

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

June 1, 2011

United States Senate
Committee on the Judiciary
Chairman Patrick Leahy
ATTN: Julia Gagne
Hearing Clerk, Dirksen Office Building
Washington, DC 20510
Julia_Gagne@judiciary-dem.senate.gov

Re: Hearing on “Protecting Mobile Privacy: Your Smartphones, Tablets,
Cell Phones, and Your Privacy”

Dear Chairman Leahy:

I am writing to respond to the written Questions For the Record submitted by Senator Blumenthal regarding Google’s interception of WiFi signals in order to build out its geolocation services database.

I appreciate the opportunity to respond to further questions arising from the hearing. Some of the Senator’s questions go beyond my own personal level of technical knowledge, and I have obtained assistance from my more technical colleagues at CDT to develop my answers below. Before directly addressing the specific questions — which generally concern two patents obtained by Google regarding network-based location approximation — let me offer one caveat and one broad observation.

First, both from a legal and an engineering perspective, the task of interpreting the precise meaning of language in a patent is one best suited to those with specialized training in patent law, which neither I nor my colleagues at CDT have. We are sufficiently familiar with patent disputes, however, to know that many patents contain elements and assertions that are both expansive and defensive in nature, and may not in fact ever be included in an actual functioning implementation of the patented technology. We cannot speak to what elements of the patents at issue here have been implemented by Google or any other company.

Second, in considering the patents in question, it is important to recognize that from our analysis, the patents in question are focused almost exclusively at what are termed “layers 1 and 2” of the multi-layered technical architecture on which all Internet communications are based, while almost all true “user content”



such as the content of e-mails or web-browsing sessions is transmitted at “layer 7” of the architecture. This can introduce significant confusion in that certain terms can refer to different things at different layers of the architecture, and the meaning of certain terms may depend heavily on the layer to which the term is referring.

To try to illustrate the overlapping nature of the layered architectural model, below is a simplified diagram that shows some (but not all) of the layers that might be implicated by the questions. What this diagram tries to illustrate is that in the layered model, the “payload” of some packets (which at layers 1 and 2 are sometimes called frames) will contain entire whole packets of information from a lower level protocol. Thus, as illustrated below, when sending an e-mail, the true “user content” of the e-mail (with the to/from routing information and the e-mail content) will be found in a layer 7 SMTP packet, which is entirely contained within a layer 3 “Internet Protocol” packet (which uses IP addresses for routing). And the IP packet is entirely contained in a layer 1 and 2 802.11 frame (which uses MAC addresses for routing):

802.11 Frame (layers 1 and 2)			
Routing and address info	MAC Address		
Other fields	“Data rate,” among others		
Content payload	Internet Protocol Packet (layer 3)		
	Routing and address info	IP Address	
	Content payload	SMTP (e-mail) Packet (layer 7)	
		Routing and address info	joe@example.com
		Content payload	E-mail content

This illustration may be helpful in understanding the patents at issue in the questions below and the ambiguity around the term “content” as regards the Google patents and WiFi interception issue.

QUESTIONS:

1. In your view, is there anything the wireless access point location approximation scheme described in 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,” that explicitly excludes the

collection of “content data” transmitted between third party users 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.*

We are interpreting the terms “content data” and “content of a user’s internet communications over a wireless network” to refer to what I have called “user content” transmitted at layer 7 of the Internet architecture, meaning (in an e-mail example) the to/from e-mail addresses and e-mail text and attachments, or (in a web browsing example) the web address or URL and the web page content. With this understanding, our review of the patents at issue indicates that the patents are silent on the treatment or analysis of user content. The patents do not explicitly exclude the collection of user content, but at the same time the patents do not make any mention at all of user content (and the patents do not indicate any intention to analyze user content in order to determine location).

In the event that your definition of “content data” is intended to incorporate routing and addressing information that is contained in 802.11x frames (and higher layer routing and addressing information such as MAC addresses, SSIDs, and IP addresses), then the patents do seem to envision the collection and analysis of such routing information.

2. These patent applications contemplate examining “data frames” to determine the location of wireless access points as contemplated in these patent applications, looking at “the data in the frame ... itself” to determine the data rates of frames that might contain content data, and contemplate sending “raw data collected” back to “a central repository ... for processing.” If Google actually engaged in any of these practices, would it be accurate to describe Google’s interception and/or storage of content data through its Street View program as unintentional? *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.*

We do not interpret the patents to contemplate “examining” any user content to make any determination of location, but instead to examine headers and data fields (such as the “data rate,” which is a field found in some 802.11x frames) and use those non-content bits of information to calculate location. Our reading of the specific language quoted from paragraph 52 of the U.S. patent is that (a) it most likely refers to management or control frames, not data frames, but that (b) in any event, the information sought by looking at “data in the frame” would be found in lower-level header fields like “data rate” (and not in user content such as e-mails or web browsing sessions).

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 for any other purpose.

As noted more fully in response to Question 1, we interpret the terms “content data” and “contents of a user’s internet communications over a wireless network” to refer to what I have called “user content” transmitted at layer 7 of the Internet architecture. With this understanding, then, we are unaware of any value, direct or indirect, that user content would have in efficiently locating wireless access points using commercially available methods. The user content of course has value to the end users (for example, the sender and recipient of an e-mail), but even if (for example) an e-mail contains a street address, a service provider seeking to locate access points would have no way of knowing whether the address related to the location of the access point in use.

In the event that the term “content data” is intended to incorporate routing and addressing information that is contained in both 802.11x frames and higher layers, such as MAC addresses, SSIDs, and IP addresses, then such routing and addressing information could be used to calculate approximate locations of access points, using methods suggested in the patents.

- 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; or
 - b. Legal or illegal under current state law.

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 legality under federal law of the reception by a device of wireless signals is a very complex technical and legal question turning on, among other things, the interpretation of provisions such as 18 U.S.C. § 2510(16), which define the category of radio communications which are “readily accessible to the general public,” access to which is not a violation of federal law. This is one of the more confusing sections in the U.S. Code, and we are aware of no cases that apply these provisions to modern WiFi technologies.

Section 2510(16)(A) says that encrypted connections are not accessible to the public and thus protects encrypted wireless communications. Section 2510(16)(C) protects public communication over certain types of subcarriers — signals carrying information as part of or associated with a larger signal. This provision may arguably protect certain WiFi technologies carried on subcarriers (802.11a, g, and n); on the other hand, because the subcarriers used

to transmit that information were not envisioned when the statute was written, they may be construed to fall outside the specific set covered by the statute as interpreted through FCC rulemaking. Section 2510(16)(E) also affords protections for public communications over certain frequencies, which seems to cover WiFi transmissions made on some common channels, but not others.

State law is more varied, and thus even more difficult to interpret with certainty.

Hopefully, this brief overview demonstrates that the status of the interception of personal wireless devices under the law is not at all clear, and the legality of a given interception can turn on specific technical questions regarding the choices made by the operators of individual WiFi hotspots, as well as the technical options in use by the WiFi equipment in question.

Separately, it is important note that for *any* wireless system to work, all devices seeking to communicate on a given frequency (whether or not those devices are the intended recipient of a communication) must in a sense “listen” to at least a portion of all communications on the frequency in order to determine whether the communication is intended for the particular device. Before interpreting certain kinds of routing and signaling information contained within a given communication, there is no way for a receiver to understand that a given packet is aimed elsewhere. Thus, to the extent that the term “content data” is intended to incorporate routing information that is contained in 802.11x frames (such as MAC addresses), devices must as a technical matter be permitted to receive such information in order for the wireless system to function.

The uncertainty of the law's application in this context is yet another illustration of why the Electronic Communications Privacy Act (ECPA) and other surveillance laws need to be updated to provide clear protection to electronic communications technologies and services that have evolved substantially in recent years. CDT is a member of the Digital Due Process coalition, which has offered a few narrow recommendations for updating ECPA.

* * *

We hope that our answers have been helpful. We appreciate the opportunity to further discuss the issues raised in the hearing, and we look forward to working with the Committee on these important issues.

Sincerely,

/s/

Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology