



---

# The Solari Report

June 29, 2016

---

## The Corruption and Compromise of the NSA With William E. Binney



Catherine Austin Fitts

William E. Binney



# The Corruption and Compromise of the NSA With William E. Binney

June 29 2017

---

**C. Austin Fitts:** Ladies and gentlemen, it's a pleasure to welcome to The Solari Report someone I've listened to and been an admirer of for many, many years. His name is Bill Binney and is a retired Senior NSA intelligence officer. He has been described by some of his colleagues as one of the finest analysts in the NSA history.

He retired in October of 2001 after a highly successful 30-year career with the NSA. He was concerned about the constitutionality of NSA policies and programs. Since his retirement, he has made a major contribution in helping US and global policymakers, media, and the general population understand what is happening and what we can do about it.

It's a real pleasure to welcome you to The Solari Report, Bill,

The media has been keeping you busy!



**William E. Binney:** Yes they have – especially with all these unfounded allegations about the Russians. They are trying to start a new Cold War.

**C. Austin Fitts:** Once upon a time you were a Russian analyst, correct?

**William E. Binney:** That is correct. There wasn't anything that they could do that I wouldn't know in advance of what they were about to do. I read them like the back of my hand and I knew exactly what they were all about.

**C. Austin Fitts:** Let's review information about you. I want to make sure everyone has a good background and understands what you have accomplished with a Thin Thread system and NSA. Before you start, I want to mention that the 'Let's Go to the Movies' this week on The Solari Report is Frederick Moser's documentary on you and your experience called *A Good American*, and his sequel, *The Maze*, which gives a great deal of background. I would encourage subscribers to hear that because of the detailed understanding of the Thin Thread system that you built and also, the Trail Blazer system that NSA adopted is very much worth understanding and very helpful to comprehend current events.

Tell us a little about what you did at NSA, particularly the Thin Thread system.



**William E. Binney:** I am primarily working on solving codes and cyphers and similar things and also data systems for or against the Warsaw Pact Soviet problems. That was where my major emphasis was until the 1990's when I got involved as the technical director of, what I called, 'the world'; I thought that was a fun title.

I was having fun with that. At any rate, when I got to that point, I was looking to see what the real problem was that our analysts were facing. There were about 6,000 analysts in our group. It was very clear that the mushrooming digital communications in the world was burying people and making it impossible for them to succeed at solving problems that were germane in terms of terrorism and the like.

That's when I started with the Thin Thread program around 1997 and really started cranking along in 1998. So I was planning in 1997 and executing in 1998 and 1999. Then by 2000 we had it ready.

It was a program that looked at sessionized data off the fiberoptic lines where it would take in the fiber rates and sessionized data on any scale you preferred – 10 gigabits or however many you wanted to go. It was only dependent on space and power. That meant, basically, that we could collect everything in the world.

My objective was to look at the data and examine it using meta-data to see what was important to pull out for our analysts to review, not bury them with meaningless drivel from other people in the world who weren't even relevant to any of the problems. So we focused on doing that, and that is what we succeeded doing at fiber optic rates.



Primarily, it gave everyone in the world privacy upfront because none of their data was available to anybody in the intelligence community or in law enforcement. So that was the first thing that we did, and that was the first thing that they got rid of. So they removed that software from the filtering software, and took in everything.

We had another set of software behind it that said that if you're taken in and not known to be a target, we encrypt your data so that nobody knows who you are until we can show that you are part of the criminal activity. Once we showed that, we could get a warrant and uncover you and target you. That was the second thing that they removed.

So they collected everything, and nobody had any privacy, whatsoever. The third thing was an audit routine that we had running across our entire network looking at who came into our network, what they did, how long they stayed, where they went, and what they did with the data.

In other words, Edward Snowden couldn't have done what he did without us knowing about it if they had implemented that. But that was the other thing that they didn't want. The NSA has criminal activity when it comes to money. It's corruption and fraud and waste, and they didn't want anybody to know where they move money around from program to program. They don't want you to know what programs are wasting money, where they are throwing away money, and where they are violating the Federal acquisitions act or anything like that.



That program would have exposed all of that, and they didn't want anybody to know – especially Congress because they could cut their budget and similar things, which they should have anyway, but they didn't.

That meant they could take in everything, know everybody in the world – including all US citizens. My estimate is at least 280 million citizens. The others were too young to use electronic devices or in hospice or people not in position to use electronic devices.

The Constitution and the laws of the land meant absolutely nothing to them; they simply violated all of them. So I called it the fundamental treason against the founding principles of this nation.

**C. Austin Fitts:** So you actually retired because you were concerned about the Constitutionality of what they were doing? The thing that I love about a good American is that it helps you understand why you can accomplish all of the national security purposes without compromising Americans' privacy and you don't have to.

**William E. Binney:** That's right. That idea that you had to trade privacy for security has been a lie from the very beginning. The difference is the magnitude of money necessary to achieve bulk acquisition on everybody on the planet: 1) Builds a big empire for you, 2) Gives you all the power against everybody in the world that you would ever need. If you have anybody who is doing something that you don't want or don't like them doing, you have all the information about them that you can collect from the world, and you can go in and investigate and find something against them and use that as leverage to stop them.



I maintain that's what happened to Eliot Spitzer because he was going after the bankers for defrauding people. That would have led back to the Congress with Dodd Frank and all those programs. That had to be stopped, and that is what they did with him.

They also did it with the CEO of Qwest, Joe Nacchio. They put him in jail for it, so he became the poster boy for CEO's. "If you don't cooperate with us, we're going to find something and put you in jail". That is what they did to him.

Then they went after James Rosen, the Associated Press journalist. They have leverage on everybody and they certainly went after whistleblowers. This is too much power and that's why we have a Fourth Amendment.

**C. Austin Fitts:** One thing that you brought out very well in *A Good American* is Thin Thread was operated and controlled by the civil service, and Trail Blazer was really turned over to outside contractors at a much greater expense.

**William E. Binney:** Yes.

**C. Austin Fitts:** I find that a lot of the shenanigans occur as soon as you can get it out of the hands of the civil service; not to say that one is all bad and one is all good, but if you're going to maintain sovereignty, then you need it under the control of government employees. As soon as you can get it into the outside contractors, that is where much of the shenanigans start.



**William E. Binney:** Yes, because their objective is to get the next contract. I came up with their vision statement. Originally I thought it was, “Aim low and miss,” because they failed all the time. I actually changed it later. In the 1990’s it was very clear to me that their whole concept was, “Keep the problem going so the money keeps flowing.”

They’re not intending to solve the problem. If they solve the problem, they can’t see beyond that and can’t see what they’re going to do next and are afraid of that. Their concern is to get the next contract. It’s not to solve the problem; that is the issue. That is why I keep saying publicly that the people in charge at NSA and the CIA and the White House essentially traded the security of the people of the United States and the free world for money. Actually, it was also power, because that knowledge of everybody gave them power over everyone.

**C. Austin Fitts:** Right. We’re going to get into that a little later on. I want to keep discussing the history. When you retired, you started a business and they targeted your business and made it difficult to operate. Then you inspired an IG investigation. Maybe you could tell us a little about that.

**William E. Binney:** Originally we were referred to the National Reconnaissance Office – the NRO – to do a task by the senior staffer on the Senate Intelligence Committee. We went there to do that, and were involved and starting to work on that. Then the NSA found out about it, and had, not only us removed from the program, but also they had the entire program cancelled.



So the staffer on the Senate Intelligence Committee went to the members of the Senate and said, “We need to investigate NSA because of what they are doing here,” because that is a felony. It’s a violation of the pursuit of happiness and all of that.

The Senate members refused to do it simply because ‘they would look bad’. Publicly it would look bad to have them going after an intelligence agency after 9/11 was fresh in everybody’s mind. “We need to support our intelligence agencies.”

That was absolutely the wrong thing to do, and all they did was squander the money. People who were known have murdered the people who have been assassinated since then. That was the whole idea of the Thin Thread program. That’s why we started it – because they were buried in meaningless data. How could you enrich the set of information that they were looking at so that they could actually succeed? That was the entire point of it.

They are still in the same boat. The British have adopted it, the Germans have done it, and we’re all in the same boat. That’s why these people are getting murdered all over the world. They’re not focusing and it’s not a disciplined, professional job now.

**C. Austin Fitts:** Right. So you said that the Germans and the Brits are also doing the bulk acquisition?

**William E. Binney:** Yes. It’s actually a “Five Eyes” effort plus about seven, eight, or maybe even nine other countries in Europe and various other allies around the world like Japan and Israel.



**C. Austin Fitts:** The tension between you and the NSA went to a new level. The *New York Times* published an article, and the next thing your house was raided and some of your many colleagues were raided as well. That, I believe, was 2005?

**William E. Binney:** It was in July of 2007. It was July 26, 2007 to be precise. It was a raid done simultaneously against all four of us who had filed the DOJ complaint against NSA for corruption, fraud, waste, and abuse. We filed that in September of 2002, and so they were trying to find some way to get back at us.

When this *New York Times* article hit, they accused us of that and bamboozled judges, who didn't know any better, to sign the warrants to come after us when there was no evidence presented in the affidavits. We have those now; it took us five years to get them. There was no evidence in the affidavits that pointed to us for anything, so there was no probable cause to do it anyway.

They already knew that we weren't involved because they the source of the *New York Times* article. He was the lawyer in the Department of Justice who was writing the request for warrants for the FISA Court. He knew when the FBI and the NSA and CIA were feeding him information to request the warrant and saw that they already had wiretaps and were reading emails on everybody. Those were the felonies to begin with. They were supposed to go through the FISA Court to get that kind of information, and instead they already had it.



That's why he did that. They also knew from the Stellar Wind program all the data on phone calls and emails and contacts and financial information that internally on domestic communications and domestic matters that we were not involved either because they had all this data from the telecoms and the internet service providers. So they knew it was false to begin with, and this was all done under Comey and Mueller – the two guys who are there now and who were involved in the Department of Justice and the FBI at that time.

**C. Austin Fitts:** The sweethearts.

**William E. Binney:** Also, the current Deputy Attorney General was a part of the process. He was somewhere down the line involved in the investigations into the leaks. So his name was on the affidavits and the warrants, too.

**C. Austin Fitts:** I don't know if you knew this, but I litigated with the Department of Justice for many, many years. In my experience it's the same thing. They all keep turning up again like a bad penny.

**William E. Binney:** Well, they had to keep covering up for one another. When you commit crimes, you have to cover it up, and need everybody to participate because if any one of them falls, they all fall.

**C. Austin Fitts:** So you were successful in your litigation with them, which is quite an accomplishment. I know in the end, you received an immunity letter. I have no idea how you did that but it was a very impressive performance.



**William E. Binney:** That's really a cute story. The raid occurred on the morning of the second day after Attorney General Gonzales's testimony to the Senate Judiciary Committee about the President's surveillance programs, which he only talked about the wiretapping that was exposed in the *New York Times*. He didn't talk about the rest of the Stellar Wind program or the collection of AT&T and Verizon and various other telecoms around the United States and all of the tap points and everything. He didn't talk about the rendering program or the torture program or the kidnapping and torture and the murder programs that were being run at the time. He didn't talk about any of that.

They were afraid that we would go there and start to talk to the Senate Judiciary Committee about these programs – the ones that Gonzales never said anything about – so it was selective talking to the Judiciary Committee. So they raided us to keep us quiet and off bounds. When that happens, you lawyer up and the lawyers say, “Don't talk to anybody.”

We didn't pay any attention to that and thought it was important to talk. So we were trying to converse among ourselves because we needed to organize to respond to the government.

As part of the follow-up process, three separate times after the Department of Justice joined in; they tried to indict us under the Espionage Act – three separate times! Each time I had exculpatory data on them that I could show. I told our lawyer about it, and they backed off. The third time, however, they called our lawyer and said, “No, we're going to indict your guys now.”



They only said it to him, so he told us that we were going to be indicted. So I said, “Okay, now it’s time for me to pull my little number. I’m going to play them like a fiddle.”

I called Tom Drake because I’d been assembling evidence of malicious prosecution on the part of the Department of Justice of the United States. They were fabricating evidence, and I had proof of that. I had very clear evidence.

I called Tom and said, “Our lawyer called us and said that we are going to be indicted – all of us – and I’ve been assembling all this evidence of malicious prosecution. Here it is,” and I proceeded to read it across the phone to him because I knew that the FBI had his phone tapped.

So I’m reading it to Tom, and telling him where to get it. I said, “You have to go in and click on the files that I mentioned. Then go down and click on ‘properties’ and you’ll see the date and time,” because I didn’t want the FBI to miss it; they had been known to do that. They’re not the swiftest people in the world.

I said, “Tom, tell your lawyer that we’re going to charge them with malicious persecution when they take us to court,” and then I hung up.

I waited, and finally a month later we received unsolicited letters of immunity from the Department of Justice.

I know our lawyer had no idea what happened because I never told him. It wasn’t important for him to know; it was important for the FBI and the DOJ to know that I was going to come at them. They’ve never bothered us since then.



**C. Austin Fitts:** You did better than me because HUD, IG, and the FBI – and it’s a long story, so I won’t bore you with it – falsified evidence, and the property manager in our offices was a witness to it and gave us an affidavit. I turned it over to the courts, and the courts said to my attorney, “That’s standard operating procedure. If you don’t have any evidence, you just try to falsify something on obstruction of justice.” They didn’t seem to take it very seriously.

**William E. Binney:** That’s the pathetic part of it, isn’t it? It’s literally pathetic.

**C. Austin Fitts:** It’s bizarre because my attorney was Jewish, and said, “My family left Germany to get away from this, and now it’s here.”

He was scared to death; he was shaking.

Your knowledge as an intelligence officer and also your reputation – which is really extraordinary and I’m sure it was then –served you well. You seem to have a fearless part to your character.

**William E. Binney:** I had to be fearless in the NSA. Every time I tried to do something, people opposed me. As I said in the movie, I never asked permission; I simply did it. Then if I had to, I asked for forgiveness.

If you tried to open up and say, “I’d like to do this,” everybody opposes you. So I said, “To hell with them! They don’t achieve anything. Why even consult them?”



At any rate, that's the way I felt about it, also. The point is that we have a Department of Justice that is fabricating evidence to put people in jail to keep them quiet. People are exposing things that they don't particularly want heard in public. My point is to keep at it.

Right now I'm supporting four separate lawsuits against the United States government for unconstitutionally collecting the data: One at the 2<sup>nd</sup> Circuit Court of Appeals, one in the 3<sup>rd</sup>, one in the 9<sup>th</sup>, and one in the 11<sup>th</sup>. I've recently heard from my lawyer in the Third Circuit that somebody in the 4<sup>th</sup> Circuit has leveraged what we said in the 3<sup>rd</sup>. So another lawsuit is happening there. I haven't found out what that one is about yet, but I'll try to support that one when I discover what that is, too.

**C. Austin Fitts:** Good for you.

**William E. Binney:** I feed all kinds of information into them so they can write up responses to motions by the government that try to hide what they're doing.

**C. Austin Fitts:** We're going to put up links for the subscribers. I know you've been doing ongoing interviews and testimony – both in the US and Europe. I think it has been very useful to help a lot of policymakers understand the difference between what is possible and what is happening now with bulk acquisition.

**William E. Binney:** I should tell you what happened during my testimony to the House of Lords in the UK.



**C. Austin Fitts:** Definitely.

**William E. Binney:** This is really funny. I started when I got into the UK by saying, “Bulk data collection kills people. They can’t see anything in advance, so they can’t stop the attack, and people die as a result”.

Then I gave a testimony to the House of Lords. One of the members said, “You mean to tell me that you’re here telling us that all the members of our government and all the members of the agencies of our government who came in here to testify have been lying to us?”

I said, “Yes, I guess I am.”

**C. Austin Fitts:** I saw a video of that exact testimony, and I will tell you that you absolutely radiated integrity and competence.

**William E. Binney:** Not only that, but I also gave them documented evidence and they ignored it.

**C. Austin Fitts:** I absolutely believe – just from watching that video – that the members knew you were right. They shouldn’t have asked that question if they didn’t want to hear it.

**William E. Binney:** That’s right.

**C. Austin Fitts:** Let me talk a little about your recent commentary, because that testimony reminds me that I’ve been watching many interviews you’ve done on the DNC hacking on allegations of Russian interference, etc.



One thing that happens in the media is, whether it's the governmental officials or the media, what you get is a completely muddled description of what has to happen and what doesn't have to happen.

Then you go on, and it's a hot knife through butter. You go right to the nuts and bolts and the facts, and it pulls the rug out from under a lot of what I call the 'Shriek-o-meter' –the political dirty tricks, whether it's the media or the government doing them.

I'd like to review some of your recent commentaries. Why don't you tell us what you said about the DNC hacking?

**William E. Binney:** It was very obvious from the very beginning the way the NSA and the intelligence communities were saying things. For example, in the cyber world, the NSA essentially owns the internet worldwide. They have programs called 'trace- route' programs. The members of the audience can Google 'traceroute' and can read about the capabilities of that program, which simply means that NSA has hundreds of switches in the internet around the world so that they are tracing billions of packets as they move throughout the world every day.

That means that if any packets were moved out of the DNC server outside the United States – which is where they have the most coverage because 80% of the networking capability is within or passing through the US – they can trace all those packets as they leave any server anywhere in the US to anyplace outside the US. From there, they can trace it where it goes in Europe or Asia or wherever, including Russia and China.



**C. Austin Fitts:** Right.

**William E. Binney:** The point is that they know where the packets are if they went there. So there wasn't a question saying, "We think..." They should say, "We know, and here's where it came from," much like they did with the Chinese.

If you remember, a few years ago they traced some of the hacking back to a specific building in China. The reason they can do that is because they have trace capabilities, and also have collection capabilities. So it's a matter of them simply saying, "Here is where it came from and there is where it went." It's not a question.

When they equivocated, you knew that they were lying.

**C. Austin Fitts:** One of the problems with bulk acquisition is you can't say that you don't have it.

**William E. Binney:** That's right.

**C. Austin Fitts:** Russian interference – you've also commented on the allegations regarding Russian interference in 2016 campaign.

**William E. Binney:** There is simply no evidence of that. I don't know what they did. Where is the evidence for it?

All we're doing is getting a collection of hot air trying to divert from what the real issues are in this country, and I think we need to focus. We're not focusing. That's that loss of discipline again.



**C. Austin Fitts:** Absolutely.

**William E. Binney:** We need to get back to the business at hand, in my view.

**C. Austin Fitts:** Right. Then there were the White House leaks. Since the new Administration came in, they can't make a phone call without the transcript showing up in the press.

**William E. Binney:** This is the most serious issue that I see.

**C. Austin Fitts:** Absolutely.

**William E. Binney:** I've been calling the intelligence community the 'Praetorian Guard' now, meaning that the Praetorian Guard determined who the emperor was and what the emperor did. So we don't have a shadow government; it's the government behind the government that is pulling the chain and the tail is wagging the dog here.

They're doing it because they have all this leverage against senators and house representatives and judges, including the Supreme Court. So it's not a matter of not having power over people; they have it. This is J. Edgar Hoover on super-steroids.

**C. Austin Fitts:** One thing that has been very interesting is that President Trump has held out in insisting that they were eavesdropping on him in Trump Tower and during the campaign. It seemed for a couple of weeks as though he was a lone voice, and then a variety of people jumped in and said, "Oh, guess what? This is really true," and one of those voices was yours.



**William E. Binney:** We had been trying to feed data to him through people who know him and know that this is going on. It's no surprise and I think he very well knows what is happening.

We were part of the network trying to inform him of the realities of life in Washington – the District of Corruption.

**C. Austin Fitts:** Let's turn to some of the policy issues. There are some very serious ones, and then we'll go to the question of what we can do.

When I litigated with the Federal government, I dealt with all sorts of different patterns of both being surveilled and harassment. I also started to watch what was happening in terms of use of data to 'market' do different things in the economy, mostly focused on investments and different financial flows.

I became convinced that whatever the bulk acquisition was by the intelligence agencies, it was being integrated with other data and used privately to have, what one Harvard business school professor calls, 'surveillance capitalism'.

I live in a poor community in Tennessee – a rural area. Literally somebody would lose their job, and within 24 hours they had two offers for a credit card with a 30% interest rate, and the drug dealer who dealt illegal drugs was at the door.

You watched all the different patterns and said, "This is relational database marketing."



If you perceive how it is operating, it is operating across multiple industries – both legal and illegal. It's quite phenomenal.

If you looked at the behavior of the other team and the lawyers and the different people from the government, they had to be listening to all of our conversations, but there was really no legal basis for them to do it.

**William E. Binney:** Right, but they don't actually care.

**C. Austin Fitts:** Yes, and they weren't even subtle about it. Do you know what I mean? It was like a 'in your face' police state. That is the only way that I can describe it, but I became convinced that there was an integration of data cross-government that was being used by a variety of different industries – whether it was to sell consumer products or to manipulate the financial markets.

If you looked at the financial ramifications of having that data available on the private side, you're talking about making trillions and trillions of dollars. What I'm wondering is if the entire point of the bulk acquisition was to feed that integrated operation, which I call the 'data beast'. I'm also wondering if it wasn't to feed the data beast. I'm wondering if Trail Blazer was not just NSA empire-building but literally a coup d'état.

**William E. Binney:** The NSA and the Federal government in general have been outsourcing to a private industry the business of government.



The NSA, for example, outsourced all of the infrastructure – all the computer support, all the computer acquisition, and all of the database and database management systems. That’s why Edward Snowden was working for Booz Allen as a contractor. He could get into all those databases and take that data. That also goes for all the other contractors working for them, which are the same kind of companies. They have fragments working for NSA, CIA, FBI, and so on. All these companies have tentacles into all these agencies, and they’re managing a lot of that data for them. They basically have all the power behind the scenes.

Now, each of these companies is not restricted to only intelligence; they have other divisions that work in other areas.

If one of their divisions is having a contract dispute or wants to make a bid on a contract, that gives them the ability to look into everyone in the world bidding on that contract and see where they could leverage it. So industrial espionage is one of the main problems.

I objected to this when the NSA, under Hayden, started doing this. He was the guy who came in and advocated all this nonsense and, of course, so is Congress. They were advocating some of this, too. They were all making a big mistake, and now we’re paying for it. That is really what is happening here.



My point is that this kind of thing is extremely dangerous for many reasons, not just political or power control, but also for financial. This gives them the capacity to do espionage on a world-wide scale. This is not something that we should be involved with at all.

**C. Austin Fitts:** When Enron first hit, I was doing a series of radio shows on Enron. One thing that had happened was the Department of Justice had failed to assert jurisdiction over many of the Enron documents. What was interesting was that the chairman of the Finance Committee on the board of Enron was the chairman of an IT provider who provided significant services to DOJ and SEC enforcement.

The Department of Justice did not assert jurisdiction over Enron's documentation, but Enron had asserted jurisdiction over the Department of Justice and SEC's documentation.

**William E. Binney:** Interesting.

**C. Austin Fitts:** One of the interesting ideas that I saw in *A Good American* is that all of this could be returned to the civil service for a much more economic result – both a more productive result and an economic result.

**William E. Binney:** Yes, they would actually focus on doing the mission.

**C. Austin Fitts:** I also wanted to tell you that when I worked in the Bush Administration, I tried to get the data from the contractor who ran the payment systems and the IT systems at HUD.



It was core data I needed to make decisions, and they wouldn't give it to me and there was nothing I could do.

**William E. Binney:** I was going to say, "Good luck!" Even the financial officers that were in NSA told me personally – one after the other – that it was impossible to audit NSA because of the shell game that they play with money once they get inside NSA. That is the other tactic that they use.

**C. Austin Fitts:** There was one interview, and I think it was the one that you did with Kirk Wiebe, where you described the extraordinary accounting practices and financial practices at the NSA. It's going to be one of the links we're putting up.

One thing that has happened that I think is the most disturbing is something called 'targeted individuals'. We've tried over the last ten years to put more and more up on the website about that. I know certainly when I was dealing with the litigation, I dealt with all sorts of 'funny business', and I know that you've been working with a group of targeted individuals and hopefully doing more research on that.

Tell us what a targeted individual is and how it relates to what has been happening at NSA and in the digital side of the intelligence community.

**William E. Binney:** Over the years Kirk and I have been approached by various people saying that they are being targeted. There is such a groundswell of people who were saying these kinds of things, so we felt we had to organize to show in some disciplined, scientific way what is possible and what is occurring, and then provide some way of being able to prove that it is happening.



In other words, we had to detect it and show this in a court of law. That is where we wanted to go with it. So that is what we did, and we had a group with Carla and Kate who were two targeted individuals. These are people who were being targeted and alleged they were being attacked by electromagnetic spectrum instruments or of soundwaves or similar activity of that nature to do various things to them as an experimental process.

What we wanted to do was try to assemble the different kinds of attributes or incidents that people were sensing that were happening to them, and then categorize those. Also, to assemble information that is being published publicly that is available through open source on governmental or military development of tools that are electromagnetic that control populations in terms of perhaps riot control and similar things. Then we tried to map the symptoms that are caused by those kinds of devices, and do a mapping from that back to what people were experiencing.

In doing that, we needed another set of data, which is what we are trying to put together to show that there are certain devices that you can use to detect events in those magnetic or soundwave spectrums. That meant that once you could define it – if your symptoms mapped to a certain set of knowledge that we knew they were testing – then we would, hopefully, be able to show the spectrum they were operating in and then say, “These devices will detect that.” You could then use that and detect them and take them to a court of law. At that point you would have documented evidence. That is our entire objective there – to get a rigorous, scientific process in place that will help people resolve these issues.



**C. Austin Fitts:** It would be a wonderful thing. Is there anything that people listening to this and who are interested in supported you do to help you with that effort?

**William E. Binney:** I recently returned from Europe. I was there, and half the time I'm out of the country and the other half of the time I'm back. I know that the online survey is available now for people to participate, if they so desire.

**C. Austin Fitts:** How do we find it?

**William E. Binney:** Can I get back to you on that? I'll send you the link. I've been out of the country for so long and doing so many different things legally that I can't keep up with everything, and I'm losing track of the names.

It's not that you're losing your mind, as you get older; it's that your mind leaks. You can't keep it all straight; there is just too much there.

**C. Austin Fitts:** It sounds to me like you have it pretty straight.

Clearly at this point the Trump Administration has to understand these issues of bulk versus targeted acquisition. Moser has done a good job in both *A Good American* and *The Maze* to describe it. In *The Maze* you walk through helping this wonderful group in Europe put together a new version of Thin Thread. It's pretty clear to any policy-maker or government official that it doesn't have to be this way and there is another way.

Is there any hope of getting the Trump Administration to move on this, or are they just simply too afraid to do it?



**William E. Binney:** We hope to be able to make that happen and I'll put it that way. Otherwise, the rest of the world is going to be doing something smart and we're going to be out in left field doing stupid things just to enrich, what I call, the 'military-industrial intelligence governmental happiness management' program.

**C. Austin Fitts:** Touché.

**William E. Binney:** That program is, "Get me money and I'll be happy." Unfortunately the problem with that is that we have to pay for that as taxpayers, and occasionally some of us have to die to keep it going.

**C. Austin Fitts:** I call it 'the tapeworm'.

**William E. Binney:** It's a leach, that's for sure.

**C. Austin Fitts:** There have been reports recently in the media that a portion of the Republican lawmakers are seriously considering not reauthorizing NSA's full authority on reauthorizations coming up. Can you tell us anything about that?

**William E. Binney:** Some of it is coming out because, for example, Rand Paul and various other senators have been saying that they have been spied on. I'm here to tell them that they've all been spied on and there is nothing new here.

**C. Austin Fitts:** Of course.



**William E. Binney:** Guess what? Join the new age, and you are it.

I said that these people are starting to wake up somewhere along the line, and they are beginning to realize how much leverage the intelligence community has on the members of Congress. They are all fundamentally under the thumb of the intelligence community, which I now call the Praetorian Guard. They are in charge, and they are the ones who are going to leverage everything.

They use the same tactics as the KGB. If they don't have something on you that they can leverage to get you to do what they want you to do, then they will find somebody you care about and find something on them, and then leverage them against you.

Sometimes I quote Wolfgang Schmidt, a former Lieutenant Colonel in the East German Stasi, where he said after he read about the NSA spying program, "For us, this would have been a dream come true."

That really says it all. In fact, there was an elderly couple in Germany when Tom Drake was there. They approached him after one of his talks and said, "You know, we are in a post-fascist state and know it, and you are in a pre-fascist state and don't know it."

It gets back to the concept that if you're not doing anything wrong, you have nothing to fear. It's a great quote, and I have three things to say about that. First, it's a great quote from Joseph Goebbels. Second, what you think is totally irrelevant. What you think is irrelevant; it doesn't matter. It matters only what the state thinks. Third, Goethe captured it very well a few hundred years ago.



He said, “No one is more hopelessly enslaved than those who falsely believe they are free,” which is fundamentally our state right now.

It should make us all very mad.

**C. Austin Fitts:** One of the reasons I insisted that we go to court when I litigated with the Department of Justice is they kept making things up and throwing it at me and it was all fabricated.

I forced them to go to court because they had to put evidence behind the allegations, and they couldn't. They cancelled the trial several times on the eve of trial; they loved to run up my expenses that way. I just kept refusing to settle, so they had to come to trial.

One of my attorneys who had been at this for seven or eight years turned to me. His face was white, and said, “Oh my God! They don't have anything.”

I said, “I told you that.”

He said, “I just couldn't believe that they would go this far when they had absolutely nothing.”

But I would see them again and again make up things and throw it at me. I can absolutely understand why a Congress member wouldn't want to put up with it.

I don't know if you saw Schumer's interview on one of the major media outlets essentially saying, “Trump can't do whatever he wants. You can't buck the CIA.”



He didn't realize it, but he was describing the governance system in this country as basically the CIA or the intelligence community indicating that the President of the United States, and the Congress have to do what the intelligence agencies want. You can't cross them.

What he was describing was an inversion of the governance system, and he was saying that the duly elected representatives of the US government are not in control and can't be in control; the intelligence agencies are in control, and that is a real governance issue. What we're really talking about is the battle of who is in charge.

**William E. Binney:** That's right. Schumer didn't actually understand what he was saying. It's much the same as the Director of the FBI, Mueller, who used to be one of my better sources of information because he didn't know what he was saying either.

An example of this is when he went before the Senate Judiciary Committee to testify on March 30, 2011. He said that he met with the Department of Defense, and they created a technology database that he could get into ('he' being the FBI), and, with one query, retrieve all past emails and all future ones on anybody as they came in. Well, that compromised the entire collection system of NSA because he said they had all our emails. That was an outright compromise of the Stellar Wind program, which is what Comey had objected during the hospital visit in 2004. But they never fixed that and Comey agreed to something that wasn't a fix.



I think it was the FISA Amendments Act of 2008, which simply created the 702 program that was the upfront charade of, “Here, we’re abiding by the law,” when, in fact behind the scenes under Executive Order 12333, they were collecting everything on everybody.

Even Representative Gowdy is under the impression that this is not happening. Guess what, guy? You need to start asking about the Fairview program and the tapping points inside the United States in Missouri and Iowa and so on. What are they tapping? Are they after foreigners? Well, listen, all the foreign communications surfaced along the coast of the country – the West and the East and the South – but where all the transoceanic cables surface is where all the foreigners are. So you can obtain them all there. So why are you tapping over here in Missouri and Iowa?

It’s not foreigners and I’ll tell you that: It’s us. That’s how they could do LOVEINT – love intelligence – at NSA because they were collecting local communications. That meant that their analysts could look into that data and see what their lovers were saying, who they were calling, and what they were talking about. That’s how they could detect that and that’s been the problem all along.

People aren’t putting very simple things together and saying, “You can’t trust the government. They lie to you.”

If they open their mouths, there is an 80% chance that they are lying, so go with the probabilities.



**C. Austin Fitts:** I heard you in a recent interview make a veiled comment about cyber security and the next big scam.

**William E. Binney:** Oh, yes, I call it a swindle. It's a basic swindle.

If you look at Vault 7 from CIA, which is fundamentally from NSA, the GCHQ, the other Five Eyes, and so on, it's an aggregate of attacking software. There are hundreds of millions of lines of code and there are thousands of attacks.

It meant that they knew all these weaknesses and all the systems for probably several decades, which meant that they kept them open so they could look in, see through a firewall, break in, and see what you're saying and what you're doing. They liked that and that's what intelligence people like; we prefer to see what other people are saying so we can detect what they're going to do.

The only problem is when you do that; I call this very shortsighted, finite thinking, because that meant that everybody in the world was vulnerable to attacks. Because they never told anybody, "Here is the problem with your software. You need to fix this." They never told anybody that because when they fixed it, the window on them would close and they couldn't read what other people were saying.

"We don't like that. Let's keep reading."



**William E. Binney:** So that meant that the OPM got hacked and the various other people were hacked. Every time they were hacked, they would say, “Cyber security is really important. We need more money for cyber security,” but they never fixed the problems that they knew about. So this is what I call a basic swindle. After all, if you want to do cyber security, do it and fix the problems you know about. Then maybe we’ll have some security. But in the meantime, stop asking for more money because you’re not giving anybody security.

**C. Austin Fitts:** Here is my question: If you study the plans of many different industries, they are planning on dramatic productivity increases as a result and major profits of the internet of things. Yet what we are also seeing is a complete lack of integrity and security in digital systems. How is this supposed to work? How are we supposed to run everything through the internet when there are this many examples of lack of integrity? I’ve never been able to understand how this is supposed to work.

**William E. Binney:** It’s supposed to work in a sense that they get all the information and we get the shaft. That’s been entire point. The internet of things is very dangerous now because what that means is they now have the capacity to see a lot more into our lives and what we’re doing. That’s a very dangerous thing to do.

I would say that if you have a device that is connected to the internet, disconnect it. Make sure that you get it disconnected. If you don’t, it’s another spying mechanism on what you’re doing.



**C. Austin Fitts:** I live in a small, rural community in Tennessee, and we have a great person who maintains and helps us get second-hand appliances that have no digital capacity on them whatsoever.

**William E. Binney:** Sometimes I've even been thinking about going back to analog because that is now secure.

**C. Austin Fitts:** I'm with you. You should see how far behind we are in Hickory Valley, Tennessee.

So what can we do? What do we do to protect our privacy in this kind of environment? Other than having 40-year-old appliances, what can we do?

**William E. Binney:** If you're going to go on the web, it depends on who you want to protect yourself from. There are various levels of protection. If you're interested in protecting yourself against NSA, GCHQ, and the Five Eyes; if they want you, they're going to get you. Period. There is just no way around that.

You can't stop them. Look at the resources they have. If they need more resources, they'll tax us for more resources. This is a form of insanity because we, fundamentally, pay for our own destruction.

**William E. Binney:** If you're interested in protecting yourself against local spying by different hackers or maybe some level of protection against people in other countries, I think you could do most of them. You could use programs like the Tor program, which would disguise your communications.



I always advocate inventing your own encryption system. This would drive them insane because you couldn't use these programs that are already there to automatically manage them with software. They would have to have somebody look at it to try to break into it to figure out what the properties were to develop a code to attack it, especially if you didn't tell them what the algorithm was.

The problem with the current commercially available programs are they all have to go through NIST for testing. When you give it to NIST, that's actually giving it to NSA. So they have all the software and know the algorithm behind all this.

It's a matter of them having that, and that's over half the battle of breaking a system anyway. I would not tell anybody and make a system and use it in your community of people – the people who you want to have secure communications with. Be creative and innovative. It will cause them a lot of headaches.

If several hundred million people did that, they would never get through it.

**C. Austin Fitts:** Right. Actually that could happen.

One thing that has clearly happened during the last five to ten years as more and more of the revelations have been revealed, it has inspired groups and countries around the world to pull away from our software, our systems, and try to create all sorts of systems that can be independent and protected from the NSA. Do you see that as a development as it continues?



**William E. Binney:** I do. When the Snowden material started appearing with the PRISM program and things like that, where you had companies that were participating in sharing data with the NSA, which was a direct violation of the constitutional rights of any number of countries around the world. I thought when that happened that was going to be a grand opportunity for other companies – in Europe especially – to begin to develop their own equivalency of Facebook and their own systems locally in the European Union and in the countries. I thought it was a great business opportunity for them, but they didn't seem to want to take it up.

I think perhaps now there may be some movement. For example, now we are supporting the EU movement to mandate targeted collection of data and make bulk acquisition of data illegal in the European Union. That's a good, positive step and will set the legal foundation. From there we can try to stimulate targeted development software and companies in Europe.

Those elements will come out of Europe, not the US.

**C. Austin Fitts:** Right. What can we do to support your efforts and those of your colleagues? You will send us the link for the online survey, but I know you're doing a great deal, whether supporting these different litigation efforts or simply just educating people through the media. What do we do to support you and make sure that you can keep doing what you're doing?



**William E. Binney:** The best thing to do, from my perspective, is to bitch and moan and gripe and groan to your local representatives and senators. The squeaky wheel gets the oil. I believe in being the squeaky wheel.

Let's be as squeaky as we possibly can, and bug them until they respond. Basically, threaten them with money, "If you don't stop this spying stuff, we're going to start contributing to your opponent or somebody who will. We're going to fire you in the next election." That is a threat that they understand.

**C. Austin Fitts:** Are there any particular Congress people who are very strong on this issue and are providing leadership that we can support?

**William E. Binney:** Bernie Sanders, of course, seems to be very strong on it, as is Rand Paul and Ted Cruz. I believe President Trump may be the one to do the action, though. He's not owned by any political party really and is the wild card. I think we have a really good chance of him standing up to this.

He's already said that he will return the US to a country of laws and abide by the Constitution. Well, if he does that, then this stuff stops.

**C. Austin Fitts:** He has obviously demonstrated tremendous courage on this issue. He has clearly communicated – whether it was what happened during the campaign or the leaking since he's been the President – and completely understands how destructive this is. It goes to the heart of a key governance question which is: Are our duly elected and authorized representatives the ones in charge, or are people who can fiddle with the communication systems and leak in charge?



**William E. Binney:** The fundamental bureaucrats are in place. I call them collectively a ‘petrified set of politicians in place’. I couldn’t think of another ‘P’ word.

**C. Austin Fitts:** How do we stay current on your work? What I do every week or month is a search on your name and see what you’ve been up to for the last couple of weeks. That seems to work perfectly well, but is there any other way to keep up with you?

**William E. Binney:** Actually, [www.ExposeFacts.org](http://www.ExposeFacts.org) is a website that usually carries some of the things that I do. Also AGoodAmerican.com has a lot of information on me. Otherwise, if you Google my name with the date, you can usually see what I’m doing during that period of time or when it gets posted. Sometimes it’s not posted until later.

I think that what you are doing is probably the best way to keep up with me because I don’t even know where I’m going. I get calls from all over the world to do things, so I react as best I can to do that.

**C. Austin Fitts:** One of the hardest things to find in this world is somebody who understands the systems and can communicate clearly and has integrity. That puts you in a very small group. I can imagine that the demand for your service is going to continue to rise.

Before we close, is there anything else you would like to communicate to our subscribers? Is there anything we should have covered that we didn’t?

**William E. Binney:** No. I just think that if you have the opportunity, sue the bastards! Get them into court. That’s the way to do it.



**C. Austin Fitts:** Actually, it is.

**William E. