US intelligence agencies expand electronic surveillance worldwide

Thomas Gaist
6 May 2016

The US National Security Agency and Central Intelligence Agency approximately doubled their surveillance of telephone and electronic communications in 2015, according to documents released in a US government "transparency report" this week.

US intelligence analysts carried out some 25,000 analytical searches of archived communications data derived from the NSA's sweeping data collection programs last year, including nearly 5,000 searches of data collected from communications by US citizens.

The figure represents a more than twofold increase over 2013, which saw the agencies conduct 9,500 searches of the surveillance database.

Neither the NSA nor CIA is, in theory, authorized to conduct domestic spying operations. Nonetheless, the CIA searched some 2,000 US communications, while the NSA searched nearly 200.

No statistics are provided covering surveillance database searches by the Federal Bureau of Investigation (FBI). The documents do reveal, however, that the FBI issued nearly 50,000 national security letters (NSLs), special memos used by the security apparatus to demand access to contents of private communications from providers in 2015, according to the transparency report.

The NSLs are binding and compel the recipient to maintain total secrecy about the government's demands for information.

The surge in US government surveillance activity has been accompanied by a legal and political offensive, spearheaded by the Obama administration and the military-intelligence bureaucracy, aimed at further eroding the democratic protections enshrined in Bill of Rights.

As a FISA court judge noted in a secret opinion declassified this week, the military-intelligence apparatus is pushing for statutory changes that "would allow the NSA and CIA to deviate from any restrictions based upon unspecified 'mandates.'"

The secret FISA order declassified Tuesday, dated November 6, 2015 states: "The FBI, NSA, and CIA all have access to 'raw,' or unminimized, information under Section 702

"The NSA and CIA Minimization Procedures included as part of the July 15, 2015 Submission each contain new language stating that 'nothing in these procedures shall prohibit the retention, processing, or dissemination of information.'"

NSA and CIA are authorized to surveil and analyze any data considered "reasonably necessary" to carry out the agencies' "legislative mandate," the document states.

The latest exposures of the US government's mass spying operations come just days after the US Supreme Court approved changes to an obscure statute, known as Rule 41 of the Federal Rule of Criminal Procedure, which covers the application of the Fourth Amendment to electronic spying by federal agents.

The changes to Rule 41 grant US government operatives essentially limitless authority to hack into, surveil and implant malware into computers and networks anywhere in the world.

According to a letter by Google law enforcement head Richard Salgado, the changes enable "various forms of hacking," known in the technical jargon as "remote search techniques," which are essentially hi-tech trojan horse programs that allow agents to manipulate, search, and extract data from infected machines.

Malware-based surveillance is "more invasive than other searches because they often have unknown,

widespread and destructive consequences," Salgado said.

While the rule previously held that state operatives must acquire a specific warrant authorizing a search of clearly defined contents on a given machine, new language allows investigators to deploy surveillance and hacking technology against as many machines and search as many contents as they deem necessary for a given investigation, all on the basis of a single warrant by a single district judge.

The changes state: "A magistrate judge, with authority in any district where activities related to a crime may have occurred, has authority to issue a warrant to use remote access to search electronic storage media, and to seize or copy electronically stored information located within or outside that district."

"The amendment would eliminate the burden of attempting to secure multiple warrants in numerous districts and allow a single judge to oversee the investigation," the new language states.

"We could definitely see the government go forum-shopping for judges. The bigger question here is should the government be engaged in hacking at all, and, if so, what should the rules of the road be? That's something Congress should decide," said Robyn Greene of New America's Open Technology Institute.

The Rule 41 changes were proposed in May 2015 by the Committee on Rules of Practice and Procedure and given final approval by a panel of officials and experts, including the high court, last week.

US Senator Ron Wyden, who recently warned that the new statute is "not just a garden-variety federal rule change," and that "we're talking about mass hacks," has called for Congress to review the hacking rules.

Wyden is one of a group of leading congressmen who have become vocal advocates on behalf of "surveillance reform," in an effort to appease popular opposition to spying that erupted after the Snowden revelations broke in June 2013, while directing it into safe channels..

In similarly demagogic remarks, Democratic Senator Charles Schumer of New York recently warned an audience that the NSA is spying on them out of city billboards.

"New spying billboards are being installed across the country, including right here in New York City, and they are being used to collect your mobile-phone data," Schumer told an audience in Times Square. "They have huge amounts of information on you. Who knows what they could use it for? It's something straight out of a scary movie," Schumer said.

Despite his posture of opposition to the spying, however, Schumer made clear that he fully accepts the spying operations.

"We have to move a little bit on the liberty side," he said. "The wholesale elimination of the [NSA surveillance] program, I think, leaves us too naked in terms of security, and you've got to have security as well as liberty."

The claim that mass spying is necessary to protect Americans' liberty against "Islamic extremism," propagated by the state and media establishment and parroted dutifully by liberal and libertarian advocates of surveillance reform alike, is a lie.

The universal acceptance of this lie by the leading promoters of surveillance reform makes clear that the "reform" agenda is little more than a dog-and-pony show, orchestrated by the Obama administration and members of both parties, aimed at restoring a facade of legitimacy to spy programs that have been utterly discredited in the eyes of millions since 2013.

More than a century of historical experience shows that spying on communications by the capitalist state is aimed, above all, at identifying, profiling, and monitoring groups and individuals considered by the state to be threats to the bourgeois order.

The most powerful agencies of the US government are working overtime to assemble dossiers on the views and relations of a population that is becoming increasingly radicalized politically in response to the capitalist crisis.