UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

October 27, 2010

Albert Gidari, Esq.
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, WA 98101-3099

Dear Mr. Gidari:

I am writing regarding your client Google's announcement about its collection of consumer data transmitted over unsecured wireless networks. According to Google's announcement, in 2007, the company installed software on its "Street View" cars[1] to collect data about consumers' wireless network access points for the purpose of improving its location-based services. Earlier this year, in response to a request from the data protection authority in Hamburg, Germany, Google discovered that the software on the Street View cars had also been collecting some "payload" data – contents of communications sent over unsecured wireless networks. The company stated that the collection of payload data was inadvertent and that the company did not use the payload data in any Google product or service.[2]

FTC staff has concerns about the internal policies and procedures that gave rise to this data collection. As noted above, the company did not discover that it had been collecting payload data until it responded to a request for information from a data protection authority. This indicates that Google's internal review processes – both prior to the initiation of the project to collect data about wireless access points and after its launch – were not adequate to discover that the software would be collecting payload data, which was not necessary to fulfill the project's business purpose. These review processes are necessary to identify risks to consumer privacy posed by the collection and use of information that is personally identifiable or reasonably linkable to a specific consumer. For *any* such information, Google should develop and implement reasonable procedures, including collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored.

---

[1] Google's Street View program provide street-level imagery of locations through the company's Google Maps product. The images are collected primarily by Street View cars, which include directional cameras to capture 360° views, a GPS unit for positioning and laser range scanners. *See* Google Maps with Street View, Behind the Scenes, *available at* http://maps.google.com/help/maps/streetview/behind-the-scenes.html#vehicles.

[2] *See* Official Google Blog, WiFi Data Collection: An Update (May 14, 2010), *available at* http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

Chairman Leibowitz highlighted some of these issues in his testimony before the Senate Commerce Committee on July 27, 2010.[3] As you know, the FTC has undertaken a project to re-examine its approach to consumer privacy in light of changing technologies and business practices.[4] During a series of public roundtables, panelists raised concerns about companies' collecting more consumer information than necessary to fulfill a legitimate business need. A related concern was that companies are storing consumer data for longer periods (at lower cost) and will find new uses for it that consumers may not have contemplated at the time of collection. Accordingly, panelists and commenters discussed the need for companies to build strong privacy protections into their products and business operations at the outset.

To this end, we note that Google has recently announced improvements to its internal processes to address some of the concerns raised above, including appointing a director of privacy for engineering and product management; adding core privacy training for key employees; and incorporating a formal privacy review process into the design phases of new initiatives. The company also publicly stated its intention to delete the inadvertently collected payload data as soon as possible.[5] Further, Google has made assurances to the FTC that the company has not used and will not use any of the payload data collected in any Google product or service, now or in the future. This assurance is critical to mitigate the potential harm to consumers from the collection of payload data.[6] Because of these commitments, we are ending our inquiry into this matter at this time.

We ask that the company continue its dialogue with the FTC about how best to protect consumer privacy as it develops its products and services.

Sincerely,

David Vladeck | KDR

David C. Vladeck

---

[3] *See* Prepared Statement of the Federal Trade Commission on Consumer Privacy before the Committee on Commerce, Science, and Transportation, United States Senate, at 22 (July 27, 2010), *available at* http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf.

[4] *See* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[5] *See* Official Google Blog, Creating Stronger Privacy Controls Inside Google (Oct. 22, 2010), *available at* http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

[6] *See id.*