U.S. News & World Report

Schmidt: Google Now Best Way to Evade NSA

Google's executive chairman says his company responded well to Edward Snowden's revelations.

By Steven Nelson
Dec. 12, 2014

Google Executive Chairman Eric Schmidt said at a surveillance forum Friday that exiled whistleblower Edward Snowden revealed the government was monitoring Americans' Internet activity by tapping the connections between his company's data centers.

But, he also said, Google's services should now be a destination for people looking to avoid surreptitious National Security Agency snooping.

Schmidt – described as "the NSA's best frenemy" by Cato Institute fellow Julian Sanchez earlier in the daylong, Cato-hosted event – told the audience he first learned about direct government surveillance of data being transmitted between company servers in a 2013 report in The Washington Post.

The surveillance operation – code-named MUSCULAR – was reportedly a partnership between the NSA and its British counterpart, the Government Communications Headquarters, that copied "entire data flows" from fiber-optic cables connecting corporate data centers, according to the Post.

"The fact that it had been done so directly and documented in the documents that were leaked was really a shock to the company," Schmidt said. "When it [comes] to monitoring data traffic between Google servers, they're clearly monitoring traffic for people who are in the U.S., which as I understand – and I'm not a lawyer – is not their mission."

Whistleblower John Napier Tye, who participated in a panel earlier in the day, has warned the NSA can use Executive Order 12333 to collect vast amounts of U.S. communications from overseas servers and cables without a warrant and with neither court nor congressional oversight.

On Wednesday, Congress for the first time passed legislation appearing to condone this overseas collection of U.S. records, establishing a five-year limit for retention of most phone and Internet communications.

Schmidt said Google responded to the Post's report by "massively" encrypting its systems to protect users from warrantless surveillance. Users now are likely to die before anyone can crack the company's 2048-bit data encryption, he said.

“If you have important information, the safest place to keep it is Google,” the billionaire businessman told listeners. “And I can assure you the safest place to not keep it is anywhere else, because of the level of attacks” from Chinese hackers and government spy agencies.

During a question-and-answer session, Schmidt also touted the incognito mode on Google’s Chrome browser.

“If for whatever reason you do not wish to be tracked by federal and state authorities, my strong recommendation would be to use incognito mode,” he said.

The Google leader’s self-promotion wasn’t universally accepted as sound advice. Christopher Soghoian, the American Civil Liberties Union’s Speech, Privacy and Technology Project's principal technologist, contradicted Schmidt's recommendation for evading surveillance.

“Incognito mode will do nothing to protect you from surveillance by the authorities – that is not the right technology and there are technologies like Tor that will do a much better job,” Soghoian said, referring to the anonymized Tor network.

“I’m referring to Google’s part of that,” Schmidt responded. “Using Tor is a whole 'nother conversation, which may or may not be appropriate in certain situations.”

Chrome users who open an incognito page are advised that "going incognito doesn’t hide your browsing from your employer, your Internet service provider, or the websites you visit."