IDG News Service

Schmidt: NSA revelations forced Google to lock down data

Grant Gross
Dec. 15, 2014

Google has worked hard to lock down the personal data it collects since revelations in the last year and a half about mass surveillance programs at the U.S. National Security Agency, company Chairman Eric Schmidt said.

The news of surveillance by the NSA and intelligence agency counterparts at allied nations has damaged the U.S. tech industry on "many levels," with many Europeans now distrusting U.S. tech companies to hold on to their personal data, Schmidt said Friday at a surveillance conference at the Cato Institute, a libertarian think tank.

Schmidt learned of efforts by U.K. intelligence agency GCHQ to intercept traffic between Google data centers through a newspaper article, he told the audience. "I was shocked," Schmidt said.

Google had envisioned a complicated method to sniff traffic, but "the fact that it had been done so directly ... was really a shock to the company," Schmidt said.

After reporters showed Google engineers a diagram of the intelligence agency's methods to tap links between Google data centers, the engineers responded with a "fusillade of words that we could not print in our family newspaper," Washington Post reporter Craig Timberg said.

Google responded to the revelations by former NSA contractor Edward Snowden by spending a lot of money to lock down its systems, including 2,048-bit encryption on its traffic, Schmidt said. "We massively encrypted our internal systems," he said. "It's generally viewed that this level of encryption is unbreakable in our lifetime by any sets of human beings in any way. We'll see if that's really true."

Schmidt told the audience that the safest place to keep important information is in Google services. "Anywhere else" is not the safest place to keep data, he said.

Schmidt touted the incognito browsing feature in Google's Chrome browser and Google's Dashboard feature, which allows its users to set their privacy preferences. He noted that some security experts have questioned his claim that Android is the safest mobile operating system. Both Google and Apple are working "very, very hard" on security features in their mobile OSes, he said.

Timberg, along with some audience members, questioned Google's own collection of personal data, however. Google itself collects huge amounts of user data, Timberg noted.

Google collects data to help deliver its services, and has, in some cases, killed projects that raised privacy concerns, Schmidt said. "I hear this perception that we're somehow not playing by the rules of modern society," he said. "I think that's wrong. I think the evidence is that Google has been incredibly sensitive to privacy issues."

Chrome's incognito feature will "do nothing" to protect users from government surveillance, said Chris Soghoian, principal technologist with the American Civil Liberties Union. Soghoian also questioned Schmidt about past comments he made suggesting Google retains user information to comply with law enforcement surveillance requests.

Google complies with legal law enforcement requests, Schmidt said, and retains user data for a year because of government mandates.

Julian Sanchez, a senior fellow at Cato, asked if Google has incentives to lock down data when much of its business model is collecting user data.

People criticizing the company's privacy efforts "don't understand how Google works," Schmidt said. "Google's job is build stuff that delights customers. When governments illegally invade their privacy, that's like a negative. It's easy to understand why we'd make these systems stronger."

Timberg asked Google about a recent push by the FBI and U.S. Department of Justice to build back doors in encrypted services as a way to fight crime. The recent requests came after announcements from Apple and Google of new encryption tools for mobile phones.

Back doors are a bad idea, Schmidt said. "It'd be great, if you're the government, to have a trap door, but how do we at Google know that the other governments are not taking over the trap door from you?" he said.

Law enforcement officials have "so many ways" to investigate crime without requiring tech companies to build back doors into products, Schmidt said.

In an earlier panel at the Cato forum, Soghoian said the U.S. public should be as concerned about surveillance by local police as it is about surveillance by the NSA.

Big-data tools created for intelligence agencies, including metadata collection programs, are "trickling down to state and local law enforcement agencies," he said. "It's simply not appropriate for local law enforcement to have intelligence community-grade surveillance technology, because these devices do not respect the privacy of innocent Americans."