Google's Schmidt Says Network Trapdoors Are a Bad Idea

December 12, 2014
By Amy Schatz

Google chairman Eric Schmidt dismissed the idea Friday of making it easier for U.S. public safety agencies to collect information about users, saying there's no need for "trapdoor" access to its networks.

Federal and state law enforcement agencies have raised concerns about new encryption protections that Apple and Google have begun adding to their smartphone operating systems which wouldn't allow the companies to unlock phones for law enforcement or government agencies.

Federal Bureau of Investigation director James Comey has asked the companies to add doors to their systems to allow law enforcement access, saying that not doing so could help criminals and terrorists and endanger the public.

"The problem with the government requests is it'd be great if you're the government to have a trapdoor," Schmidt said, adding that Google would be concerned about who else might gain access to its network if it built such an opening into its systems.

"Our argument, which I think is clear now, is the government has so many ways — properly so, by the way — to go in the front door. They're called warrants. They're called good police work," he said.

The FBI director and other law enforcement officials have called on Congress to update a 1994 law which requires phone companies to build back doors into their systems to allow government agencies to install wiretaps and collect information. That law doesn't cover newer forms of Internet-based communications.

Schmidt was speaking at a Cato Institute conference on government surveillance. Video of the event is here. (He speaks from roughly 3:35 to 4:12 on the recording.)

During the interview, Schmidt repeated previous statements that he had no personal knowledge of the National Security Agency's Prism data collection program (although leaked documents suggest Google wasn't entirely in the dark about some aspects of the program).

Schmidt said he learned about the program after reading about it in the Washington Post. "I was shocked because Jared Cohen and I had written a book about this being possible. The fact that it

had been done so directly and documented in the documents that were leaked was really a shock to the company," he said.

Although the documents leaked by Edward Snowden were damaging in some ways, particularly in Europe, Schmidt said the revelations about the mass surveillance program did lead Google to increase its encryption protections and was "helpful" for raising public awareness of the issue.

"We clearly do not want to encourage bulk data leaking," Schmidt said, ticking off examples of databases that contain vast amounts of personal or financial information about consumers. "It's not good for society to encourage people to do that."