State sanctioned secrecy: NSA's criminality shield

Patrick G. Eddington

September 11, 2020

Last week, the U.S. Court of Appeals for the 9th Circuit ruled that the National Security Agency (NSA) telephone metadata program first exposed in June 2013 by whistleblower Edward Snowden "…may have violated the Fourth Amendment and did violate the Foreign Intelligence Surveillance Act ("FISA") when it collected the telephony metadata of millions of Americans…" The program was repeatedly reauthorized by Congress before finally (allegedly) being shelved in 2019, despite a Trump administration effort to revive legal authority for it. Snowden recognized the program's inherent criminality and unconstitutional character, which is precisely why he exposed it — and why all pending federal charges against him should be dismissed with prejudice.

Unfortunately, NSA still has a critical legal tool to hide other criminal or unconstitutional acts: the six-decade old National Security Agency (NSA) Act of 1959 (P. L. 86-36).

Enacted at the height of the Cold War, the NSA Act gives the agency radically sweeping powers to withhold *any* information from public disclosure. Specifically, Section 6 of the Act states "…nothing in this Act or any other law…shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency."

NSA has used that blanket authority to try to keep secret details about its lethal 9/11 intelligence failure. A Freedom of Information Act (FOIA) lawsuit I brought on behalf of the Cato Institute against the Defense Department (NSA's parent organization) in January 2017 has, after over three-and-a-half years in federal court, partially punctured NSA's veil of secrecy over the cancelled TRAILBLAZER and THINTHREAD digital network exploitation (DNE) programs.

In brief, during the five-year period leading up to the 9/11 attacks, a bureaucratic war raged inside of NSA over the best way to handle the exploding volume of digital communications the agency was trying to keep up with. On one side was a group of veteran NSA cryptographers, mathematicians and computer scientists who developed a cheap, extremely effective, and Constitutionally compliant in-house DNE system codenamed THINTHREAD. On the other side was then-NSA Director Michael Hayden, who favored an unproven, external, contractor developed DNE system called TRAILBLAZER. When then-GOP House Intelligence Committee staffer Diane Roark got the THINTHREAD team development money and language in the FY 2002 Intelligence Authorization bill directing wider deployment of the cheaper, off-the-shelf

THINTHREAD system, Hayden refused to deploy it as directed — even though THINTHREAD, still in prototype development, was already producing intelligence NSA couldn't get from any of its other existing systems.

Three weeks before the 9/11 attacks, Hayden killed further THINTHREAD development, despite the fact that TRAILBLAZER was still little more than an idea on PowerPoint slides. The former THINTHREAD team members believe to this day that had their system been deployed even a few weeks before the 9/11 attacks, bin Laden's hijackers would never have made it onto a single plane. I agree.

Ultimately, Hayden would squander at least $696 million on TRAILBLAZER between October 2001 and September 2005; the money produced exactly one failed prototype DNE system. The total is likely far higher, as the full amount of money wasted on TRAILBLAZER remains classified.

The only reason we know these facts is because of the Cato Institute FOIA lawsuit (managed by Josh Burday of Loevy & Loevy), which focused on NSA's attempts to prevent multiple Department of Defense Inspector General (DoD IG) reports on the TRAILBLAZER and THINTHREAD systems from ever seeing the light of day (you can read the still heavily redacted but revealing 2004 DoD IG report here and the 2006 report here).

Those reports only came about because the original THINTHREAD team members filed a DoD IG hotline complaint about TRAILBLAZER in September 2002. I learned about and actually read the classified versions of those reports while working for then-Rep. Rush Holt (D-N.J.) in 2013. After Holt's retirement from Congress in 2014, I continued to pursue my investigation into the scandal after joining the Cato Institute, filing the FOIA lawsuit in January 2017.

Throughout the lawsuit, NSA and DoD lawyers repeatedly invoked Section 6 of the NSA Act to try to keep as much of the TRAILBLAZER/THINTHREAD scandal secret as possible. However, the threat of an actual public FOIA trial — ordered by DC Circuit Judge Trevor McFadden — finally forced NSA to disclose the amount cited above. Unfortunately, the 2016 FOIA Improvements Act passed by Congress does not provide FOIA requestors the necessary legal tools to overcome the government accountability and transparency barrier represented by the NSA Act. NSA dug in its heels and refused to release any further information.

No legal mechanism exists to allow myself and the former THINTHREAD team members to have our security clearances restored so we could fight out the classification and disclosure battle *in camera* before the judge. And despite our request, Judge McFadden declined to use an existing precedent to appoint a cleared Special Master (court appointed legal or technical experts who advise judges in cases) to review 800 pages of still-classified material in the case to determine whether, in fact, NSA was improperly invoking the NSA Act to conceal still other illegal acts — like Hayden's refusal to follow the law and more widely deploy THINTHREAD as ordered by Congress, which we had finally pressured NSA into revealing. The existing executive order on classification and declassification expressly forbids such acts, but there is nothing in statute requiring such a review in FOIA cases, and at present there is no legal penalty for the kind of misuse of the NSA Act that NSA employed in this episode. Faced with these barriers, we were forced to settle the case this month.

The problem is that the NSA Act is what is known as a "(b)(3)" FOIA exemption statute — meaning that it is an existing law that can be used to withhold information from the public in spite of FOIA. The 2016 FOIA Improvements Act failed to address that problem, which also applies to laws allowing the CIA, Office of the Director of National Intelligence, and other federal department and agencies to withhold — often in blanket form — information that might reveal waste, fraud, abuse, mismanagement or even criminal conduct.

If NSA or any other department or agency that currently enjoys the use of a "(b)(3)" exemption statute is allowed to keep it, you can take it to the bank they will use it to conceal bad management, wasteful spending, and even criminal conduct. If Congress were to strike Section 6 of the NSA Act, it would go a long way towards improving public oversight and government transparency as it pertains to NSA, but much more is needed.

In the TRAILBLAZER/THINTHREAD episode, the agency that was the subject of investigation — NSA — used Section 6 of the NSA Act to try to prevent highly critical audit and investigation reports by another DoD element — the DoD IG — from ever being revealed. When the entity being audited can prevent the auditor from reporting findings of wrongdoing to taxpayers, the system is by definition corrupt. Congress should statutorily bar any agency or department subjected to an IG or Government Accountability Office (GAO) audit from blocking release of that report to the public.

Additionally, Congress should *mandate* judicial *in camera* reviews in FOIA cases involving classified information or in which a "(b)(3)" exemption statute (if still on the books) is invoked to determine whether it is being misused by an executive branch department or agency to conceal waste, fraud, abuse, mismanagement or criminal conduct. An outright statutory bar on using *any* law to conceal the aforementioned misconduct should likewise be enacted.

Americans should not have to rely on whistleblowers like Snowden to reveal our government is targeting us for unconstitutional surveillance behind a shield of secrecy. Nor should executive branch bureaucrats be able to conceal their misconduct behind false claims that exposing their ineptitude or criminality would involve "compromising sources and methods."

The author, a former CIA analyst and ex-Senior Policy Advisor to Rep. Rush Holt (D-N.J.), is a Research Fellow at the Cato Institute. You can follow him on Twitter via @PGEddington.