

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

JONATHAN MEDALSY
212.551.2637
jmedalsy@wiggin.com

This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

Connecticut Attorney General Announces \$7 Million Settlement with Google for Data-Snatching WI-FI Drive-Bys

Connecticut Attorney General George Jepsen [1] announced yesterday a \$7 million multistate settlement with Google, Inc. arising out of Google's ambitious, but over-intrusive 'Street View' project to map the United States at street level and improve Google's geo-location services. Attorney General Jepsen's office led an executive committee of eight states that conducted negotiations with Google over the past two years, culminating in yesterday's announcement of Google's "Assurance of Voluntary Compliance." [2] The agreement, which becomes effective immediately, was signed by the attorneys general of 38 states and the District of Columbia. In announcing the settlement, the Attorney General emphasized that the \$7 million dollar fine was not the main objective of the authorities:

"Consumers have a reasonable expectation of privacy. This agreement recognizes those rights and ensures that Google will not use similar tactics in the future to collect personal information from unsuspecting customers."

GOOGLE'S STREET VIEW PROJECT AND THE CAPTURE OF WIRELESS 'PAYLOAD DATA' FROM CONSUMERS

Between 2008 and March 2010, Google let loose a fleet of quirky, antenna-laden 'Street View vehicles' across the United States (and abroad) to map and geo-locate the country's cities, towns and suburbs. Part of Google's data collection involved

capturing information on business and personal wireless networks identified by Google's antennae and 'Kismet' open source software as its vehicles roamed the streets. Google has maintained that its intention was to capture only publicly available network identification information to enhance Google's geo-location features on Google Maps; however, the company admits that it also occasionally captured data frames, including 'payload data' in the process –i.e., bits of message content in user communications. Payload data from unsecured Wi-Fi networks included e-mail text, web pages being viewed by users, e-mail addresses and other types of personal and business content passing through the networks being surveyed by Google's car fleet.

When it was discovered that the Street View project was capturing personal information from unsuspecting users as Google drove by their houses and apartments, Google initially denied the allegations. Regulators around the world soon launched investigations, as did the Federal Trade Commission ("FTC") and a group of U.S. attorneys general. Most of the Street View investigations by data protection authorities outside the United States have now been settled, with Google promising to destroy any payload data it collected. In October 2010, the FTC dropped its investigation of the Street View matter, citing Google's assurances that it had not used the payload data and its promise to reform its privacy practices. A consolidated

CONTINUED ON NEXT PAGE

Connecticut Attorney General Announces \$7 Million Settlement with Google for Data-snatching

WI-FI Drive-bys CONTINUED

privacy class action suit arising out of the Street View project is still pending in the Northern District of California. [3] Google has consistently maintained that management was unaware of the payload data collection, claiming that the data was isolated once it was discovered and that the company never used payload data in any Google product or service. This position was reiterated in the settlement announcement yesterday.

TERMS OF GOOGLE'S ASSURANCE OF VOLUNTARY COMPLIANCE

In addition to the \$7 million fine (which will be shared among the 38 states), the terms of the Google settlement include Google's commitments to:

- Roll out an internal privacy program lasting for 10 years to disseminate and implement the terms of the settlement throughout Google's management, legal department and product counsel, and rank and file employees;
- Offer general privacy education and certification programs to Google employees and hold an annual "Privacy Week" event across Google's offices;
- Exercise reasonable care in selecting third party service providers that are competent to protect the privacy of Google users' information (the Kismet software used in the Street View is blamed in part for the unwitting collection of payload data);
- Securely delete or destroy all payload data collected in the United States (subject to pending or future litigation holds) and certify the same to the 38 attorneys general; and
- Launch a public service campaign to educate consumers about protecting their personal information while using wireless networks, including creation of an informational YouTube video, running online ads for two years promoting this video, writing blog posts on Google's Public Policy blog, and placing public service ads in newspapers.

In exchange for its commitments under the settlement agreement, Google is released from all civil claims that the signing attorneys general may have asserted against Google for the payload data collection under their respective consumer protection statutes. The settlement also provides that Google admits no wrongdoing and that the terms of the settlement may not be admitted as evidence of any wrongdoing on Google's part.

LESSONS LEARNED

The Street View incident has served as one of the poster children of the "privacy by design" movement that has been gathering steam in the U.S. privacy community. The mantra of this movement is that companies should build privacy considerations into their new products and services before they send them out into the world. By some accounts, Google was simply unaware of

the full data capture capabilities of the open source software used to collect network data as Google's fleet of cars drove around the country picking up Wi-Fi hot spots. Google's "pound of cure" with the Street View project may serve as a warning to other data intensive businesses to consider the "ounce of prevention" approach to product innovation.

[1] <http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=520518>

[2] http://www.ct.gov/ag/lib/ag/press_releases/2013/20130312_google_avc.pdf

[3] *In re Google Inc. St. View Elec. Communications Litig.*, 794 F. Supp. 2d 1067 (N.D. Cal. 2011).