

New documents highlight sweeping NSA surveillance powers at home and abroad

Thomas Gaist
2 July 2014

Documents released by Edward Snowden, reported Tuesday in the *Washington Post*, show that the US government has granted the National Security Agency sweeping authorization to engage in mass spying worldwide.

According to the *Post*, a “classified legal certification” from 2010 and other documents leaked by Snowden show that the Foreign Intelligence Surveillance Court (FISC) authorized US intelligence to carry out unrestrained surveillance activities targeting at least 193 countries worldwide—every country except Australia, the UK, Canada, and New Zealand. The legal certification also authorized NSA surveillance against international institutions including the European Union, the International Monetary Fund, the International Atomic Energy Agency, and the World Bank.

Jennifer Granick of the Stanford Center for Internet and Society said of the 2010 document, “The breadth of the certification suggests that the court is authorizing the government to spy on average foreigners and doesn’t exercise much if any control beyond that.”

A 2010 affidavit in support of the certification authorizing surveillance of foreigners states that foreigners who “possess, are expected to receive and/or are likely to communicate foreign intelligence information” can be targeted. Such a definition can clearly be used to target foreigners, including journalists and academics, virtually at will, as well as their contacts within the US. A report from the office of the Director of National Intelligence released Friday confirmed that the US government surveilled at least 90,000 foreign targets in 2013.

The vague concept of “foreign intelligence information” makes practically any foreign communication a potential surveillance target, while

also giving the intelligence agencies a back door to access the constitutionally protected communications of US citizens.

In what is known as “about the target” collection, the NSA has been acquiring communications on the basis that they merely include the e-mail address of another targeted internet user. This requires that the NSA accumulate and have the ability to search all e-mail communications.

Another recent report by researchers at Harvard University and Boston College, “Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad,” found that loopholes in the legal framework governing surveillance leave US citizens “as vulnerable” as foreigners to the data collection efforts of the US government.

The report found that the NSA re-routes US data to locations outside the country as a means of “circumventing constitutional and statutory safeguards seeking to protect the privacy of Americans.” Legal rationalization for this practice stems from Executive Order 12333 (EO12333) and United States Signals Intelligence Directive SP0018 (USSID18), statutes that were drawn up and approved within the executive branch. According to the Electronic Frontier Foundation, USSID18 is “littered with loopholes” that allow the intelligence agencies to “over-collect, over-retain, and over-share Americans’ communications—all without a probable cause warrant or any judicial oversight.”

Together with EO12333, USSID18 effectively enables mass collection of data from US targets without a warrant. The NSA’s Operation MUSCULAR, which collects millions of files of data from Yahoo! and Google data centers and transmits them to agency

headquarters in Fort Meade, Maryland, operates on the basis of EO12333 and USSID18 and the loopholes they contain.

EO12333 also authorizes deliberate re-routing of communications “to ensure that traffic between US endpoints takes an unusual path through a device located abroad,” according to the study. Renesys, an internet monitoring firm, found multiple instances of such “route hijacking” in 2013, in which US intelligence re-directed internet activity through countries such as Iceland and Belarus, where it could be surveilled under the pseudo-legal regulations set forth in EO12333.

The NSA says that EO12333 is the “primary legal authority” for its surveillance activities. This is significant because while the more widely known legal authorizations of surveillance, Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA) were established with congressional authorization, EO12333 is strictly a creation of the executive branch.

Within the framework of Executive Order 12333, the Obama administration has developed a secret guideline, the Special Procedures Governing Communications Metadata Analysis, which authorizes the NSA to generate social networks mapping the relationships of US and non-US citizens on the basis of their communications data.

EO12333 was signed in December of 1981 by President Ronald Reagan, to expand the powers of the Central Intelligence Agency (CIA) and other intelligence bureaucracies. USSID18 was issued as a secret “letter of promulgation” by the NSA in July 1993, with the now publicly available copy remaining highly redacted.

In other words, even if Congress rescinded all of its legislation authorizing surveillance, the NSA could still claim blanket powers to engage in mass data collection on the basis of secretive decrees issued from inside the executive branch and by its own administration.

More NSA bombshells can be expected in the immediate future. Glenn Greenwald of the *Intercept* delayed release of his latest story on NSA surveillance, rumored to contain names of US citizens targeted by US surveillance, in response to undisclosed claims by the US government about the content of the expose.

About one year out from the initial Snowden

exposures, all claims to the effect that the surveillance programs are narrowly targeted and subject to rigorous legal and political control have been thoroughly discredited. Operating on the basis of secret legal authorizations and executive orders, the NSA is using every conceivable tactic to overcome and render impotent constitutional protections against warrantless spying.



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact