

New revelations expose fraud of congressional, court oversight of NSA spying

Thomas Gaist
17 August 2013

An internal audit of National Security Agency (NSA) activities dated May 2012, leaked earlier this summer by former NSA contractor Edward Snowden and published Friday by the *Washington Post*, found 2,776 violations of rules governing NSA surveillance over the previous twelve months. Unauthorized data collection of legally protected private communications accounted for most of the violations.

The audit detailed major violations of the rules that supposedly reign in NSA surveillance. The *Post* wrote that “the more serious lapses include unauthorized access to intercepted communications, the distribution of protected content, and the use of automated systems without built-in safeguards to prevent unlawful surveillance.”

The audit covered only the NSA’s headquarters in Fort Meade, Maryland and its facilities in Washington DC. An audit that took into account all of the agency’s far-flung outposts would produce a far higher number of violations.

According to the *Post* article, the audit showed that violations are occurring at an increasing rate.

The audit was made available neither to Congress nor to the Foreign Intelligence Surveillance Court (FISC), the secret court that nominally oversees NSA spying on Americans.

The revelations detailed in the *Post* confirm Edward Snowden’s claim that the world’s communications are at the fingertips of NSA analysts, who can quickly access data on practically anyone from their workstations. A large number of the reported violations involve ordinary analysts summoning up communications that have been seized in mass dragnets and stored in vast databases, and reading or listening to them.

The claim repeatedly made by the Obama administration, US intelligence officials and lawmakers of both parties that it is extremely difficult to get to the data and that innocent people’s communications are protected by legal and technological barriers from direct access by intelligence analysts lies in tatters.

Once again, top US officials, beginning with President

Barack Obama, have been caught in outright lies. Just one week before the *Post* exposures, Obama gave a press conference in which he declared, “America is not interested in spying on ordinary people.”

He went on to assert that no abuses of laws or guidelines governing the NSA spy programs have been revealed. “If you look at the reports,” he said, “all the stories that have been written, what you’re not reading about is the government actually abusing these programs and listening in on people’s phone calls or inappropriately reading people’s emails.

“What you’re hearing about is the prospect that these could be abused. Now, part of the reason they’re not abused is because these checks are in place...”

Last June, Deputy Attorney General James Cole, testifying before Congress, said of NSA violations, “Every now and then, there may be a mistake.”

NSA Director Gen. Keith Alexander last year declared, “We don’t hold data on US citizens.”

The violations listed in the audit involve NSA analysts trolling through streams of communications data, fishing for phone calls and messages on the basis of a general keyword or area code. In one case, NSA analysts in Hawaii used a surveillance system called DISHFIRE to acquire all communications using the words “radar” or “radio” and “Ericsson.”

The NSA audit states that 1 in 10 incidents of unauthorized data surveillance occurs because an analyst types in a wrong number. In one such incident from 2008, an analyst intercepted numerous telephone calls from Washington DC by typing “202,” the Washington area code, instead of “20,” the international country code for Egypt.

The *Post* also cites “unauthorized use of data about more than 3,000 Americans and green card holders.” It notes a case in which the NSA carried out a new collection method, knowing that it vacuumed up the emails of Americans along with those of non-Americans, without even notifying the FISC, which was unaware of the data collection program for months.

The program was based on redirecting massive flows of international data streaming through American fiber-optic cables into a data reservoir for examination. The program was rejected by the FISA court in October 2011, long after it had begun systematic data accumulation.

The article also describes how analysts are trained, by means of mandatory tutorials, to provide only the bare minimum of information when they fill out oversight forms. The NSA's "Target Analyst Rationale Instructions" enjoin NSA agents to exclude "extraneous information" and "strip out details and substitute generic descriptions of the evidence and analysis behind their targeting choices."

The overall number of incidents reported in the audit does not reflect the scale of snooping carried out by the NSA that violates the agency's own rules and the token legal restrictions contained in the 2008 FISA Amendments Act (FAA), which expanded the authority of the NSA to carry out domestic surveillance.

Each single "incident" can reflect an action file that contains hundreds of thousands or millions of records of Americans' telephone calls. Under the NSA auditing framework, the sort of incident accounts published by the *Post* do not detail the number of Americans affected by the violations.

Under official NSA guidelines, moreover, "incidental" acquisition of legally protected communication data by agents engaged in data mining is not considered a violation of agency rules. "Incidentally" acquired data is stored and becomes part of the NSA's massive database.

As the *Washington Post* writes: "The NSA uses the term 'incidental' when it sweeps up the records of an American while targeting a foreigner or a US person who is believed to be involved in terrorism. Official guidelines for NSA personnel say that kind of incident, pervasive under current practices, 'does not constitute a...violation' and 'does not have to be reported' to the NSA inspector general for inclusion in quarterly reports to Congress. Once added to its databases, absent other restrictions, the communications of Americans may be searched freely."

The focus on "abuses" itself obscures the central problem with the NSA spying programs, which is not "violations" but the programs themselves, and the very existence of a secret spy agency that is, for all practical purposes, above the law. All of the operations that have been exposed by Snowden, and the many others that have not been revealed, directly violate the Fourth Amendment to the US Constitution, which requires specific warrants based on probable cause, and bans "unreasonable" searches and seizures. The Fourth Amendment, part of the Constitution's Bill of Rights—which all presidents are sworn to uphold—specifically bars precisely the type of mass seizures

of private information that the NSA is carrying out on a daily basis.

The unconstitutional spying carried out by the NSA was given full sanction by Congress in 2008 when it passed the FAA. The expanded powers of the intelligence agency were supposedly to be held in check by increased congressional oversight.

The FAA passed in both houses of Congress by comfortable majorities, underscoring the bipartisan support for illegal spying on the American people. In late 2012, with the full support of the Obama White House, the House of Representatives voted 301 to 118 to extend the FAA and the Senate followed suit, voting 73 to 23.

The farcical character of congressional oversight is spelled out in the FAA, which requires the NSA to submit unclassified versions of semiannual reports to Congress. These contain large blacked-out portions. If lawmakers want to read the unredacted documents, they must do so in a special, secured room, and they are not allowed to take notes.

That Congress submits to this humiliating procedure shows not only the domination of the government by the military-intelligence apparatus, but Congress's willing prostration and lack of any serious commitment to democratic processes.

Leading Democrats as well as Republicans sprang to the defense of the NSA following the *Post*'s revelations on Friday. Dianne Feinstein, the Democratic chairwoman of the Senate Intelligence Committee, issued a statement saying, "As I have said previously, the committee has never identified an instance in which the NSA has intentionally abused its authority to conduct surveillance for inappropriate purposes."

This pretense that the NSA is guilty of nothing more than human error and unintentional "mistakes" is itself a conscious lie and an insult to the intelligence of the American people.

The NSA material published in the *Post* shows that the whole framework of FISA court and congressional oversight is itself a fraud, which was never intended to be anything other than a legal fig leaf for pervasive illegal and unconstitutional spying on the American people.



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact