



Written by [C. Mitchell Shaw](#) on May 25, 2017

## Declassified Docs: NSA Routinely Violates Rules Protecting Privacy of Americans

Under the pretext of the war on terror, the surveillance state has continued to grow in the years since 9/11. And while claiming a series of checks and balances to give the surveillance state a veneer of credibility, the truth is that — as a recent report shows — the surveillance hawks continue to violate even those scant rules they are supposed to follow.



The NSA is forbidden by law to conduct surveillance on American citizens living stateside, but the very nature of mass surveillance means that those citizens routinely get swept up in the surveillance that captures everything from computer browsing histories to e-mails, from text messages to phone calls, from GPS locations to social-media posts, and everything in between. When — which is frequently — Americans living stateside have their data vacuumed up by the NSA's various and sundry surveillance programs, that information is stored in what is known as the Section 702 database. It is only supposed to be accessible under very specific conditions.

There are at least two major problems with data collection under [Section 702](#). The first is that the NSA gets to interpret its own rules. As a result of that, the agency has historically interpreted the prohibition against targeting Americans to mean that as long as 51 percent of the data collection is foreign, the 49 percent of data that is domestic is fair game. The second problem — as mentioned above — is that the NSA and other agencies routinely access the domestic data, even when the rules forbid that access.

As Circa [reported](#) Wednesday, newly declassified documents reveal a pattern of violating the privacy of American citizens: “The National Security Agency under former President Barack Obama routinely violated American privacy protections while scouring through overseas intercepts and failed to disclose the extent of the problems until the final days before Donald Trump was elected president last fall, according to once top-secret documents that chronicle some of the most serious constitutional abuses to date by the U.S. intelligence community.”

While it is self-evident that this surveillance should not be happening in the first place, it is also a reality that it is. Given that the surveillance is one issue and access to the data is a separate (but related) issue, let's just focus on the latter of the two. Perhaps — and that is probably a stretch — it would be reasonable if an occasional search of the database violated the rules. That could be seen as an



Written by [C. Mitchell Shaw](#) on May 25, 2017

anomaly and treated as an isolated incident. But this is not that. According to those “once top-secret documents,” the violations are far from anomalous; they approach the norm. As Circa reported, “More than 5 percent, or one out of every 20 searches seeking upstream Internet data on Americans inside the NSA’s so-called Section 702 database violated the safeguards Obama and his intelligence chiefs vowed to follow in 2011, according to one classified internal report reviewed by Circa.”

Let’s try to put that in perspective. If a police officer violated departmental regulations concerning something as basic as chain of custody for evidence, or use of force, or serving a warrant in one out of every twenty cases, the media and the community would call for his badge and probably for his conviction. This is more like an entire police department doing that. One out of twenty is not an accident; it is a pattern showing careless disregard for the rules. This is not an isolated incident; it is indicative of a systemic problem.

The Obama administration revealed the violations to the Foreign Intelligence Surveillance Court on October 26. That self-disclosure — in a closed-door session — was just before the election and was likely intended to appear to be above-board before the next president — which was already likely to be Donald Trump — took office.

The FISA court, which customarily rubber-stamps the actions of the surveillance state, was more stringent this time. In a recently unsealed court document dated April 26, 2017, the court censured the administration for not revealing the violations sooner, calling that lack of disclosure an “institutional lack of candor.” The court document also said that the improper searches were a “very serious Fourth Amendment issue.”

Furthermore, the increase in illegally accessing the private data of Americans was coupled with an increase in “unmasking” Americans. “Unmasking” is a term used to describe the process of identifying people whose data is “accidentally” swept up by surveillance programs. The NSA routinely conducts surveillance that it knows will “accidentally” include the communications, locations, and other data of American citizens living stateside. When that happens, the NSA is required by law to “mask” (redact) the names and other personally identifiable data of those Americans.

Theoretically, that “masking” process is supposed to protect the rights and identities of Americans; in practice, it does little more than add a small speed-bump on the road to the surveillance state. Beginning in 2011, President Obama made it easier — by executive orders approved by the United States Foreign Surveillance Court (FISC) — to “unmask” American citizens. While the ostensible reason for Obama’s orders was to make it easier to fight terrorism, the net effect of those orders was the dismantling of yet another layer of legal protection preventing the NSA from doing what it is not supposed to do: spy on American citizens.

Senator Rand Paul (R-Ky.) told Fox News Wednesday that the Obama administration appears to have deliberately increased the number of Americans who were unmasked. He added, “If we determine this to be true, this is an enormous abuse of power.” Paul went on to say, “This will dwarf all other stories” since it involves “hundreds and hundreds of people.”

Paul is correct. If anything, he is understating the size and scope of the abuses of the surveillance state. A [previous report](#) showed: “In all, government officials conducted 30,355 searches in 2016 seeking information about Americans in NSA intercept metadata, which include telephone numbers and e-mail addresses. The activity amounted to a 27.5 percent increase over the prior year and more than triple the 9,500 such searches that occurred in 2013, the first year such data was kept. The government in



Written by [C. Mitchell Shaw](#) on May 25, 2017

---

2016 also scoured the actual contents of NSA intercepted calls and e-mails for 5,288 Americans, an increase of 13 percent over the prior year and a massive spike from the 198 names searched in 2013.”

As a result of those 30,355 searches, 3,134 NSA intelligence reports unmasked Americans who should have been afforded privacy protections under the rules, not to mention under the Fourth Amendment. This most recent revelation confirms that the surveillance hawks cannot be trusted to keep even the rules they set for themselves.



## 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.



**Subscribe**

### 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.