



June 9, 2010

Chairman Henry A. Waxman
Representative Joe Barton
Representative Edward J. Markey
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Waxman, Ranking Member Barton, and Congressman Markey:

Thank you for your letter of May 26, 2010, requesting information about collection of data from WiFi networks. We welcome this opportunity to provide more information, and we would be happy to discuss this with you further.

As an initial matter, we thought it might be helpful to provide some background information about WiFi networks generally and about how information about WiFi networks can be used to enhance location-based services.

The purpose of a WiFi network is to permit enabled devices (such as a laptop or mobile phone) to connect to the Internet and communicate with each other. To do so, the network broadcasts a radio signal with its "service set identifier," or SSID, and its unique hardware or router identifier, known as a MAC address, and other network-related information. This broadcast information can be detected by WiFi-enabled devices to facilitate the network connection. Networks generally are configured to be readily accessible to the general public. The network owner can choose to keep the network openly accessible (not secured by encryption and thus accessible by any user's device) or to have the network closed (secured by encryption and accessible only by authorized devices).

Information about the location of WiFi networks improves the accuracy of the location-based services, such as Google Maps or driving directions, that Google provides to consumers. For example, a user of Google Maps for mobile phones can turn on a smart phone's "My Location" feature to identify his or her approximate location based on GPS signals (where available) and signals from the cell towers and WiFi networks visible to the device. Because GPS and cell tower location data can be unreliable or inaccurate, in some cases using the location of WiFi access points can enable a smart phone to pinpoint its own location more quickly and accurately.

Google Street View cars were outfitted with commercially available WiFi antennas and software on board our Street View cars. The system detected and collected WiFi network data, including SSID,

MAC address, signal strength, data rate, channel of the broadcast, and type of encryption method. The data was relayed to Google-developed software that processed the data for storage, and eventually used to improve location-based services. This information was not used to identify any specific individual or household.

Other than the use of Street View cars as a platform for the WiFi equipment, Google's Street View and the collection of WiFi network information have been two entirely separate efforts. Street View is a feature of Google Maps that allows consumers to view 360-degree panoramic street-level photographs. The photographs are taken by cameras mounted on Google's Street View cars and depict what is visible from the street. WiFi information is not linked with Street View imagery, and Google does not share this WiFi information with third parties.

Recently, we became aware that we had mistakenly included code in our software that collected samples of "payload data" -- information sent over the network -- from open (unencrypted) networks. Payload data from closed (encrypted) networks was not stored. Because Google Street View cars are on the move and the WiFi equipment automatically changes channels five times per second (and because WiFi frequency bands include 11 channels in the U.S.), we believe any payload data collected would likely be fragmented. It is possible that the payload data may have included personal data if a user at the moment of collection broadcast such information, but we have not conducted an analysis of the payload data in a way that enables us to know exactly what was collected.

The payload data has never been used in any Google product or service, nor do we intend to use it. In fact, based on our current investigation, we are aware of only two instances when any Google engineer even viewed the payload data. The first instance involved the individual engineer who designed the software. The second instance was when we became aware that payload data may have been collected from unencrypted WiFi networks and a single security engineer tested the data to verify that this was the case.

As soon as we became aware of this problem, we grounded our Street View cars and segregated the payload data on our network. We then removed the data from the Google network so that it is inaccessible to anyone other than those responsible for securing the data, and we continue to take steps to safeguard payload data.

As part of our investigation of this matter, we have had an independent technical services firm, Stroz Friedberg LLC, review the software at issue. We have just posted a copy of the completed report, and invite you to examine it (<http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>). We have also attached a copy for your reference. As the report confirms, we did not store encrypted payload data, and the payload data was not parsed for use; instead, it was stored in raw, aggregate, binary form. We are also reviewing our procedures to ensure that our controls are

sufficiently robust to address these kinds of problems in the future. Given the concerns raised, we have decided to stop our Street View cars from collecting WiFi data entirely.

Maintaining people's trust is crucial to everything we do and, by mistakenly using code that collected payload data, we fell short. We are determined to learn all the lessons we can from our mistake.

