

Google report documents surge in electronic surveillance requests by governments worldwide

Thomas Gaist
20 September 2014

Google received some 32,000 data requests from governments worldwide during the first six months of 2014. The total number of data requests submitted by governments have surged 150 percent in the past five years, according to a “transparency report” published this week by the company.

Google complied with 65 percent of the requests, including 84 percent of the requests submitted by the US government, according to the report.

Data requests by the US government increased 250 percent over the same period, including almost 20 percent in the first half of 2014 alone. The US government accounted for 40 percent of total data requests, demanding data from some 21,500 specific user accounts in the first half of this year.

Internationally, Google reported receiving at least 1,000 user data requests from France, Germany, India, Italy, Singapore and UK; more than 500 requests from Australia, Brazil, Poland, Spain and Taiwan; and more than 100 requests from Argentina, Belgium, Chile, Hong Kong, Japan, Mexico, Portugal, South Korea, Switzerland and Turkey. Data requests submitted by the Australian government have tripled since 2010, Google reported.

A number of governments began demanding data from Google for the first time in 2014, including Albania, the Dominican Republic, Egypt, Indonesia, Kosovo, Luxembourg, Maldives, Namibia and Nepal.

Google’s document makes clear that its transparency reporting is subject to various loopholes and delays. Statistics covered in the report do not include data requests that carry “gag orders,” nor does Google report on “emergency data requests” relating to national security or some criminal investigations.

Requests submitted to the company through the Foreign Intelligence Surveillance Court (FISC) are subject to a six-month reporting delay. “New Capability Orders,” or data requests relating to a new form of electronic surveillance, are only reported by Google after a two-year delay, the report said.

US government agencies can also access data without a specific warrant through several avenues. Under the Electronic Communications Privacy Act (ECPA), top FBI officials can issue National Security Letters (NSL) demanding names, addresses, calling records and other information, all without a warrant. Specific users targeted by NSLs are generally not informed that they are being surveilled, Google reported.

Google releases a range of different forms of data to the government:

- * Subscriber registration information, including names, account creation information, associated email addresses, and phone numbers
- * Sign-in IP addresses and associated times
- * Email header information and email content
- * From YouTube, subscriber registration information, video upload IP addresses and time stamps
- * Copies of private videos, private messages, private blog posts and other content

Google claims that it only transfers actual content of electronic communications to the government in response to specific warrants.

However, the National Security Agency’s PRISM program enables the NSA to directly seize communications data in bulk by tapping into the fiber optic cables that carry the majority of the world’s internet traffic.

After PRISM’s existence was revealed by Edward

Snowden in the summer of 2013, Google and the other tech companies denied any knowledge of the program. Subsequent leaks revealed that Google, Yahoo, Microsoft, Facebook, and other tech giants accepted millions of dollars from the NSA's Special Source Operations (SSO) division, the NSA branch responsible for managing the agency's "corporate partnerships," as part of their collaboration with PRISM.

Seeking to rehabilitate its public image in the wake of the Snowden disclosures, Google has been collaborating with Digital Due Process (DDP), a coalition of NGOs and corporations that includes the American Civil Liberties Union (ACLU), Amazon, Apple, the Constitution Project, the Center for Financial Privacy and Human Rights, Facebook, Microsoft, Reddit and other organizations. The DDP aims "to balance the law enforcement interests of the government, the privacy interests of users, and the interests of communications service providers," according to its statement of principles.

In reality, the privacy interests of internet users are in direct conflict with the interests of the communications companies, which have played a central role in the erection of the global surveillance machinery.

Far from having an adversarial relationship with the surveillance agencies of the state, Google functions as an indispensable co-partner and facilitator of the mass spying. As Wikileaks head Julian Assange commented late this week, "Google's business model is the spy. It makes more than 80 percent of its money by collecting information about people, pooling it together, storing it, indexing it, building profiles of people to predict their interests and behavior, and then selling those profiles principally to advertisers, but also others," Assange said.

"So the result is that Google, in terms of how it works, its actual practice, is almost identical to the National Security Agency or GCHQ," Assange said.

Google has been working with the NSA "at least since 2002," Assange noted.

"They are formally listed as part of the defense industrial base since 2009. They have been engaged with the Prism system, where nearly all information collected by Google is available to the NSA. At the institutional level, Google is deeply involved in US foreign policy," Assange said.



To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact