



Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
“Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy”

Questions for the record from Senator Blumenthal
Alan Davidson, Director of Public Policy, Google Inc.
June 8, 2011

Google appreciates the opportunity to respond to the Committee’s further questions arising from Google’s testimony concerning the steps it takes to protect mobile privacy with its Android operating system and in regard to the prior collection of publicly broadcast Wi-Fi information through Google’s Street View cars. Before responding to the questions, one point of clarification is necessary. Each question includes as a predicate the “interception” of wireless data transmissions between third party computers and wireless access points. As the Committee knows, the term “intercept” has legal meaning under Sections 2510 and 2511 of Title 18. Accordingly, as a general response, the answer to all of the questions is that Google does not engage in the unauthorized interception of the content of communications. Nonetheless, we provide this response in a good faith effort to provide the Committee with useful information about Google’s activities in regard to Wi-Fi.

- 1. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points for any purpose?**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise.

To the extent Senator Blumenthal’s questions follow up on the questions he raised at the hearing concerning the Wi-Fi payload data collected via Google’s Street View cars, Google has publicly explained what happened, including what information was collected and how, on our blog (<http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html> and <http://googlepublicpolicy.blogspot.com/2010/10/creating-stronger-privacy-controls.html>).

Further, the Committee has also expressed interest in the collection of location data by devices running the Android operating system. While also not involving any unauthorized interception of data transmissions between third party computers and wireless access points, Google, like many other companies, has developed systems for identifying wireless access points to provide better location-based services. Although a substantial amount of the information relating to these systems is non-public and proprietary, we have described how these systems work in our testimony.

If so:

- a. **Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from the interception of wireless data transmissions described above.**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise, whether in the United States or abroad. To the extent that the Committee has interest in Google’s other location-based services described in our testimony, Google operates location-based services in many countries around the world, including all states and territories of the United States.

- b. **Please indicate any and all purpose(s) underlying any such signal interceptions.**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise, whether in the United States or abroad, for any purpose. Like many other companies, Google does receive and collect information regarding wireless access points and other publicly broadcast geographic markers. The purpose of doing so is to offer location-based services.

- c. **Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. Location-based services have been an important part of Google’s research and development for many years. We do not have a timeline for each product or service, but can say in regard to the collection of publicly broadcast Wi-Fi information via Street View, Google first began its collection of such information for purposes of providing location based services in 2008 and discontinued the activity in May 2010.

- d. **Please describe any and all methods initially contemplated and/or implemented for these purposes.**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. With regard to Google’s collection of publicly broadcast Wi-Fi information via Street View vehicles, we direct you to the report prepared by independent technical services firm Stroz Friedberg LLC, which describes in detail the methods used and the type of information collected (the “Stroz Report”). See <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>. In regard to the

Android operating system, a substantial amount of the information relating to the system is non-public and proprietary, but we point the Committee to our testimony, which describes our practices and methods in that regard.

- e. **Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.**

See our response to Question 1(d).

- f. **Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc.). For each category of data, please define the term used to reference that category, including an indication of how it is derived.**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. The question also implies that Wi-Fi signaling information is susceptible to “interception.” Google understands the term interception to refer to the content of communications. Every Wi-Fi enabled radio publicly broadcasts, and every Wi-Fi enabled device receives, Wi-Fi frame transmissions in accordance with the 802.11 standard. Google’s ability to provide location-based services, like any company providing location-based services, depends upon receiving publicly broadcast Wi-Fi data such as MAC addresses, SSID, signal strength, time stamps, etc. A number of Google products and services include Wi-Fi enabled features. Information collected and how it is used may be found in Google’s Mobile Privacy Policy at <http://www.google.com/mobile/privacy.html> as well as product specific policies for Maps, Latitude, and our other location-based services.

- g. **Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. Google has no patents, patent applications, published works or other publicly available materials that describe the unauthorized interception of wireless communications traveling between third party computers and wireless access points. While not involving the unauthorized interception of the content of communications, to the extent the Committee is interested in the specific patent discussed the the hearing, we point the Committee to our answers to the supplemental questions for the record below.

- h. **Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of “content data”**

transmitted between third party users and wireless access points? If so, please explain how and why such content data is excluded from interception. If not, please explain how and why such content data is not excluded from interception. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

See response to 1.D. As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. With regard to Google's collection of publicly broadcast Wi-Fi information via Street View vehicles, we direct you to the report prepared by independent technical services firm Stroz Friedberg LLC, which describes in detail the methods used and the type of information collected (the "Stroz Report"). See <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>.

- i. Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized.** *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. As we have said before with respect the collection of publicly broadcast Wi-Fi information via Street View vehicles, Google did not use payload data in any product or service.

- j. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.**

No.

- k. Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?**

No.

- 2. Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.**

- a. **How many wireless access points exist, or have ever existed, in any database of wireless access point locations?**
 - i. **How many of these wireless access points were unencrypted when identified?**
 - ii. **How many of these wireless access points were encrypted when identified?**
 - iii. **How many of these wireless access points were “hidden” when identified?**

Location-based services depend in part on the ability to identify Wi-Fi access points. Such information is publicly broadcast in accordance with the 802.11 standard, involves no interception of wireless data communications, and therefore Questions 1.a-h are inapplicable. The total numbers of access points used for our location-based services is non-public, proprietary information, and Google does not publish a directory of such information.

3. Please describe any and all ways in which the interception and/or storage of “content data” transmitted between third party users and wireless access points might be:

- a. **Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and**
- b. **Indirectly valuable to your company for any other purpose.**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. To the extent the question contemplates the payload data collected by Google via its Street View vehicles, Google has not used the payload data collected by Street View vehicles in any product or service. That information has no use or value, directly or indirectly, to Google for any purpose, and never did.

4. Please describe your view of the circumstances under which the interception and/or storage of “content data” transmitted between third party users and wireless access points might be:

- a. **Legal or illegal under current federal law;**
- b. **Legal or illegal under current state law; and**
- c. **Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.** *Content data is defined as any data that may contain, in whole or in part, the content of a user’s internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

Google directs the Committee to Section 2511(2)(g) of Title 18, which states “[i]t shall not be unlawful . . . for any person (1) to intercept or access an electronic communication made

through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.” Wi-Fi transmissions broadcast from unencrypted networks are readily accessible to the general public by definition.

Most states follow federal law and any inconsistent state law would yield to federal law under the Supremacy Clause of the U.S. Constitution. Many foreign jurisdictions follow the same principles or their laws have not addressed the situation.

Supplemental Questions for the Record to Alan Davidson, Google, Inc.

Google appreciates the opportunity to respond to the Committee’s further requests and in particular to Senator Blumenthal’s followup questions below. First, several of the questions include as a predicate that patents exist for the purpose of “interception” of wireless data transmissions. As the Committee knows, the term “intercept” has legal meaning under Section 2510 and 2511 of Title 18. Accordingly, as a general response, the answer to all of the questions is that Google does not engage in the unauthorized interception of content of communications, and Google has no patents or applications pending that describe the “interception” of wireless communications traveling between third party computers and wireless access points. Also, the questions could be read to require the disclosure of non-public proprietary information. Nonetheless, in a good faith effort to answer the Committee’s questions, Google provides the following responses.

- 1. Please provide text and citations for any and all materials directly or indirectly associated with or related to the methods for intercepting wireless data transmissions traveling between third party computers and wireless access points described in U.S. Patent Application 2010/0020776, “Wireless Network-Based Location Approximation,” and WIPO Patent Application WO 2010/044872, “Wireless Network-Based Location Approximation” (including foreign or domestic patents, patent applications, published works, or other publicly available materials).**

As noted above, the term “intercept” has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. It has no patents or applications pending that describe the “interception” of wireless communications traveling between third party computers and wireless access points. The patent application referenced in the Question describes a method for approximating the location of a wireless device. The patent application is concerned with measuring the data rates of publicly broadcast Wi-Fi frames. The measurement of data rates does not involve the use of the content of any communications.

- 2. Please indicate where in the scheme described in U.S. Patent Application 2010/0020776, “Wireless Network-Based Location Approximation,” and WIPO Patent Application WO 2010/044872, “Wireless Network-Based Location Approximation” these patents explicitly exclude the interception of content data.** *Content data is defined as any data that may contain, in whole or in part, the content of a user’s internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

See Response to Question 1, which is incorporated herein. Content data is irrelevant to the patent process described in the application and has nothing whatsoever to do with

establishing confidence in the location of an access point, and therefore there is no reason to disclaim it.

3. **Wireless signal interception as described in Paragraph 51 of U.S. Patent Application 2010/0020776, “Wireless Network-Based Location Approximation,” and Paragraph 47 of WIPO Patent Application WO 2010/044872, “Wireless Network-Based Location Approximation” involves configuring a Google computer “to observe or capture data packets .. transmitted to or from” a wireless access point, with the Google computer “operat[ing] in a ‘sniffer’ or ‘monitor’ mode, thereby handling transmitted frames ... without requiring” the Google computer “to be associated with” the wireless access point. This scheme appears to contemplate ‘sniffing’ (i.e., intercepting and decoding) all transmitted frames.**
- a. **Where does this patent distinguish between ‘sniffing’ or ‘monitoring’ frames containing content data and ‘sniffing’ or monitoring frames that did not contain content data?** *Content data is defined as any data that may contain, in whole or in part, the content of a user’s internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

See Response to Questions 1 and 2. Every Wi-Fi enabled radio publicly broadcasts, and every Wi-Fi enabled device receives, Wi-Fi frame transmissions in accordance with the 802.11 standard. Google’s ability to provide location-based services, like any company providing location-based services, depends upon receiving publicly broadcast Wi-Fi data such as MAC addresses, SSID, signal strength, time stamps, etc. Content data is irrelevant to the patent process described in the application and has nothing whatsoever to do with establishing confidence in the location of an access point.

- b. **Was there ever a version of Google’s Street View programming designed to intercept and decode all of the information received from a wireless access point and then subsequently discard unwanted data?**

No. We direct you to the report prepared by an independent technical services firm, Stroz Friedberg LLC, which describes in detail the describes in detail how the Wi-Fi equipment and software operated, the frequencies and protocols covered, and type of information collected (“the Stroz Friedberg Report”). See <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>. As noted in the Stroz Friedberg Report, the software was designed to recognize encrypted networks and never to store payload data from those networks.

- c. **Was there ever a version of Google’s Street View programming that distinguished between frames containing content data and frames that did not contain content data?** *Content data is defined as any data that may contain, in whole or in part, the content of a user’s internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

No.

- d. **Was there ever a version of the software on Google’s Street View cars that specifically deleted, blanked, or removed intercepted IP payload data?**

No.

- e. **Did the software addition that Google points to as responsible for collecting “payload data” affirmatively intercept and decode content, or did it remove a preexisting block on decoding content?**

No, the software did not decode content at all. See the Stroz Friedberg Report referenced above for information on how the software operated.

4. **Does the term "data rate" as used in these patent applications consistently refer to information about the communication with the access point such as "data rate" as defined by 802.11 standards, or does it refer to a “measured” data rate?**

The "data rate" is a property of the transmission, as defined by 802.11 standards.

5. **Paragraphs 70-71 of U.S. Patent Application 2010/0020776, “Wireless Network-Based Location Approximation,” and Paragraphs 66-67 of WIPO Patent Application WO 2010/044872, “Wireless Network-Based Location Approximation,” discuss ‘evaluating different types of frames sent to (or received from) the device of interest’ including “management frames, control frames, data frames, etc.” as part of a scheme to estimate “the confidence of the location” of a wireless access point.**

- a. **Please explain what types of evaluations are contemplated for each of the three types of frames listed.**

Each of the frames types are sent at specific data rates. The receiving device driver obtains and appends the data rate to each frame that was sent to, or received from, an access point. The data rate is extracted from the various frames for evaluation by means of a mechanical, automated process.

- b. **How does evaluation of data frames contemplated in these paragraphs affect Google’s estimate of the confidence of the location of a wireless access point?**

As described in the patent application, it is assumed that data rate, like signal strength, can be used to estimate "distance." Thus, given the expected location of an access point and the GPS location of where a frame is captured plus the data rate, Google could determine how probable it is to receive a frame at the given data rate and at a given distance from the access point to the location where the frame was captured.

Data frames are sent at different data rates (unlike management/control frames which are sent at fixed data rates). For example, the higher the data rate, the shorter the distance at which it can be received. These assumptions could help build or reduce confidence in an access point’s estimated location.

6. **Paragraphs 74-75 of U.S. Patent Application 2010/0020776, “Wireless Network-Based Location Approximation,” and Paragraphs 70-71 of WIPO Patent Application WO 2010/044872, “Wireless Network-Based Location Approximation,” discuss determining “the confidence in the location” of a wireless access point, and note that “the types of frames that are used in the**

measurement, such as data frames, management frames, and/or control frames may affect the confidence.”

- a. How do these patents contemplate evaluating these three types of frames in order to improve the confidence estimate for the location of the wireless access point?

See Response to Question 5(b).

- b. How does evaluation of data frames contemplated in these paragraphs affect Google’s estimate of the confidence of the location of a wireless access point?

See Response to Question 5(b).

7. Paragraph 82 of U.S. Patent Application 2010/0020776, “Wireless Network-Based Location Approximation,” and Paragraph 78 of WIPO Patent Application WO 2010/044872, “Wireless Network-Based Location Approximation,” discusses how “[T]he location of a given [wireless access point] may be based on a number of measurements taken by one or more client devices. The raw data collected by a client device may be processed locally or sent to a central repository ... for processing” (emphasis added).

- a. Do these patent applications specifically exclude the collection of raw data that includes “content data” before sending it to a central repository for processing? *Content data is defined as any data that may contain, in whole or in part, the content of a user’s internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

The sentence cited in the Question simply states the proposition that the publicly broadcast Wi-Fi frames received may be processed locally or in storage. The patent application is concerned with measuring the data rates of publicly broadcast Wi-Fi frames. Content data is irrelevant to the patent process described in the application and has nothing whatsoever to do with establishing confidence in the location of an access point. Thus, where the frames are processed is irrelevant as well.

- b. Is there any relation between the scheme described in Paragraph 82 and the operation of the Google Street View cars during the period when those cars were used to identify the locations of wireless access points?

The quotation from Paragraph 82 referenced in the question simply states that data may be analyzed locally or later in a central data store. The same is true for any data collection and analysis. In the case of Wi-Fi data collected via Street View vehicles, the data was stored in Google’s File Servers.