

NSA Whistle-Blower: Obama “Worse than Bush”

The national security state needs a boogeyman to keep the money flowing

By [Thomas Drake](#) and [Matthew Harwood](#)

Global Research, March 09, 2012

[Salon](#) 7 March 2012

Region: [USA](#)

Theme: [Law and Justice](#), [Police State & Civil Rights](#)

Thomas Drake, the whistle-blower whom the Obama administration tried and failed to prosecute for leaking information about waste, fraud and abuse at the National Security Agency, now works at an Apple store in Maryland. In an interview with Salon, Drake laughed about the time he [confronted Attorney General Eric Holder at his store](#) while Holder perused the gadgetry on display with his security detail around him. When Drake started asking Holder questions about his case, America’s chief law enforcement officer turned and fled the store.

But the humor drained away quickly from Drake’s thin and tired face as he recounted his ordeal since 2010 when federal prosecutors charged him with violating the Espionage Act for retaining classified information they believed he would pass on to then Baltimore Sun reporter Siobhan Gorman. While Drake never disclosed classified information, he did pass on unclassified information to Gorman revealing that the NSA had [wasted billions of taxpayers’ dollars on Trailblazer](#), a contractor-heavy intelligence software program that failed to find terrorist threats in the tsunami of digital data the agency was sucking up globally — and sometimes unconstitutionally. While Trailblazer burned through cash, in the process enriching many NSA employees turned contractors, Drake found that another software program named ThinThread had already met the core requirements of a federal acquisition regulation that governed the proposed system at a sliver of the cost, all while protecting American civil liberties at the code level. The NSA leadership, however, had already bet their careers on Trailblazer. So Drake blew the whistle, first to Congress, then to the Department of Defense Inspector General’s Office, and finally, and fatefully, to Gorman.

Last June, the government’s case collapsed. On the eve of trial, [all 10 counts were dropped](#). In a Kafkaesque turn of events, Drake actually helped the government find a misdemeanor to charge him with — exceeding authorized use of an NSA computer — so federal prosecutors could save face. Once facing 35 years behind bars, Drake pled guilty to the misdemeanor charge and was sentenced to one year of probation and 240 hours of community service, what he sardonically calls “his penance.”

But his legal battles haven’t ended. Currently, Drake, along with the four other whistle-blowers he worked with to expose NSA waste, fraud and abuse, are fighting to get their property back that the FBI confiscated during its criminal investigations. Once a registered Republican and now a self-described “free-speech absolutist,” Drake describes the NSA as a rogue agency that operates in a black box that the public cannot penetrate.

Drake, along with his attorney [Jesselyn Radack](#) of the Government Accountability Project, sat down for a three-hour interview with Salon. Here are some excerpts from our

conversation.

Matthew Harwood: What happens at a place like the NSA when they don't trust you anymore?

I blew the whistle literally on Trailblazer during that 2003-2005 time frame. That led to a whole series of what I will call the retaliation, reprisal and retribution by a thousand cuts, bureaucratic and administrative, where they slowly take you away from your primary responsibilities. They isolate you so you increasingly have less and less of a role to play, even though I was a senior executive in the government.

It's like Milton out of "Office Space." You're put in the basement in a cubicle away from everyone.

You talk about Milton in the basement with his stapler. That's effectively what happened. You are uninvited from certain kinds of meetings. You end up having certain key functions reassigned to even your own staff members or informed that the funding that you had been receiving, well, you know we don't need to do that anymore.

In your opinion, is it in the hope that you resign?

Yeah, part of it is the isolation. A bureaucracy can really create this artificial desert, but the desert is real. And in essence, what happens is that they're taking away the meaning and purpose for who you are when at work. Given that work for so many people is their identity, it attempts to fragment your identity. If you fragment that identity enough, then the hope is you'll just pack up and take your bag somewhere else. And good riddance. I remember when they realized that I was a threat. The white blood cells were kicking in big time.

It sounds like some dystopian corporate environment but in an absurd, petty way.

You talk about the dark side of Dilbert; they were literally manufacturing incidents that never occurred. That's the level at which they excel. The distrust within this dystopia of each other: people come into work looking to make someone else's life bad and they're deriving great pleasure from the psychological pain they're inflicting bureaucratically on one another. What does that tell you?

Did you lose your pension?

I was within five-and-a-half years of retirement based on a combination of my military and government time, both CIA and NSA. That's not there. I have what's called a thrift savings plan, but I had to take half of that money out. You talk about the price you pay. Most people don't know it's significant. I spent close to \$100,000 on attorney fees plus expenses. I have literally given up hundreds of thousands of dollars and a government pension that would have been worth close to a million dollars.

Would you still blow the whistle if you knew what you know now?

Yes. There are a few things I would have done differently, though. I would not have spoken to the FBI. I knew that in speaking with them that something could be used against me. I was read my Miranda rights, but I waved them to cooperate, but to report crimes: misdemeanors, illegalities, management malfeasance, program fraud, waste and abuse. I

would have immediately had an attorney, but that's in hindsight.

Another regret: I would have gone public before indictment. Remember, once they indict you're already in a severely negative place. But the last place I would have shared any information with is WikiLeaks, and yet it is a viable internationally based alternative for getting the truth out. This is partly why [Bradley] Manning is in the hot water because he's not going through, allegedly, an American citizen; he's going somewhere else. And it's not the enemy, let's get that straight right off the bat, but he's going to an organization that's non-U.S.-based, non-U.S. citizen.

And I never would have gone to NSA as a senior executive. I would have stayed a contractor. I would have just made money. But, see, it's easy to say that. And there are no regrets because I have to live with the integrity of who I am. I recognize that it's a very lonely space as a whistle-blower, how incredibly isolating it is. And how you keep what you know because of the risks that are involved, recognizing you're in a much bigger system. You end up keeping the truth from those who you think you could share it with. That includes close family members because you don't want them implicated. You don't want them to be viewed as an accessory. My spouse, because she works as an NSA contractor, was interrogated/interviewed by the FBI for a couple of hours. She had no knowledge of any of the specifics of the cooperation I had with DoD. Or the fact that I had contact with a reporter. They were betting that in terms of sitting one pillow next to another that you would share.

In your opinion, is Bradley Manning a whistle-blower?

There is also a lot of what I call false flag arguments with Manning. It took incredible courage, incredible risk. He ended up listening to his conscience. All the other stuff you hear about is a red herring. All the other stuff is personal and it's misdirection. Remember, the government uses the court of public opinion, just as much if not more so than whistle-blowers. The advantage they had, in my case, remember, I was way behind the 8-ball. In essence they already made like six moves in chess, before I could make a move at all. They already had the upper hand. They had the narrative. They had the charges. They had painted me as a traitor. That I had violated my oath. That I had betrayed my country.

The only defense you have then is the truth.

But what if it's not sufficient? The truth was always on my side. I knew the truth. It's one of the advantages of the truth; you don't have to make up a story. You just tell the truth. I never had to think about what to say, I just said it.

You talk regularly about how a feeding frenzy occurred throughout the U.S. security establishment and its defense contractors after Congress starting writing blank checks in an effort to prevent another 9/11. A decade later, are we at a place now then where they have to manufacture threats to keep the money flowing?

You have to persist the threat. You have to find another existential reason why this is indefinite. The only way to do that is the boogeyman. You have to paint that.

Whether that's Iran or homegrown terrorists or China?

Doesn't matter, and especially when you have less understanding about it. Radically

different cultures. Radically different environments. We don't learn very well, except where it's reflexively us. We have a tendency to project ourselves onto others. So yes, you have to manufacture if you're making that kind of money. The national security state became a growth industry — huge redistribution of wealth. I had people coming to me: "Tom, you have to get out. The money is unbelievable. You can be a millionaire."

Literally the idea is after 9/11, you could retire, exit the door, and then walk back in a week later as a contractor making way more money.

That's correct. Some people did. We're talking lots of money. The revolving door is an understatement. The number of millionaires made at NSA, one of these open dark secrets, is phenomenal. I had very senior defense contractors attempting to compromise me, co-opt me. "Tom, you have all this access now. Sheesh. We could bring you over. You could lead our NSA business office."

Advanced software, like what Palantir sells, boasts that it can establish connections between individuals that a human investigator or analyst would find impossible. Can't that be reverse engineered to track down whistle-blowers?

Yes, by the very means by which you can detect patterns. What is true about technology like ThinThread or Palantir Government is the real potential for irresponsible abuse in secret and targeting those who are deemed as trouble, dissenters in government or industry — using the very technology designed for intelligence indications and warning about real threats, and then using it against internal threats like whistle-blowing and profiling their activities for identification and punishment.

They certainly did it with me using similar kinds of monitoring technology. I recognize that I was a template. I was profiled. There was no question. And part of the profiling is what was the activity set that identifies whistle-blowers. But remember, part of this requires persistent surveillance electronically. I was electronically surveilled 15 ways to Sunday. And I was physically surveilled. My car was searched, in terms of patterns, far more frequently than I would have expected. And I realized what was happening but I couldn't say anything. They made no bones about that fact and part of it is intimidation. It's sending the message: "We know what you're up to."

Jesselyn Radack: Which brings us back to the dark ages. Pay in cash. Meet in person in obscure locations. You adopt drug dealer tactics. You adopt the tactics of high-level criminals.

But by doing that, guess what you establish: you're suspicious. And see isn't that a Catch-22. But there is a defense to this. Forget all the furtiveness. Forget all of this stuff about what criminal enterprises do to hide their criminal activity, which is what the government is doing themselves. They're hiding their own activity. The answer is openness and transparency, period. Right now with my colleagues, we're not encrypting with each other when we're communicating on the civil lawsuit. We're wide open. We're in the open. If they're monitoring us, then so be it.

In [the New Yorker article](#), Jane Mayer quotes you as saying, "I actually had hopes for Obama." What's your opinion on the Obama administration's stated support for whistle-blowers and, more generally, his counterterrorism record?

Worse than Bush. I have to say that. I actually voted for Obama. It's all rhetoric for me now. As Americans we were hoodwinked. He's expanding the secrecy regime far beyond what the Bush even intended, interestingly enough. I think Bush is probably like, "Whoa."

Matthew Harwood is a journalist based in Alexandria, Va. His work has appeared in the *Columbia Journalism Review*, *the Guardian*, *Reason*, *Truthout*, and the *Washington Monthly*. Follow him on Twitter @mharwood31 [More Matthew Harwood](#)

The original source of this article is [Salon](#)

Copyright © [Thomas Drake](#) and [Matthew Harwood](#), [Salon](#), 2012

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Thomas Drake](#)
and [Matthew Harwood](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca