Google's illegal Wi-Fi Hacking Exposed by Engineer

by David Streitfeld via lynx - SMH *Sunday, Apr 29 2012, 10:04pm*
international / mass media / other press

> Google's harvesting of emails, passwords and other sensitive personal information from unsuspecting households in Australia and around the world was neither a mistake nor the work of a rogue engineer, as the company long maintained, but a program that supervisors knew about, according to new details from the full text of a regulatory report.

Google spying

The report, prepared by the US Federal Communications Commission after a 17-month investigation of Google's Street View project, was released, heavily redacted, two weeks ago. Although it found that Google had not violated any laws, the agency said Google had obstructed the inquiry and fined the company $US25,000. On Saturday, Google released a version of the report with only employees' names redacted.

The full version [PDF/4.5MB] draws a portrait of a company where an engineer can easily embark on a project to gather personal emails and web searches of potentially hundreds of millions of people as part of his or her unscheduled work time, and where privacy concerns are shrugged off.

The payload data was secretly collected between 2007 and 2010 as part of Street View, a project to photograph streetscapes over much of the civilised world. When the program was being designed, the report says, it included the following 'to do' item: "Discuss privacy considerations with Product Counsel."

"That never occurred," the report says.

Google says the data collection was legal. But when regulators asked to see what had been collected, Google refused, the report says, saying it might break privacy and wiretapping laws if it shared the material.

A Google spokeswoman said Saturday that the company had much stricter privacy controls than it used to, in part because of the Street View controversy. She expressed the hope that with the release of the full report, "we can now put this matter behind us."

Ever since information about the secret data collection first began to emerge two years ago, Google

has portrayed it as the mistakes of an unauthorised engineer operating on his own and stressed that the data was never used in any Google product.

The report, quoting the engineer's original proposal, gives a somewhat different impression. The data, the engineer wrote, would "be analysed offline for use in other initiatives." Google says this was never done.

The report, which was first published in its unredacted form by The Los Angeles Times, also states that the engineer, who began the project as part of his "20 per cent" time that Google gives employees to do work on their own initiative, "specifically told two engineers working on the project, including a senior manager, about collecting payload data."

As early as 2007, the report says, Street View engineers had "wide access" to the plan to collect payload data. Five engineers tested the Street View code, a sixth reviewed it line by line, and a seventh also worked on it, the report says.

Privacy advocates said the full report put Google in a bad light.

"Google's rogue engineer scenario collapses in light of the fact that others were aware of the project and did not object," said Marc Rotenberg, executive director of the Electronic Privacy Information Centre. "This is what happens in the absence of enforcement and the absence of regulation."

The Street View program used special cars outfitted with cameras. Google first said it was just photographing streets and did not disclose that it was collecting internet communications called payload data, transmitted over Wi-Fi networks, until May 2010, when it was confronted by German regulators.

Eventually, it was forced to reveal that the information it had collected could include the full text of emails, sites visited and other data.

Even if a user was not working on a computer at the moment the Street View car slowly passed, if the device was on and the network was unencrypted, all sorts of information about what the user had been doing could be scooped up, data experts say.

"So how did this happen? Quite simply, it was a mistake," a Google executive wrote on a company blog in 2010. "The project leaders did not want, and had no intention of using, payload data."

But according to the report, the engineer suggested in his proposal that it was entirely intentional: "We are logging user traffic along with sufficient data to precisely triangulate their position at a given time, along with information about what they were doing."

Attending to paperwork did not seem to be a high priority, however. Managers of the Street View project told FCC investigators that they never read the engineer's proposal, called a design document. A senior manager of Street View said he "preapproved" the document before it was written.

More than a dozen countries began investigations of Street View in 2010. In the United States, the Justice Department, the Federal Trade Commission, state attorneys general and the FCC looked into the matter.

The engineer at the centre of the project cited the Fifth Amendment protection against self-

incrimination. Because FCC investigators could not interview him, they said there were still unresolved questions about the case.

Copyright applies.

Footnote:
[If that cocksucking fairy chair'woman,' Eric Schmidt, is wondering who is supplying compromising data to competitors, then take a fuckin' guess -- suppress us at your own risk, faggot!

It's all in the numbers, dickheads; we have nothing to lose, you have been suppressing this site for over 5 years and we have been logging and accruing evidence over that period. btw, we were offered 'incentives' to supply but we did one better, we released our data FREE to corps that can do Google the most damage -- fuck with us will ya! Benign impartial search engine, my ass!]

Suck on that, sweetie!

http://tinyurl.com/7d9g997
