

WIRED

U.S. Says It Spied on 89,000 Targets Last Year, But the Number Is Deceptive

By Kim Zetter

June 27, 2014

About 89,000 foreigners or organizations were targeted for spying under a U.S. surveillance order last year, according to a new transparency report. The report was released for the first time Friday by the Office of the Director of Intelligence, upon order of the president, in the wake of surveillance leaks by NSA whistleblower Edward Snowden.

But the report, which covers only surveillance orders issued in 2013, doesn't tell the whole story about how many individuals the spying targeted or how many Americans were caught in the surveillance that targeted foreigners. Civil liberties groups say the real number is likely "orders of magnitude" larger than this.

"Even if it was an honest definition of 'target'—that is, an individual instead of a group—that also is not encompassing those who are ancillary to a target and are caught up in the dragnet," says Kurt Opsahl, deputy general counsel of the Electronic Frontier Foundation.

The report, remarkably, shows that the government obtained just one order last year under Section 702 of FISA—which allows for bulk collection of data on foreigners—and that this one order covered 89,138 targets. But, as the report notes, "target" can refer to "an individual person, a group, an organization composed of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence information."

Furthermore, Section 702 orders are actually certificates issued by the FISA Court that can cover surveillance of an entire facility. And since, as the government points out in its report, the government cannot know how many people use a facility, the figure only "reflects an estimate of the number of known users of particular facilities (sometimes referred to as selectors) subject to intelligence collection under those Certifications," the report notes.

"If you're actually trying to get a sense of the number of human beings affected or the number of Americans affected, the number of people affected is vastly, vastly larger," says Julian Sanchez, senior fellow at the Cato Institute. "And how many of those are Americans is impossible to say. But [although] you may not think you are routinely communicating with foreign persons, [this] is not any kind of assurance that your communications are not part of the traffic subject to interception."

Sanchez points out that each individual targeted is likely communicating with dozens or hundred of others, whose communications will be picked up in the surveillance.

“And probably a lot of these targets are not individuals but entire web sites or companies. While [a company like the Chinese firm] Huawei might be a target, thousands of emails used by thousands of employees will be swept up.”

How many of those employees might be American or communicating with Americans is unknown.

The government’s estimate of the number of people affected by the surveillance order is only “based on the information readily available to the Intelligence Community to identify unique targets—users, whose identity may be unknown, but who are reasonably believed to use the particular facility from outside the United States and who are reasonably believed to be non-United States persons,” the government notes.

The EFF’s Opsahl says the information about the Section 702 order issued in 2013 is significant for what it doesn’t tell us about the particular targets or types of surveillance covered under these orders.

A single order affecting 89,000 people, for example, might involve collecting all of the Facebook communications or email of people involved in a particular organization or living in a particular country. But it might also involve collection of all internet activity from an upstream provider involving people in many organizations and countries or collection from satellite interceptions.

“It doesn’t seem possible you could have a focused order and achieve these statistics,” he notes. “And if the basis for doing [all of this collection] can be covered in just one order... it suggests that this order doesn’t have any limitations to groups, to countries, to whether it is a terrorism investigation or other forms of foreign intelligence, or any other [investigation] that you might imagine could be in an order.”

Phone Records

Also revealed in today’s report is the number of times the government has queried the controversial phone records database it created by collecting the phone records of every subscriber from U.S. providers.

According to the report, the government used 423 “selectors” to search its massive phone records database, which includes records going back to at least 2006 when the program began.

A search involves querying a specific phone number or device ID that appears in the database. The government has long maintained that its collection of phone records isn’t a violation of its authority, since it only views the records of specific individuals targeted in an investigation. But such searches, even if targeted at phone numbers used by foreigners, would include calls made to and from Americans as well as calls exchanged with people two or three hops out from the targeted number.

In its report, the government indicated that the 423 selectors involved just 248 “known or presumed” Americans whose information was collected by the agency in the database. But

Opsahl says that both of these numbers are deceptive given what we know about the database and how it's been used.

“We know it's affecting millions of people,” he points out. But “then we have estimated numbers of affected people [that are just] in the three digits. That requires some effort [on the government's part] to find a way to do the definition of the number [in such a way] to make it as small as possible.”

If analysts “are examining the records of people two or three hops out and as a result they get detailed looks at phone records of hundred or thousands of people, does that count as one [person] because they queried just one person but got their three hops [worth of data]?” he asks. “The only way of reconciling [the numbers in the report] with the information that was seen in other news reports and the realities of bulk collection, is that this is a number not of the people affected but a number related to how they are using the search tools.”

Over 19,000 Requests for Customer Data

One additional figure today's report covers is the number of National Security Letters the government issued last year to businesses to obtain data on account holders and users—19,212.

NSLs are written demands from the FBI that compel internet service providers, credit companies, financial institutions and others to hand over confidential records about their customers, such as subscriber information, phone numbers and e-mail addresses, websites visited, and more.

These letters are a powerful tool because they do not require court approval, and they come with a built-in gag order, preventing recipients from disclosing to anyone that they have received an NSL. An FBI agent looking into a possible anti-terrorism case can self-issue an NSL to a credit bureau, ISP, or phone company with only the sign-off of the Special Agent in Charge of their office. The FBI has merely to assert that the information is “relevant” to an investigation into international terrorism or clandestine intelligence activities.

The FBI has issued hundreds of thousands of NSLs over the years and has been reprimanded for abusing them. Last year a federal judge ruled that the use of NSLs is unconstitutional, due to the gag order that accompanies them, and ordered the government to stop using them. Her ruling, however, was stayed pending the government's appeal.

Although the FBI is required to submit an annual report to Congress about the number of NSLs it issues each year, today's transparency adds a detail to the FBI figure by disclosing the number of requests for data covered by each NSL that was issued. Since one NSL can involve requests for data about multiple accounts—such as an NSL sent to Google seeking information on three email accounts believed to be relevant to a single investigation—the government would count this as three requests.

According to the government's report today, the 19,000 NSLs issued last year involved more than 38,000 requests for information.