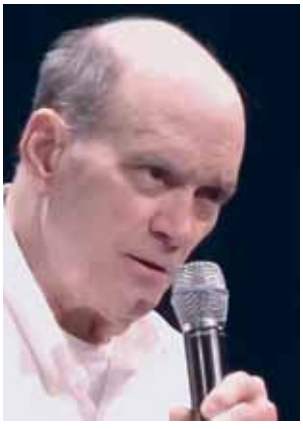
Bulk Acquisition Is Why I Quit, But There Is a Solution



LPAC-TV

William Binney

William Binney: Thank you. As Dennis said, the government we had, opted for bulk acquisition for two basic reasons, I think. One was set up by Vice President Dick Cheney. He wanted to know everything about all his potential adversaries, politically or otherwise. So, that meant he had to have information about everybody. So, the bulk acquisition satisfied his need in that respect. But in the other respect, in the bureaucracies of the government, bureaucrats tend to like to get bigger and bigger budgets, and bigger and bigger organizations, so that meant more and more money, and more and more influence. In order to do that, if you opt for this bulk acquisition on everybody so that you can satisfy Cheney's needs, it also requires the Congress to give you much more money so you can build your bureaucracy. And those are, I think, the basic motivations to do this.

But they had known also from the very beginning that there was another solution that would actually do productive things, because when you took the bulk acquisition, that meant you couldn't see the threats coming; there was just too much data. That's why they haven't been able to prevent any of the terrorist attacks that have occurred anywhere in the world. Because everybody has adopted this policy, and they can't see the threats coming. This is documented internally in NSA records produced by Edward Snowden and also by MI5 and MI6 records, and some in GCHQ. They are saying, their analysts are telling them, that there is too much data; you've buried us, you've overloaded us. We can't see the threat coming.

Thin Thread

Just for that reason alone, they shouldn't be doing it. But the real point is, the solution existed all along. We were developing that in the Thin Thread program. That basically had three tenets: one was a deductive approach; one an abductive approach; and one was an inductive approach.

For the deductive approach, we simply looked at social organizations that stayed within one degree of the known bad guys, and used that data to pull out information, and only that information, from the data flow that we were looking at. We were looking at a number of terabytes a minute or so at the time, and we wanted to up that to about 20 terabytes a minute. That was our approach. That was the deductive side. So, that was the human behavior property that showed probable cause. If you're contacting a terrorist, then you need to be looked at; that's easy to justify in a warrant.

In the inductive approach, you're looking at sites that are advocating pedophilia or sites that advocate terrorism or violence against the West, or bomb-making, or things like that. You could try to watch people who visit those sites so you can see their frequency of visit, and say that they are probably getting radicalized, or in the process of radicalization. Or, you have people who have cell phones in the mountains of Afghanistan, or satellite phones in the mountains of Afghanistan, or the jungles of Peru. And you say, they're dope traffickers, or they're terror potentials. And you look at those kinds of things. That's kind of the inductive approach.

So far, those two approaches would have caught every terrorist attack in the world before, during, and after 9/11; every one. But did we do that? No, because that's a focussed, disciplined, professional attack on the data and against bad behavior by people indicating potential threats. The abductive approach is a little bit more abstract; it says you look at geographical distributions. If you have a network at one degree that is distributed in countries that are involved in terrorist advocation or something like that, you need to look at them to see if

USAF/Sue Sapp

Former Vice President Dick Cheney.

CC

NSA's massive Utah Data Center, also known as the Intelligence Community Comprehensive National Cybersecurity Initiative Data Center, in Riverton, Utah, as it looked in 2014.

they're terrorists or in any way affiliated with a terrorist attack or organization. Once you look at them, if they're not, then you take them out, and you simply say they're out. The rest of the data you simply let go right by.

Now what that does is, it gives everybody in the world privacy. And it respects the Constitutional and privacy rights of everybody in this country and every country in the world. Plus, it creates an extremely rich environment for analysts to succeed at preventing threats and potential adversarial attacks. That's the whole point of why we did the Thin Thread program to begin with, because even back then our analysts were buried with data.

So the end result today is, we have a situation where,—the key point here is NSA databasing of information. Our country is the only country in the world that can afford all the data storage, that can store all the information they're collecting. They're collecting multiple petabytes a day. My estimate of the Utah storage facility alone was based on the number of Cisco routers being put into it, and what they were estimating was 966 exabytes of data going into that data center a year by 2015. So, I figure they had to have at least five years of storage capacity, which meant five zettabytes, which is much less than a yottabyte, but still, it's quite a bit. After that, we get a bunch of bytes, and a lot of bytes, and all that kind of stuff. So, it hadn't been named above a yottabyte.

But the point is, NSA is the key element here, because it's a storage facility for not just NSA, but all of the agencies of the United States government, all the Five Eyes, and the nine other countries that are participating with them in this worldwide collection of data and bulk acquisition of data on everybody on the planet. And all we would have to do is take our rules—deductive, inductive, and abductive—take those rules and run it and process the entire database that's stored, and pull out only that which is relevant and purge the rest of it.

At that point, there would be no data available for anybody in the U.S. government or the British government or anywhere to use against their people. So it couldn't be abused. So, that would fix the problem. That would mean that the FBI, the DEA, the DOJ, or anybody in the intelligence community, or in the Five Eyes, or any of the others, could not go into that database and find information on any one citizen, unless that citizen had probable cause, warrant-based evidence that they should be there. That's the way to fix this whole problem and do it rather quickly. Because once you take that data out, no one has the ability to abuse it.

Intelligence and the U.S. Constitution

LPAC-TV

Kirk Wiebe

Kirk Wiebe: Hello. Thank you, Dennis, and thank you to the LaRouche organization for making this possible, and for inviting us to address these fine people before us.

A lot of people don't realize it, but the National Security Agency—and I'm going to pick on them, because I worked there for a long time, with Bill—has operated unconstitutionally for about 70% of the time it has existed on the planet. What do I mean by that? Well, the people in charge—namely, the Executive, namely the Legislative branches of government—have formed a cabal, a cartel, if you will, that has decided to mass surveil the world, stuff the information in a big database somewhere, and