


CNET News

[CNET News](#)

- sign in with 
- log in
- join CNET

- [Home](#)
- [Reviews](#)
- [You are here: News](#)
- [Downloads](#)
- [Video](#)
- [How To](#)

- [Latest News](#)
- [CNET River](#)
- [Latest News](#)
- [Webware](#)
- [Crave](#)
- [Business Tech](#)
- [Green Tech](#)
- [Wireless](#)
- [Security](#)
- [Blogs](#)
- [Video](#)
- [Photos](#)
- [More Menu](#)

[Privacy Inc.](#)

Ad Info ▼

JUNE 15, 2011 4:00 AM PDT

Exclusive: Google's Web mapping can track your phone

by [Declan McCullagh](#)

Recommend

853

439

14



Nick Doty's computer was listed by Google as being located at his previous home address in Seattle.

(Credit: Declan McCullagh/CNET)

SAN FRANCISCO--If you have Wi-Fi turned on, the previous whereabouts of your computer or mobile device may be visible on the Web for anyone to see.

Google publishes the estimated location of millions of iPhones, laptops, and other devices with Wi-Fi connections, a practice that represents the latest twist in a [series of revelations](#) this year about wireless devices and privacy, CNET has learned.

[Android phones](#) with location services enabled regularly [beam the unique hardware IDs](#) of nearby Wi-Fi devices back to Google, a similar practice followed by Microsoft, Apple, and Skyhook Wireless as part of each company's effort to map the street addresses of access points and routers around the globe. That benefits users by helping their mobile devices determine locations faster than they could with GPS alone.

Only Google and Skyhook Wireless, however, make their location databases linking hardware IDs to street addresses publicly available on the Internet, which raises novel privacy concerns when the IDs they're tracking are mobile. If someone knows your hardware ID, he may be able to find a physical address that the companies associate with you--even if you never intended it to become public.

Tests performed over the last week by CNET and security researcher [Ashkan Soltani](#) showed that approximately 10 percent of laptops and mobile phones using Wi-Fi appear to be listed by Google as corresponding to street addresses. Skyhook Wireless' list of matches appears to be closer to 5 percent.

"I was surprised to see such precise data on where my laptop--and I--used to live," says [Nick Doty](#), a lecturer at the University of California at Berkeley who co-teaches the Technology and Policy Lab. Entering Doty's unique hardware ID into Google's database returns his former home in the Capitol Hill neighborhood in Seattle.

Here's how it works: Wi-Fi-enabled devices, including PCs, iPhones, iPads, and Android phones, transmit a unique hardware identifier, called a [MAC address](#), to anyone within a radius of approximately 100 to 200 feet. If someone captures or already knows that unique address, Google and Skyhook's services can reveal a previous location where that device was located, a practice that can reveal personal information including home or work addresses or even the addresses of restaurants frequented.

A Google spokesman would not answer whether Android phones or Street View [cars](#) have collected the MAC addresses of phones or computers *not* acting as Wi-Fi access points--a practice that, if true, would pose a greater privacy risk. Skyhook Wireless CEO Ted Morgan says that his company only collects access point addresses. Doty says that his computer may have been used as an access point for testing, but "I certainly didn't do so commonly."

[Alissa Cooper](#), chief computer scientist at the [Center for Democracy and Technology](#) and co-chair of an Internet Engineering Task Force on geolocation, says that her laptop was never used as a Wi-Fi access point. Her previous street address off of Connecticut



A wireless MAC address from a coffeeshop in San Francisco's Mission district was also spotted here. (Click for full-sized image.)

Avenue in Washington, D.C., where she lived from 2007 to 2009, nevertheless shows up in Google's location database.

Over the course of a minute in a coffeehouse in San Francisco's Mission district, the unique MAC addresses of 76 computers using Wi-Fi connections were visible. Seven appeared in Google's database with corresponding street locations, and three appeared in Skyhook's. (A test of 257 devices accessing a public Wi-Fi connection in San Francisco's South of Market neighborhood also found that Google displayed locations corresponding to about 10 percent of the devices.)

Alas for enterprising snoops, it's not always trivial to learn a target's MAC address. It's generally not transmitted over the Internet. But anyone within Wi-Fi range can record it, and it's easy to narrow down which MAC addresses correspond to which manufacturer. Someone, such as a suspicious spouse, who can navigate to the About screen on an iPhone can obtain it that way too.

The locations corresponding to the MAC addresses visible in San Francisco were all over the map. An Apple device visible in the coffeehouse had a street address of Grouse Lane in Woodbridge, Conn., meaning it was previously recorded as being present there. Another was listed as being a few miles away, near 170 New Montgomery St. A third was spotted in Los Altos, Calif., and a fourth in Berlin.

The MAC addresses of computers used by two CNET reporters appeared in Google's location database as located in the CNET newsroom on Second Street in San Francisco. Soltani said a friend's iPhone is listed as appearing at a Belgian french fry restaurant that he last visited in May.

Google's location database also can be used, in a few cases, to track movements. One HTC device connecting to the South of Market Wi-Fi hot spot on Wednesday moved from the BWI airport last Friday afternoon to a street address in an Atlanta suburb that evening. One from the coffeehouse moved from the engineering building of Ruhr-University in Bochum, Germany, across the main road to the university center. It's unclear, however, how frequently the database is updated, and the locations for those two devices have not changed again since last week.

Companies respond

In a statement, Google said: "We collect the publicly broadcast MAC addresses of Wi-Fi access points. If a user has enabled wireless tethering on a mobile device, that device becomes a Wi-Fi access point, so the MAC address of such an access point may also be included in the database. Wi-Fi access points that move frequently are not useful for our location database, and we take various steps to try to discard them."

Google did not respond to a series of questions posed last week, including what measures it takes to filter out mobile devices and laptops

"Someone who doesn't have a lot of information about me can track me down. You can find where someone lived previously and where someone moved to."

--Ashkan Soltani, security researcher

from its database, what privacy policy governs this data collection, and whether law enforcement or civil litigants submitted requests for records from its database. The company also declined to specify how someone can remove their device's MAC address from the database, and a [question](#) asking that in a support forum last September was never answered.

Android devices appear to take one privacy-protective step that Apple iPhones do not: they randomize their MAC address when acting as hot spots, using a range of addresses that are marked as unassigned.

Mike Shean, co-founder of Skyhook Wireless, which [filed a patent infringement lawsuit against Google over its mapping technology](#) last year, says if a MAC address is an access point, whether it's an iPhone or a Linksys router, "we would collect it."

Shean says, however, that his company tries to filter out mobile devices because they aren't useful in providing location fixes. "Do we see access points in several places? Are they mobile?" he said. "If so, we'd rank that access point in a way that marked it as mobile, and reduced our level of confidence in using it in our system."

To be sure, it's not entirely surprising that the whereabouts of devices acting as Wi-Fi hot spots are swept up in these ambitious efforts to map the planet's access points (which can also let desktop computers without GPS functionality learn their locations). More and more phones offer tethering, which [came to the iPhone last year](#), and 4G hot spots are becoming more common.

One way to filter out mobile MAC addresses would be to [compare them](#) against a list of manufacturers. If it's an HTC-issued address, and HTC doesn't make fixed wireless access points, that could be discarded. Linksys devices, on the other hand, are probably more likely to remain in one place.

A test of Skyhook's location database showed that as long as the queries were performed from the San Francisco Bay Area, the company's servers responded with geolocation fixes for the MAC addresses. One returned an address of 791 Valencia St. (the coffeehouse is at 780 Valencia St.). Another [returned](#) an address along San Francisco's Embarcadero near AT&T Park.

But when the queries were performed from Washington, D.C., less than 24 hours later, the company's servers responded with the error: "Unable to determine location." That's apparently because Skyhook's servers concluded the MAC address had shifted to the East Coast and therefore was a mobile device that should be removed from their database.

"Someone who doesn't have a lot of information about me can track me down," says Soltani, the security researcher who [testified](#)



Security researcher Ashkan Soltani says a big problem is no opt-out method.

(Credit: Declan McCullagh/CNET)

[before the U.S. Senate last month](#). "You can find where someone lived previously and where someone moved to."

While Google and Skyhook have long offered ways for programmers to send queries to their database, Web interfaces have increased their visibility. Hobbyist hacker [Samy Kamkar](#) created [a Web page](#) in April that allows MAC address locations to be displayed without writing code. [Another](#) works with Skyhook.

"We do not offer a Web API as a product or service," Morgan, Skyhook's chief executive, said yesterday. "What you have seen is a hack of our protocol and a violation of our license agreement." Skyhook does, however, offer [free C++ source code](#) that does the same thing.

The real problem, says Soltani, the security researcher, is that there's "zero transparency" about how this crowdsourced data collection works and how people can opt out of it. "We carry these devices with us all the time, and they closely map to our whereabouts."

Disclosure: McCullagh is married to a Google employee not involved in this topic.

[**Editor's Note:** We're trying to learn more about how the physical locations of device MAC addresses are recorded and updated. Please help! You can do that by [sending us e-mail](#) with your wireless MAC address, what city you live in, and what type of device it is. Here's how to find your wireless MAC address under [Windows, OS X](#), and [Android](#). On an iPhone, tap on Settings->General->About. Thank you!]

Recommend 853

439

Share 125



Declan McCullagh

[E-mail Declan McCullagh](#)

Like 449

[Declan McCullagh](#) is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

- [Reviews](#)
- [All Reviews](#)
- [Camcorders](#)
- [Car Tech](#)

- [Cell Phones](#)
- [Digital Cameras](#)
- [GPS](#)
- [Laptops](#)
- [TVs](#)

- News
- [All News](#)
- [Business Tech](#)
- [Crave](#)
- [Cutting Edge](#)
- [Green Tech](#)
- [Security](#)
- [Wireless](#)

- Downloads
- [Add Your Software](#)
- [All Downloads](#)
- [Mac](#)
- [Mobile](#)
- [Software Deals](#)
- [Webware](#)
- [Windows](#)

- Video
- [All Videos](#)
- [Apple Byte](#)
- [Buzz Report](#)
- [CNET Top 5](#)
- [Loaded](#)
- [Prizefight](#)

- More
- [About CBS Interactive](#)
- [About CNET](#)
- [CNET Deals](#)
- [CNET Forums](#)
- [CNET Mobile](#)
- [CNET Site Map](#)
- [CNET Widgets](#)
- [Corrections](#)

- [Help Center](#)
- [Newsletters](#)
- [Permissions](#)
- [RSS](#)

- Join us on
- [Facebook](#)
- [LinkedIn](#)
- [Twitter](#)
- [YouTube](#)

POPULAR TOPICS:

- [Apple iPhone,](#)
- [Apple iPod,](#)
- [LCD TV,](#)
- [Apple iPad,](#)
- [Smartphones,](#)
- [Windows 7,](#)
- [CES 2011,](#)
- [Google Android,](#)
- [HTC phones,](#)
- [Android phones](#)

- [© 2011 CBS Interactive. All rights reserved.](#)
- [Privacy Policy](#)
- [Ad Choice](#)
- [Terms of Use](#)
- [Mobile User Agreement](#)
- Visit other CBS Interactive sites: