**What Google Knows About You**  
  
**By Tyler Durden**

<http://www.informationclearinghouse.info/article35748.htm>

August 03, 2013 "[Information Clearing House](http://www.informationclearinghouse.info/) - Earlier, we reported the [personal narrative of Michele Catalano](http://www.zerohedge.com/news/2013-08-01/guest-post-pressure-cookers-backpacks-and-quinoa-oh-my) who recounted how one day she found herself face to face with six agents from the joint terrorism task force. The reason? "Our seemingly innocent, if curious to a fault, Googling of certain things was creating a perfect storm of terrorism profiling. **Because somewhere out there, someone was watching.** Someone whose job it is to piece together the things people do on the internet raised the red flag when they saw our search history."

The answer of "who" was watching should be far clearer in the aftermath of the Snowden revelations from the past two months. But instead of rehashing the old story of the NSA intercepting and recording virtually every form of electronic communication that exists, or ruminating on what filters Ms. Catalano triggered to lead to this truly disturbing outcome, perhaps a better question is ***just what is it that Google knows about each and everyone who uses its interface daily***, which in this day and age means everyone with a computer. **As it turns out, pretty much everything.**

Here is the thought, and not so "thought" experiment that the [WSJ's Tom Gara ran yesterday](http://blogs.wsj.com/corporate-intelligence/2013/07/31/googles-all-seeing-eye-does-it-see-into-me-clearly-or-darkly/), before Ms. Catalano's story had hit, to uncover just how rich his informational tapestry is in the repositories of the firm that once upon a time urged itself, rhetorically, to "not be evil."

Let’s run through a little thought experiment.

Imagine there’s a list somewhere that contains every single webpage you have visited in the last five years. It also has everything you have ever searched for, every address you looked up on Google GOOG +1.86% Maps, every email you sent, every chat message, every YouTube video you watched. Each entry is time-stamped, so it’s clear exactly, down to the minute, when all of this was done.

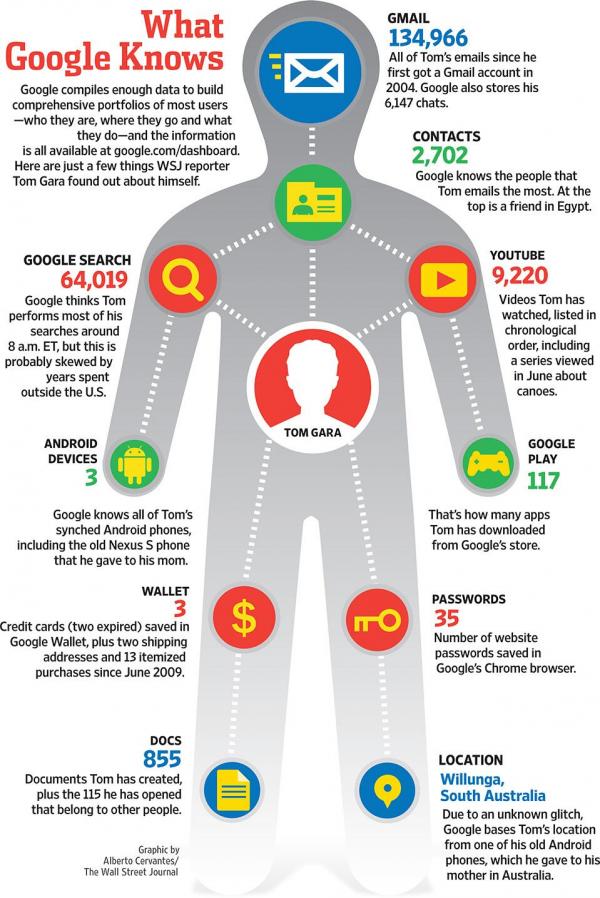
Now imagine that list is all searchable. And imagine it’s on a clean, easy-to-use website. With all that imagined, can you think of a way a hacker, with access to this, could use it against you?

**And once you’ve imagined all that, go over to google.com/dashboard, and see it all become reality.**

For a piece complementing today’s story on Google and privacy by the WSJ’s Amir Efrati, I took a deep dive into Google Dashboard, a kind of Grand Central Terminus for all the information the company has stored on you. It’s a truly amazing amount, especially if, like me, you have been a heavy Gmail user since its launch in 2004. As long as you are logged into Gmail, or any other Google account, the company isn’t just keeping track of how you use its own service — it’s noting every site you visit on the web.

**Here’s a snapshot of the kind of data we found on my Google Dashboard, put together as a graphic for today’s newspaper. It includes my 64,019 Google searches, and 134,966 Gmail conversations:**

The snapshot in question:

[](http://www.zerohedge.com/sites/default/files/images/user5/imageroot/2013/08/What%20Google%20Knows.jpg)

Gara's purely theoretical ruminations continue:

The idea that all of this data exists as a mass of ones and zeros deep in a server farm in California, being studied by disinterested robots to serve up better search results and more relevant ads, is something most of us can process in the abstract.

But the fact that it is all viewable right now, on a user-friendly Web page complete with its own search service (yes, you can run Google searches on your own web history), is something else entirely. For example, I searched for every website I’ve ever visited containing the word “octopus.” And yes, the results were wonderful.

**Of course, if somebody else managed to access my Google Dashboard — and the chances of this happening are well above zero — they could search for things far less innocent than an eight-tentacled sea creature. The bad possibilities seem endless, from digital blackmail to much deeper forms of identity theft**.

Or six joint terrorism task force agents showing up on your front step just because you googled "pressure cookers."

But wait, there's more.

Because it is not just the NSA, and its downstream enforcement tentacles, that has open access to the informational nexus that is Google and its "Don't be evil" creed. So does the FBI.

The [WSJ is again on the trail](http://online.wsj.com/article_email/SB10001424127887323997004578641993388259674-lMyQjAxMTAzMDAwMTEwNDEyWj.html?mod=wsj_valettop_email).

Law-enforcement officials in the U.S. are expanding the use of tools routinely used by computer hackers to gather information on suspects, bringing the criminal wiretap into the cyber age.

Federal agencies have largely kept quiet about these capabilities, but court documents and interviews with people involved in the programs provide new details about the hacking tools, including spyware delivered to computers and phones through email or Web links—techniques more commonly associated with attacks by criminals.

People familiar with the Federal Bureau of Investigation's programs say that the use of hacking tools under court orders has grown as agents seek to keep up with suspects who use new communications technology, including some types of online chat and encryption tools. The use of such communications, which can't be wiretapped like a phone, is called "going dark" among law enforcement.

A spokeswoman for the FBI declined to comment.

**The FBI develops some hacking tools internally and purchases others from the private sector. With such technology, the bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations, one former U.S. official said. It can do the same to microphones in laptops without the user knowing, the person said.** Google declined to comment.

There is more but the gist is clear: all those seemingly ridiculous surveillance methods used by Jack Bauer and countless other fictional characters... they were all too real.

Just as real, in fact, as the Big Brother predicted by George Orwell so many years ago. And just as real, although we will need another Edward Snowden to reveal it, as the modern-day equivalent of [Room 101](http://en.wikipedia.org/wiki/Room_101).

*Copyright ©2009-2013 ZeroHedge.com/ABC Media, LTD -* [*http://www.zerohedge.com/*](http://www.zerohedge.com/)

**What's your response? - *Scroll down to add / read comments***