

Vast majority of those spied on by NSA are non-suspects

New revelations shatter US government lies on illegal surveillance

Thomas Gaist
7 July 2014

The overwhelming majority of individuals who have had their emails and other private communications intercepted by the US National Security Agency (NSA) have not been singled out for surveillance as suspected terrorists, according to a report in Sunday's *Washington Post*. This includes tens or perhaps hundreds of thousands of US citizens who were monitored without a warrant or any semblance of judicial oversight.

The report, based on documents provided by whistleblower Edward Snowden, concerns not just metadata, but the actual content of communications. The revelations expose the lies not only of US intelligence officials, but also President Barack Obama, who has repeatedly assured the public that the NSA is "not allowed" to access the content of communications, and that "Nobody is listening to your telephone calls."

The *Post* analysis is based on a review of 160,000 emails and instant messages, more than 5,000 private photos, and 7,900 documents extracted from 11,000 Internet accounts by the NSA during surveillance operations lasting between 2009 and 2012. It is only one part of a vast dragnet of illegal spy programs run by the agency and its counterparts internationally.

The *Post* reports that 9 out of 10 affected account holders had their communications collected "incidentally" in the course of surveillance.

According to the newspaper, "Nearly half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to US citizens or residents. NSA analysts masked, or "minimized," more than 65,000 such references to protect Americans' privacy, but the *Post* found nearly 900 additional email

addresses, unmasked in the files, that could be strongly linked to US citizens or US residents."

In May, former NSA Director General Keith Alexander denied that Snowden, while working as an NSA contractor, had access to the content of communications acquired on the basis of the Foreign Intelligence Surveillance Act (FISA). "He didn't get this data... That database, he didn't have access to," Alexander said.

In an interview, however, Snowden made clear that as an analyst he had wide latitude to search the content of communications of virtually anyone, and that he was given "broad, unescorted access to raw SIGINT [signals intelligence]."

"If I had wanted to pull a copy of a judge's or a senator's email, all I had to do was enter that selector into XKEYSCORE," Snowden said.

Extrapolating from the data sample furnished by Snowden, the *Post* estimated that at least 900,000 Internet accounts have been swept up by the NSA without being specifically targeted as part of an investigation. The NSA refuses to release its own estimate of the number of individuals it has "incidentally" surveilled through the use of dragnet surveillance techniques.

The files show that the NSA collected and archived numerous types of personal data, including private medical records, résumés, academic transcripts, and private photos of children and of romantic liaisons. The surveilled communications, the *Post* said, were characterized by a "startlingly intimate, even voyeuristic quality," and included "stories of love and heartbreak, illicit sexual liaisons, mental health crises, political and religious conversions, financial anxieties

and disappointed hopes.”

“The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless,” the *Post* wrote.

One example highlighted by the report involved 800 pages of emotionally fraught communications, retained by the NSA and the Australian Signals Directorate (ASD), between a man seeking to join the Taliban and his romantic interest in Australia.

The rampant warrantless spying is an expression of the expansion of the powers of the US surveillance state over the past decade, especially since the economic crisis of 2008. As the *Post* noted, since the passage of the 2008 FISA Amendments Act, the NSA has moved to “make freer use of methods that for 30 years had required probable cause and a warrant from a judge.”

Dragnet surveillance practices employed by the NSA include taking data from every user who messages a given chat room—and even from “lurkers” who passively visit without posting—once that chat room has been associated with a single target. The NSA directly targets IP addresses of servers accessed by hundreds of Internet users, a practice that makes mass “incidental” data acquisition inevitable.

The Snowden leaks show that people who use an IP address located or even suspected to be located outside the US are assumed to be non-US citizens. In one case, a user was labeled a non-US citizen merely because he wrote emails in a foreign language.

If NSA analysts are unable to attain a FISA warrant, NSA agents simply turn to other methods to acquire desired data, the *Post* report shows. In their internal communications, NSA analysts referred favorably to the “lower threshold for foreignness ‘standard of proof’” associated with the PRISM and Upstream programs (which require only “reasonable belief” on the part of the agent) in comparison to that of standard FISA warrants.

That the NSA flouts even the authority of the FISA Court, an authoritarian shadow court developed to provide “legal” cover for the operations of the intelligence and military bureaucracies, is indicative of the lawlessness prevailing at the heights of the US government.

As the *Post* noted, “When NSA and allied analysts really want to target an account, their concern for US

privacy diminishes. The rationales they use to judge foreignness sometimes stretch legal rules or well-known technical facts to the breaking point.”

Even the executive branch of the US government does not escape the NSA’s dragnet. NSA data indicates that the communications of President Barack Obama, prior to and following his inauguration, were being acquired by the agency. The files leaked by Snowden show references to a “minimized US president-elect,” and more than 1,200 references to a “minimized US president.”

“Minimization” procedures have been touted for supposedly removing incidentally collected content, thereby preventing long-term storage of personal data about ordinary citizens. The latest revelations make clear that whatever the treatment of the president’s correspondence, communications sent by the general population and completely unrelated to anything resembling terrorism are being retained by the NSA, in large quantities and for indefinite duration.

The *Post* article itself points to the complicity of the media in covering up and excusing the crimes of the surveillance state. The authors reveal that the content of their article was reviewed by the CIA.

The newspaper reports that the leaks include “discoveries of considerable intelligence value” that aided in the capture of Muhammad Tahir Shahzad and Umar Patek, the former a “Pakistan-based bomb builder” and the latter “a suspect in a 2002 terrorist bombing” on Bali. No further information on these cases is offered, and the article states, “At the request of CIA officials, the *Post* is withholding other examples that officials said would compromise ongoing operations.”

The data also contains revelations relating to military, security and cyber-warfare issues. The *Post* insists that it will not reveal details on these matters, another decision no doubt made in consultation with the CIA.



To contact the WSWP and the
Socialist Equality Party visit:

wsws.org/contact