



Written by [Bob Adelman](#) on March 19, 2012

NSA's Spy Program "Stellar Wind" Exposed

[Stellar Wind](#) is the code name for an effort approved by President George W. Bush following the September 11, 2001 attacks to mine a large database of communications of American citizens but which was allegedly terminated when Congress pushed back against it.

However, the National Security Agency, awash with funds provided by Congress, is nearly finished constructing its Utah Data Center as the collection point for data provided from around the country and around the world. Its purpose: "to intercept, decipher, analyze and store vast swaths of the world's communications ... [including] all forms of communication, including the complete contents of private emails, cell phone calls and Google searches." In other words, according to James Bamford, author of [The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America](#), when the \$2 billion facility (consisting of four 25,000 square-foot buildings full of computer servers and their air conditioning units plus a 900,000 square-foot building to house its technical and administration people) is completed in September, 2013,



virtually everything one communicates through any traceable medium, or any record of one's existence in the electronic medium, which these days is everything, will ... become the property of the US government to deal with as it sees fit.

William Binney, a former NSA crypto-mathematician who quit NSA after he realized it was openly and deliberately ignoring privacy limitations built into the Constitution, said in an interview with Bamford, holding his thumb and forefinger close together: "We are this far from a turnkey totalitarian state."

Binney headed up a team that built the infrastructure to spy on everyone all the time and, at the time, recommended that NSA install its "tapping gear" only at the nation's "landing sites" — physical locations where fiber optic cables come ashore — to limit its eavesdropping to international communications only and preserving Americans' right to privacy. But NSA ignored Binney's recommendation and instead decided to build its spy center in Utah, connecting it with satellites and listening posts in Colorado, Georgia, Texas, Hawaii, and elsewhere, with direct links to NSA headquarters in Fort Meade, Maryland, NSA's research facility in Oak Ridge, Tennessee, and last but



Written by [Bob Adelman](#) on March 19, 2012

not least, the White House.

In addition NSA has two huge data-gathering facilities, each with three 105-foot satellite dishes, one at Catawissa, Pennsylvania, called Roaring Creek, the other at Arbuckle, California, called Salt Creek.

Says Binney, "They violated the Constitution setting it up. But they didn't care. They were going to do it anyway, and they were going to crucify anyone who stood in their way. When they started violating the Constitution, I couldn't stay."

One of the challenges NSA faced was decrypting data, such as that encoded by PGP or the much more robust encryption software used by governments. The Advanced Encryption Standard is used to protect most commercial e-mail programs and web browsers and has, until very recently, been considered unbreakable. To break a 128-bit encryption code, for example, the number of trial-and-error attempts — call "brute force" — requires an incomprehensibly large number of attempts before succeeding: 340 undecillion (10 to the 26th power). But current breakthroughs by NSA, using Cray super-fast computers, now can break such codes in fractions of a second, exposing all information to the light of day and the peering eyes of NSA observers.

At the moment it appears that the two strongest barriers to intrusions on privacy, technological and constitutional, have been shredded. But courts are involved in a variety of challenges to the NSA's efforts, and the project isn't due to come online in full flower until a year from September. Such an operation, now out in the open, requires enormous funding. Congress, given sufficient encouragement and electoral change of heart this November, could just shut it down by defunding it. It's really up to informed Americans to see where their elected officials stand on privacy versus security and then take appropriate action in the voting booth.



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.