NSA monitoring US communications without a warrant, documents show

Thomas Gaist
21 June 2013

Classified top secret documents submitted to the secret Foreign Intelligence Surveillance Court by US Attorney General Eric Holder, published by *The Guardian* on Thursday, show that US Foreign Intelligence Surveillance Court (FISA) judges have approved sweeping general orders authorizing the National Security Agency (NSA) to monitor US communications data without individual warrants.

According to the *Guardian*, the documents—presumably obtained from NSA whistleblower Edward Snowden—"show that even under authorities governing the collection of foreign intelligence from foreign targets, US communications can still be collected, retained and used."

In their defense of the NSA surveillance programs, Obama administration officials—including Obama himself—have frequently and insistently declared that no communications of people in the US are monitored without a warrant. The documents released by *The Guardian* reveal these claims to be outright lies.

The FISA Court, the administration has claimed, provides oversight and "transparency" over the process. The actual procedures that the secret court has authorized have, until now, remained concealed from the population of the United States and the world.

Section 702 of the FISA Amendments Act (FAA) authorizes the NSA to engage in bulk data collection. Under this authorization, the NSA is supposedly only allowed to obtain communications without a warrant from "non-US persons." This includes any communications between people outside the US, and any communications from someone outside the US to someone within the US—if it is the "non-US person" who is the target of the snooping.

As previous revelations have shown, the US government has sucked up billions of communications from all over the world under this authorization, rubber stamped by the FISA Court. This global spying operation is separate from another program that collects virtually all phone records on anyone living in the United States through secret subpoenas to telecommunications companies.

The official limitations on NSA communications monitoring, however, have so many loopholes that they effectively allow for the agency and its analysts to spy on anyone, including those in the US, without a warrant—precisely as claimed by Snowden.

According to the documents, NSA personnel, using their "reasonable judgment," can keep and use "inadvertently acquired" domestic communications if (a) the data contain "significant foreign intelligence information," (b) the data are encrypted or "reasonably believed to contain secret meaning," (c) the data contain "evidence of a crime," or (d) the data contain information related to cyber security.

The court specifically states that encrypted emails can be kept for as long as needed to decrypt them.

According to the *Guardian*, moreover, while the procedures approved by the court require that interception stop if a communication is determined to involve only US persons, "these circumstances do not apply to large-scale data where the NSA claims it is unable to filter US communications from non-US ones." These communications can be retained, and presumably accessed, for five years.

In collecting communications, the NSA is allowed to examine a range of data on telephone and internet usage to determine whether a target is located in the US or not. To collect the communication, the individual analyst must have a "reasonable belief" that the target is outside the US.

When the NSA analyst is not able to determine

definitively the location of a target, he can simply assume that the target is overseas. “In the absence of specific information regarding whether a target is a United States person,” the FISA Court document states “a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person.”

In other words, the presumption is that a communication can be collected and monitored. If the NSA wants to wiretap anyone, anywhere, without a warrant, it merely has to declare—to itself—that it either does not know where the person is or has a reasonable belief that that person is outside the US.

Decisions about whether a person is considered US or non-US are made, according to the documents, on the basis of the “totality of circumstances,” specifically whether “the nature and circumstances of the person’s communications rise to a reasonable belief that such person is a United States person.”

One example of a condition which can be used to assert that someone is a not US person, and therefore all of his communications can be monitored, is if he is in contact with members of a “foreign-based political organization.”

Moreover, in ambiguous cases, NSA analysts are authorized to examine the content of communications in order to determine whether that content qualifies for surveillance: “NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.”

US persons are thus “protected” from surveillance by having the content of their communications surveilled, supposedly to determine whether they are US persons.

In its final section, “Departure from Procedures,” the document on procedures for targeting non-US persons includes an escape clause, allowing the NSA to ignore all legal protections under exceptional circumstances, “If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action.”

This is a blueprint for universal accumulation and indefinite retention of all communications of everyone in the world.