

RICHARD BLUMENTHAL
ATTORNEY GENERAL



55 Elm Street
P.O. Box 120
Hartford, CT 06141-0120

Office of The Attorney General
State of Connecticut

July 21, 2010

SEND VIA EMAIL: swexler@google.com

Stacey Wexler, Esquire
Senior Counsel
Google, Inc.
600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Attorney Wexler:

This letter is being sent to you on behalf of the Executive Committee (the "EC") of the Multistate Working Group that is presently investigating Google's interception of wireless network transmissions by way of its Street View cars. As part of its work investigating this significant privacy issue, the EC has reviewed Google's responses to letters of the member states and has developed a list of follow-up questions.

We would like Google to answer the below questions by July 23, 2010.

1. Did Google, through use of Kismet or any other code or software in the Street View cars, ever listen to any channel for more than 0.2 seconds?
2. Was any information ever recorded by Google Street View cars, whether ultimately written to disk or deleted, from any single channel for more than 0.2 seconds?
3. Was Kismet or any other code or software in the Street View cars designed, or did it operate, in any way to allow transmissions over wireless networks to complete/finish/terminate before hopping to the next channel?
4. Did Google test the Street View software before its launch to determine what, if any, consumer data (whether payload data or otherwise) would be collected? Please provide all correspondence and documentation relating to any such testing.
5. Please explain how, after testing the Street View software, Google was unaware that code in the software was able to collect payload data from unencrypted WiFi networks.

6. Does Google have a process for reviewing new code before it is implemented/deployed? What is that process? Was that process followed for the Street View software? Please provide all documentation relating to Google's code review process in general, and for Street View in particular.
7. Please identify each state in which network content was collected by Google Street View software.
8. What policies does Google have with respect to employees putting unauthorized code in software and what disciplinary measures, if any, are in place if unauthorized code is included in software?
9. Who inserted the "unauthorized" or "experimental" code into the Street View program?
10. Has/have the person(s) identified in your response to Question 9 above been asked to provide an explanation for why the code was inserted? What was the explanation?
11. Was any of the data that Google collected via its Street View cars, other than the actual photographs, disclosed to third parties or used for marketing purposes? If so, please explain in detail.
12. Were the photographs taken by the Google Street View cars stamped with date, time and any GPS or other location information? If so, please explain in detail why Google cannot more easily determine the towns and cities in which wireless network data was collected.
13. Did Google request, command or have any knowledge that the person(s) identified in response to Question 9 created, inserted and employed code that would detect, capture, and record unencrypted payload data?

Google's prompt and forthright responses to these questions are imperative, and we appreciate Google's continued cooperation with this important, nation-wide investigation.

Very truly yours,



RICHARD BLUMENTHAL

RB/AJ