San Francisco Chronicle

Technically speaking, how could NSA's PRISM wield Google and Facebook as spies?

By Caleb Garling – July 7, 2013

In the wake of revelations around the extent of the NSA surveillance programs it's worth asking how such a program would operate, from a technical standpoint. The feds have been collecting cell phone, Internet and credit card data and to detect — and ostensibly stop — crimes.

Recently leaked document and previous court cases indicate much of that data comes from Internet companies and telecom providers we use every day like Google, Facebook, Microsoft, Verizon and AT&T. So far each associated-company has denied knowledge of PRISM or that the government had access to their computer servers. (Though, it's highly unlikely government officials would ever use the term "PRISM" with said tech company.)

But when speaking about complicated computer systems it is easy to play word games and — technically — tell the truth. "Direct access" or "open-ended access" are terms that can be truthful simply when you install another system between the first two or by putting any restriction on the query.

"I find it extraordinarily unlikely that this could happen without these companies' cooperation," says Dan Auerbach, the Electronic Frontier Foundation's staff technologist.

Precious few facts exist about the NSA's digital dragnet techniques. But there are a few measures that could be implemented that would still keep the tech companies honest when they say the NSA didn't have access to their servers.

Tech companies could send information about users to the NSA on a regular basis, with this information mirroring what's in its servers. Or it could allow access to an application program interface, which would allow the NSA to make calls of the data it wanted on users.

But Julian Sanchez, a technology research fellow at the Cato Institute, points out that the NSA doesn't want tech companies to be aware of the agency's search criteria on user data.

The Washington Post reports that documents that say the arrangement between the tech companies and the feds allowed "collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations," rather than directly to company servers.

Big tech companies operate their own data centers — vast buildings packed with computers that underpin the services we use every day like Hotmail, Gmail and Facebook. This is where your emails and status updates are physically stored when called up by a web browser. The NSA could install devices in the data centers for traffic to pass through and be collected.

Not to mention that the data from your computer has to travel through all the digital hubs that make up the Internet's infrastructure to get to those data centers. Sniffing those would allow collection of user data also.

But this leaves the question of decoding the data since sensitive data is encrypted with security protocols — "secure socket layer" (SSL). If the sender and the receiver have the decoding key, then they can send encrypted user information safely back and forth. Only someone with the key could read it.

Though Auerbach acknowledges that the NSA is "head and shoulders above the rest of the world" when it comes to breaking encrypted data, he finds the possibility of the NSA cracking the code for tech companies "pretty unlikely."

However, tech companies could provide those private keys for the SSL certificates to the NSA. And then the NSA could decrypt the messages itself. In discussing the various possibilities, Sanchez finds this scenario likely and calls it "consistent" with other NSA practices, such as the case with AT&T.

By basically allowing a wiretap of the communication between the servers and the outside world, and providing the decoder to read the messages, tech companies could honestly say they don't allow direct access or a "back door" to the servers — while still allowing the NSA unrestricted access to the information.