

## Privacy in Peril: Lawyers, Nations Clamor for Google Wi-Fi Data

By [David Kravets](#) June 11, 2010 | 2:18 pm |

<http://www.wired.com/threatlevel/2010/06/privacy-in-peril/#ixzz0qZYNuCpm>

A hard drive with perhaps several hundred gigabytes of internet surfers' private data resides under lock and key in a Portland, Oregon, federal courthouse.

Regulators and private lawyers across Europe and the United States are demanding, and in some cases obtaining, access to data that Google sniffed for the past three years from unsecured Wi-Fi hot spots across the globe.

The requests are coming in some of the eight proposed class actions targeting Google that have cropped up across the United States, as well as from various governments investigating whether Google violated their laws.

The demands for data raise a paradox of sorts: How many eyeballs, in the name of privacy, will eventually see the data that likely includes snippets of e-mail, web surfing, documents and other private data?

“It will be relevant evidence in our lawsuit. We will ask for production of that data. Lawyers representing plaintiffs in the case will review the data,” said Patrick Keyes, a top lawyer in one of the proposed class actions lodged in the District of Columbia. “This would be in the context of presenting the legal interests of those who have had their data intercepted, and would typically be produced under a protective order.”

Google has already said it would forward to German, French and Spanish authorities the portion of the data intercepted in those countries.

No government agency in the United States has yet demanded a copy of the intercepted data, but several are investigating Google.

Missouri Attorney General Chris Koster said he wanted to “[scrutinize this situation](#)” while Connecticut Attorney General Richard Blumenthal has demanded “[detailed records on any information taken from networks](#)” from his state.

Federal Trade Commission Chairman Jon Leibowitz told Congress, “We’re going to take a very, very close look at this.”

Rep. Joe Barton (R-Texas) said Friday that Google’s actions “warrants a hearing, at minimum.”

Ironically, it appears that protecting privacy and administering justice might just involve violating privacy.

“That’s true. All of this raises a lot of First Amendment questions,” said Jeffrey Chester, director of the Center for Digital Democracy. “It is problematic. Some of these lawyers see a quick buck without thinking of the consequences.”

U.S. District Judge Michael Mosman in Oregon [has locked away the data](#) (.pdf) as that class action proceeds. ISec Partners, a San Francisco security consulting firm, has made encrypted copies of the drives at Google's request and destroyed the originals.

"The encryption keys for these drives are possessed by only myself and one other person. and the hard drives are securely stored in a safe controlled by [Google's physical security team](#)," (.pdf) Alexander Stamos, one of iSec's founding partners, told the Oregon judge in a court filing before the data was forwarded to the Portland courthouse.

But Aaron Zigler, a lawyer in the Illinois class action, said, "I don't want to see the actual data that has been intercepted."

Class members of the lawsuits can be determined without actually reading the contents of the payload data packets, he said. "There is enough data to figure out who everyone is: date, time and location, and unique MAC addresses of the Wi-Fi network they intercepted," he said.

Pablo Chavez, director of public policy for Google, said in a letter to Congress released Friday that Google is "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](#)," (.pdf) he wrote. "The second instance was when we became aware that payload data may have been collected from unencrypted Wi-Fi networks, and a single security engineer tested the data to verify that this was the case."

Google has repeatedly said it is working with the relevant government investigators, and is demanding that all the litigation be consolidated in California, where it's headquartered.

The Mountain View internet giant maintains the collection of data while taking photos for its Street View program was inadvertent -- the result of a programming error with code written for an early experimental project that wound up in the [Street View code](#) (.pdf), an explanation some of the [lawyers suing Google have disputed](#).

Google said it didn't realize it was sniffing packets of data on unsecured Wi-Fi networks in dozens of countries for the last three years, until German privacy authorities questioned what data Google's Street View cameras were collecting. Street View is part of Google Maps and Google Earth, and provides panoramic pictures of streets and their surroundings across the globe.

And Google said no U.S. wiretapping laws were breached because the Wi-Fi signals were "[readily accessible to the general public](#)" (.pdf).

At least insofar as the proposed class actions were concerned, Jennifer Granick, a civil liberties attorney with the Electronic Frontier Foundation, suggested having a judge or a so-called "special master" sift through the data to determine whose data Google obtained. That should only happen if Google is found to have [done something unlawful](#), she said.

"This raises my eyebrows," she said. "I don't think we need to know what any of this data is yet, because there's nothing to suggest Google did this intentionally."