



Written by [C. Mitchell Shaw](#) on June 23, 2017

Surveillance State Employee Violated Law Hundreds of Times With Illegal Searches

A heavily redacted report from 2014 released Wednesday shows that a senior security database program officer at the Office of the Director of National Intelligence (ODNI) routinely violated both department policy and the law by performing illegal surveillance database searches more than 600 times, among other violations.



The report — obtained and [made public](#) Wednesday by BuzzFeed journalist Jason Leopold — is a product of the Office of the Inspector General of the Intelligence Community from late 2014. It shows a litany of illegalities and abuses by a female employee whose name is redacted. That employee — hired May of 2010 at over \$84,000 per year — used the Joint Personnel Adjudication System (JPAS) database to perform 636 unauthorized searches of data on individuals, searched her own name 442 times, held 14 part-time security consulting jobs while working at ODNI, downloaded “several unauthorized executable files (programs) including game programs” to ODNI computers, spent four to six hours a day on Facebook or playing video games, and engaged in sexually explicit video chats via the IBM Sametime platform while at work.

While employees slacking off or violating policy is certainly not unheard of, one has to wonder if this employee ever performed a minute’s work for her more than \$84,000 salary. It appears that her major contribution to the cause of “national security” was getting caught rifling through files to which she had unrestrained access, but no authorization to access. The system, it appears, is designed for abuse.

Setting aside for the moment everything except her abuse of the privacy of individuals, this report dismantles the oft-repeated claim by surveillance hawks that abuses of the databases are rare and accidental. After the 32-page report was made public, famed NSA leaker Ed Snowden [Tweeted](#), “When you hear politicians say @NSAGov, @CIA and @FBI never ‘willfully’ abuse their access, remember just one employee did it 600 times.” Of course, Snowden had reasons beyond his love of privacy and liberty for pointing that out. He also had a reason closer to home. The employee mentioned in the report



Written by [C. Mitchell Shaw](#) on June 23, 2017

(whose name is redacted) performed 357 searches on Snowden.

Snowden makes a good point: More than 600 illegal searches by one employee is not accidental. Neither is it rare. While this report focuses on one employee who may or may not take the cake for the most abuses, she is far from alone. In fact, this problem has been known — and largely ignored — for years. In August 2013, *Bloomberg* reported that the Senate Intelligence Committee was investigating “about a dozen cases” involving “improper behavior on the part of the individual employees” accessing collected surveillance data in an unauthorized manner.

In a statement released to *Bloomberg* at the time of that article, the NSA said, “Over the past decade, very rare instances of willful violations of NSA’s authorities have been found.” That statement also said, “NSA takes very seriously allegations of misconduct and cooperates fully with any investigations — responding as appropriate. NSA has zero tolerance for willful violations of the agency’s authorities.”

Right.

Because as *Bloomberg* reported:

This new information, of course, contravenes with another statement made by General Keith Alexander, director of the NSA. Earlier this month he said that absolutely no one had willfully or knowingly disobeyed the law “or tried to invade your civil liberties or privacy.”

Another misleading statement came from president Obama just a few days ago, when he claimed that he was confident no one at the NSA was trying to abuse this surveillance program or listen in on people’s e-mails and communications.

So, while the NSA and President Obama were claiming that no one was willfully or knowingly breaking the law or invading the privacy of the people whose communications and other personal data are routinely sucked up by the surveillance apparatus of the surveillance state, they were lying and they knew it. This newly released report serves to reinforce that 636 times.

In fact, the problem is so pervasive, so common that subsets of it have even been named. In the intelligence community, certain types of intelligence are called by unique titles to distinguish the various types of intelligence that is gathered. For instance, intelligence gathering by interception of signals (radio, telegraph, satellite, etc.) is known as SIGINT, for Signals Intelligence. Likewise Communications Intelligence is called COMINT and Electronic Intelligence is called ELINT. The problem of NSA analysts and spies as well as others using their access to surveillance databases for the purpose of violating the privacy of husbands, wives, boyfriends, girlfriends, and other “love interests” is so well known that it has been internally tagged as LOVEINT.

LOVEINT first really came to light as a result of the Senate Intelligence Committee’s investigation mentioned above. A number of those dozen or so cases the committee was investigating involved LOVEINT. As *Slate* reported at the time:

The letter sent to Grassley reveals that there have been at least 12 recorded cases of spies abusing their powers since 2003, with several of these cases involving LOVINT. In 2011, one NSA employee working at an overseas base spied on the calls of her foreign boyfriend and other foreigners she met socially because she wanted to find out if they were “shady characters.” In 2004, an NSA spy monitored the calls of a foreign number she found in her husband’s cellphone because she suspected he had been unfaithful. In 2003, an NSA employee was internally investigated after a woman with whom he had a sexual relationship reported him to the government because she



Written by [C. Mitchell Shaw](#) on June 23, 2017

suspected he was monitoring her calls. An investigation revealed that over a period of five years, the employee had unlawfully monitored nine phone numbers associated with female foreign nationals. In each of these three cases there was no prosecution or disciplinary action taken because the NSA staff involved in the abuses resigned.

Is that what the NSA considers “zero tolerance” of willfully violating both policy and the law? Because, if it is, the good folks over at the NSA need to look up the definition of “zero tolerance.”

The *Slate* article also mentioned “at least six other” cases of LOVEINT, including a spy who “entered six email addresses used by an American ex-girlfriend into a surveillance system on the first day he gained access to it” and another spy who “monitored the phone calls of his foreign girlfriend for a month.”

Slate also reported:

The worst punishment that was handed out in any of these cases was a reduction in pay for two months, a reduction in grade, and access to classified information being revoked. One LOVEINT case was referred to the Justice Department in 2011 — but it declined to prosecute. The inspector general’s letter says that two investigations are currently ongoing into alleged misuse of NSA spy systems, and one allegation is being reviewed for possible investigation.

One does not bother to name an anomaly. That there is even such a thing as LOVEINT indicates that there is a problem — no matter how much the surveillance hawks in politics and intelligence want to pretend otherwise.

The Office of the Director of National Intelligence was created as a Cabinet-level office in 2004 as part of the Intelligence Reform and Terrorism Prevention Act of 2004 to serve as a gatekeeper of accountability over the 16 U.S. intelligence agencies. As this newly released report shows, having ODNI oversee the intelligence agencies that make up the surveillance state — the Deep State — is exactly like having a prisoner run a prison.

As stated above, it appears the system is designed for abuse. The real problem is not that people will abuse the power given to them; it is that there is simply too much power in the surveillance state to begin with. If you build an all-powerful surveillance state equipped with nearly limitless surveillance apparatus, it will be abused. This case simply proves what did not need proving.

It is past time to dismantle the surveillance state and the apparatus it uses to spy on people. Besides the fact that the surveillance state can’t be trusted, it is a clear violation of the God-given rights protected by the Fourth Amendment.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

Subscribe