



July 7, 2010

The Honorable Jane Harman
United States House of Representatives
2400 Rayburn House Office Building
Washington, D.C. 20515-0536

Dear Rep. Harman:

We write to warn you that with commonplace technologies, the Internet and email activity at the homes of Members of Congress can easily be spied upon. We are sure of this because Google recently admitted it has collected large quantities of internet data from houses all over the United States. One of these houses may have been yours. We know this because we recently performed a simulation of Google's operation and sent "packet sniffers" to the neighborhoods of several Members. In several locations we found unencrypted networks, including at least one that we are certain belongs to your residence in Washington, DC. Of course, we did not track or download any information other than basic information about the networks, but we can't say the same about Google.

Attached and available on our InsideGoogle.org web site are pictures of your residence taken by Google Street View cars. We know now that Google not only took pictures of your home, the company also attempted to record your wireless Internet data. We call on the House Energy and Commerce Committee to investigate and hold hearings on these privacy invasions by Google.

Recently Google admitted its Street View cars were not just taking photographs, but snooping on private WiFi networks over the last three years as they prowled streets in thirty countries around the world. This week we duplicated Google's method of locating networks, but unlike Google, we scrupulously avoided recording "payload data." We found that some members may have open WiFi networks that Google likely spied on.

Never asking permission, Google is amassing unprecedented amounts of data about individuals so it can target us for personalized advertising. Consumers are tracked not just on the Internet, but in their very own homes. As far as Google is concerned, an individual's home is not his castle, but a gold mine of personal data that can be sold to advertisers at a hefty premium.

Google's practice directly affects you. Enclosed please find information about your residence. We gathered the data from public records and found the photographs of your residence from Google Maps and its Street View option. Your home is on display for the entire Internet with just a few clicks of a computer mouse. A Street View picture of your home means Google also tried to tap into your personal WiFi networks, likely in violation of federal wire tapping laws. If your wireless system was unencrypted, Google may have recorded your electronic communications with your colleagues, staff, families and friends. Potential state secrets remain in the custody of Google's servers.

In addition, as mentioned above, our own limited investigation confirmed that the home networks of some senior members of your committee whose houses appear on Street View are indeed vulnerable to the type of signal sensing equipment used by Google. This leaves little question that Google is currently in possession of sensitive data from the information networks used by members of Congress in their residences.

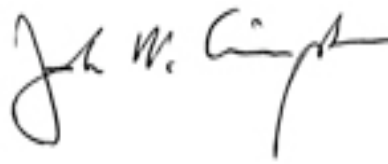
Because of your position, we believe this is not just an invasion of privacy but an unwarranted intrusion by Google into legislative branch matters. In our view, you have the right to demand that Google disclose to you any information it has collected regarding your home wireless networks.

In addition we urge the Energy and Commerce Committee to, at its earliest convenience, hold a hearing on Google's WiSpying and data gathering practices.

Sincerely,

A handwritten signature in cursive script, appearing to read "Jamie Court".

Jamie Court
Consumer Advocate

A handwritten signature in cursive script, appearing to read "John M. Simpson".

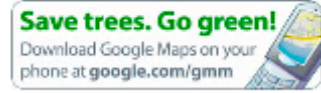
John M. Simpson

Jane Harman, CA

Property

Google Screenshot for Washington DC:

Google maps



<http://maps.google.com/maps?f=q&so...>

1/1

Network Analysis

Jane Harman, CA The following networks were detected. It is obvious that the two networks listed belong to the Congresswoman and neither one network is utilizing the available security mechanisms built into the wireless access point. It would be a simple matter of setting and collecting the packets and then reconstructing any unencrypted documents, email or transmitted files.

Networks Detected at the Harman Residence						
#	BSSID	SSID	Pkts	Encryption	Clients	
1	00:1E:E5:A1:4D:42	harmanmbr	6	None	Client 1	00:1E:E5:A1:4D:42
2	00:23:69:78:65:AF	harmantheater	123	None	Client 1	00:18:3A:37:B9:0A
					Client 2	00:23:69:78:65:AF
					Client 3	00:26:24:16:4C:D0
					Client 4	00:26:82:4B:87:6F