Our answers to your questions, based on our investigation to date, are below:

1. What percentage of United States roads have been documented for Google Street View?

Google publishes a map of geographical locations where the Street View cars have driven and collected WiFi information. The map is updated periodically, typically every several months, and does not include those areas that are pending publication or that we have chosen not to publish. To view this data for the United States, please visit <http://maps.google.com/help/maps/streetview/where-is-street-view.html>. The driving locations (to the extent they have been published) are traced in blue on the map.

As you can see from the website, the Street View cars have driven most urban areas and major roads in the U.S. over the last three years. When we are able to get a reliable estimate of the percentage of U.S. roads documented by Street View, we will update you as soon as possible.

2. Over what time period did the collection of information for Google Street View take place or, if roads are visited by Google Street View vehicles more than once, what is the schedule for return visits to roads?

As noted above, the Street View product is separate from Google's WiFi data collection. The Street View product launched in 2007 and Google also began collecting WiFi data via Street View cars in the United States that same year. We are working to provide information regarding the frequency with which we drove, and will update you as soon as possible.

3. Have all Street View vehicles documenting United States roads been engaged in the monitoring or data collection of Wi-Fi transmissions at all times during those activities? If the answer is no, please explain in detail in what communities the monitoring or data collection was conducted and the reasons that these communities were chosen for monitoring or data collection.

The antennas were mounted on some of Google's Street View cars in the United States beginning in late 2007 and on all of Google's Street View cars in the United States by early 2008. While the WiFi antennas were installed on Street View cars, WiFi data was collected on the same schedule as Street View photographs. However, in May 2010, in light of concerns about the collection of payload data,

we stopped using Street View cars to collect any WiFi data at all. Again, we are working to provide more comprehensive information, and will update you as soon as possible.

4. How many Wi-Fi networks across the country have been logged since Google began its Street View program? How many consumers were subject to the data collection?

We have not identified a reliable method to determine the number of WiFi networks for which data has been collected. We will update you as soon as possible.

The WiFi network data collected, including SSID and MAC address, was not used to identify any specific individual or household. Moreover, we have not conducted an analysis of the payload data in a way that enables us to know exactly what was collected. We therefore cannot determine the number of individuals affected by the payload data collection.

5. Was any notification of this monitoring and data collection made to affected communities prior to deploying Street View vehicles, and was consent sought from consumers? If so, please explain the notice and consent procedures involved. If not, please explain why this was not done.

The fact that Google collects network information broadcast by WiFi routers to improve location-based services has been widely known -- it is described on Wikipedia (http://en.wikipedia.org/wiki/Google_Street_View) and has been featured in articles in the New York Times (<http://www.nytimes.com/2009/06/01/technology/start-ups/01locate.html>), among other sources. In addition, we have provided public descriptions of our location-based services -- e.g., My Location feature on Maps for mobile (<http://googlemobile.blogspot.com/2007/11/new-magical-blue-circle-on-your-map.html>), My Location on the desktop (<http://google-latlong.blogspot.com/2009/07/blue-circle-comes-to-your-desktop.html>), and the Gears Geolocation API (<http://googlecode.blogspot.com/2008/10/introducing-gears-geolocation-api-for.html>). Other companies also map wireless access points for use in commercial products or to help consumers find public Internet access (e.g., Skyhook Wireless, <http://www.skyhookwireless.com/howitworks/>). In retrospect, it is clear there should have been greater transparency about the collection of this data.

As Google only recently became aware of the collection of payload data and never used it in any product or service, we did not provide notice of this collection.

6. Has Google at any time conducted a legal analysis regarding the applicability of consumer privacy laws on the monitoring and data collection of Wi-Fi transmissions? If so, please provide a copy of that analysis.

Without disclosing confidential legal advice, we answer as follows:

As we have noted, neither Google's management nor any Google product group requested that the payload data be collected, and Google never used the payload data in any of its products or services.

As an initial matter, collection of network information broadcast by WiFi routers (such as SSID and MAC address) is used to improve location-based services and is a lawful, established business practice.

We believe it does not violate U.S. law to collect payload data from networks that are configured to be openly accessible (*i.e.*, not secured by encryption and thus accessible by any user's device). We emphasize that being lawful and being the right thing to do are two different things, and that collecting payload data was a mistake for which we are profoundly sorry.

7. Please explain in detail why Google chose to collect the data and how it intended to use the data.

Google collected and uses network information broadcast by WiFi routers (such as SSID and MAC address) to improve the accuracy of the location-based services, such as Google Maps or driving directions. For example, a user of Google Maps for mobile phones can turn on a smart phone's "My Location" feature to identify his or her approximate location based on GPS signals (where available) and signals from the cell towers and WiFi networks visible to the device. Because GPS and cell tower location data can be unreliable or inaccurate, in some cases using the location of WiFi access points can enable a smart phone to pinpoint its own location more quickly and accurately. Given the concerns raised, we have decided to stop our Street View cars from collecting WiFi data entirely, including SSID and MAC address data.

Collection of WiFi payload data was a mistake. The payload data has never been used in any Google product or service, nor do we intend to use it.

8. What is the status of the consumer data collected? Has it been analyzed and used in any way? Does Google have plans to use it in the future? Please explain in detail.

As we noted in Question 7, Google collected and uses network information broadcast by WiFi routers (such as SSID and MAC address) to improve the accuracy of the location-based services, such as Google Maps or driving directions. Given the concerns raised, we have decided to stop our Street View cars from collecting WiFi data entirely, including SSID and MAC address data.

With respect to payload data, it has never been used in any Google product or service, nor do we intend to use it. In fact, based on our current investigation, we are aware of only two instances when any Google engineer even viewed the payload data. The first instance involved the individual

engineer who designed the software. The second instance was when we became aware that payload data may have been collected from unencrypted WiFi networks and a single security engineer tested the data to verify that this was the case.

9. Has the collected data been destroyed? If yes, when and by which method(s)? If not, why not?

At the request of authorities in Ireland, Denmark, and Austria, we deleted payload data identified as coming from those countries. However, we have been retaining data collected in the United States, consistent with our obligations related to pending civil litigation matters.

10. What is the status of Google's internal review of Street View's monitoring and data collection practices to ensure adequate controls? What is the methodology? When did the review start? Who is conducting the review? Are there any interim findings? When is it expected to be completed? Will the review, or portions of it, be made available to the public?

As part of our investigation of this matter, we have had an independent technical services firm, Stroz Friedberg LLC, review the software at issue. The report confirmed that the software performed as we publicly disclosed in our May 14 blog post, storing only that information derived from wireless networks configured so as to be readily accessible to the general public and discarding any payload sent over encrypted networks. Moreover, the payload data was not parsed for use; instead, it was stored in raw, aggregate, binary form. We have just posted a copy of the completed report, and invite you to examine it (<http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>). We have also attached a copy for your reference.

We are also reviewing our procedures to ensure that our controls are sufficiently robust to address these kinds of problems in the future.

11. What is Google's process to ensure that data collection associated with new products and services offered by the company is adequately controlled?

We are reviewing our procedures to ensure that our controls are sufficiently robust to address these kinds of problems in the future. We are determined to learn all the lessons we can from our mistake.

12. Has Google asked a third party to review the software at issue? If so, who is the third party, and what is the nature of the review?

Yes. We have had an independent technical services firm, Stroz Friedberg LLC, review the software at issue. As we noted above, the report confirmed that the software performed as we publicly disclosed in our May 14 blog post, storing only that information derived from wireless networks

Letter to Chairman Waxman, Representative Barton, and Representative Markey

June 9, 2010

Page 7

configured so as to be readily accessible to the general public and discarding any payload sent over encrypted networks. Moreover, the payload data was not parsed for use; instead, it was stored in raw, aggregate, binary form. We have just posted a copy of the completed report (<http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>). We have also attached a copy for your reference.

* * *

We appreciate your engagement on this matter and would be happy to address any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read 'Pablo Chavez', written in a cursive style.

Pablo Chavez
Director of Public Policy
Google Inc.

Attachment