enhance the core training for engineers and other important groups with a particular focus on the responsible collection, use and handling of data.
- To institute a security awareness program for Google employees, which will include clear guidance on both security and privacy.

- To institute a policy that requires engineering project leaders to maintain a privacy design document for each initiative they are working on, and a policy that such document should (a) record how user data is handled and (b) be reviewed regularly by managers.
- Within nine months from the date of the undertakings to facilitate a consensual audit by the ICO of the above internal privacy and security practices.
- To delete the UK payload data it collected, to the extent that Google has no other outstanding legal obligation to retain such data.

I attach a copy of the undertaking which I ask is signed and returned to my office within 21 days. As you are aware once signed the undertaking will be published on the ICO website.

Yours Sincerely

Christopher Graham