US government requests for Internet communications soar

Don Knowland
9 February 2013

A Google report released Monday shows a marked increase in government requests for private communications of Internet users.

The report indicates that between 2010 and 2012, US government requests for data of separate users increased by 85 percent, from 8,888 in 2010 to 16,407 in 2012. This is a global phenomenon, with user data requests increasing during this time period by 70 percent worldwide, to 43,327 requests in 2012.

Google says it complied and handed over user information on two-thirds of the total requests it received in 2012, and to 88 percent of requests from the US government.

The majority of requests in the US for data—beyond items like a user's name, location, phone number and the time that an email was sent—are through subpoenas served by prosecutors. In other words, there is no search warrant issued after judicial review, despite the mandate of the Fourth Amendment to the US Constitution that the government obtain a determination by a judge that there is probable cause to believe that the items seized will evidence a crime.

Unlike with postal mail and telephone calls, which US government criminal agencies concede require a judicial finding of probable cause before interception, the government takes the position that emails and other electronic communications more than 180 days old are not protected under the Electronic Communications Privacy Act of 1986, because of an exemption in the statute. However, that legislation was enacted years before widespread use of email, the invention of social networking or cloud storage of data. Moreover, this position has been asserted despite a federal appellate court ruling that the 180-day provision is unconstitutional.

The US government does not notify people when it is searching their online information, and frequently demands that the Internet service not notify targets, as happened initially with respect to WikiLeaks personnel in light of the investigation of Army Private Bradley Manning.

The US Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994, during the Clinton administration, to require telecommunications carriers and manufacturers of telecommunications equipment to ensure that they have built-in surveillance capabilities allowing federal agencies to monitor all telephone, broadband Internet, and VoIP (voice-over-IP) traffic in real time. Later the Federal Communications Commission, at the request of the Federal Bureau of Investigation (FBI) and other US government agencies, expanded CALEA to include all VoIP and broadband Internet traffic.

In similar fashion, the FBI has now sought to require Gmail, Facebook, Twitter, BlackBerry, Skype and other Internet communication service providers to design their systems to comply with wiretap orders, such that contents of email and other communications can be readily retrieved.

In a primer published on Monday, Google says it is requiring a search warrant to turn over the contents of mail messages, private YouTube videos, stored voicemails or text messages on Google Voice and private blog posts on Blogger.

There are other major providers that are not adopting even the limited impediments to searches that Google says it is now applying.

The Electronic Frontier Foundation (EFF), along with dozens of other privacy advocacy groups, recently sent an open letter to Skype's owner Microsoft, requesting disclosure of its search policies for user data.

Specifically, the letter demands a "Transparency

Report," including:

• Quantitative data regarding the release of Skype user information to third parties, including which governments have requested the data, what kind of data, and the proportion of requests that were complied with. The group also wants to know why certain requests may have been rejected.

• The data collected by Microsoft and Skype on users, along with how long that data is stored—so-called "retention policies";

• Skype's best understanding of what data can be intercepted, particularly through technologies such as deep-packet inspection, which may include details of how secure the network is to send voice-over-IP traffic and conversation data;

• Skype's policies on assisting law enforcement, including how it responds to "gagging orders," and how it responds to law enforcement and intelligence agencies when data is requested on Skype customers.

The letter underlined the "persistently unclear and confusing statements about the confidentiality of Skype conversations," and, in particular, "the access that governments and other third parties have to Skype user data and communications."

The EFF emphasizes the urgency of the matter, given that Microsoft is in the process of switching over tens of millions of Windows Live Messenger users to Skype.

Another particular concern voiced is that TOM, a co-branded version of Skype for users in China, is subject to routine and widespread monitoring and interception of communications by the Chinese government.

The EFF coalition asked about the exact "current operational relationship between Skype with TOM Online in China and other third-party licensed users of Skype technology."

Previously, in 2008, Skype stated that it could not eavesdrop on user conversations due to its peer-to-peer architecture and encryption techniques. Skype had also taken the position that it was not required to comply with expanded CALEA rules on real-time interception of digital communications because it was based in Europe.

All this is in doubt since Microsoft acquired Skype in 2011.

In fact, since that time Microsoft and Skype have both refused to answer questions about exactly what kinds of user data can be intercepted, what user data is retained, and whether eavesdropping on Skype conversations may take place.

In 2012, the FBI issued a subpoena for Skype chats going back to 2007, and then used those chats as the basis of evidence for criminal charges. This casts in doubt on Skype's representation that it retains chats for no more than 30 days.

In December, the US Senate Judiciary Committee passed an amendment mandating that the government get a probable cause warrant before reading emails or other electronic communications. The amendment died on the vine. There is little chance that, even if reintroduced this year, it will pass the full Senate, pass the the House, or be signed into law by President Obama.

The discussion above does not even address the US government's interception of communications under the Foreign Intelligence Surveillance Act (FISA) of "foreign intelligence information." This can be done in certain circumstances under FISA without even the review of the secret FISA court.

Moreover, it has been revealed that the US National Security Agency (NSA) has monitored, without obtaining search warrants, the phone calls, Internet activity (web, email, etc.), text messaging, and other electronic communication involving parties believed by the NSA to be outside the US, even if the other end of the communication lies within the country. The agency has otherwise engaged in mass "data mining" in order to correlate data of US residents from emails, phone calls, Internet searches, and credit card activity and store it in a database for analysis.

These developments show that the move toward an authoritarian police state is not just creeping, but is an oncoming flood.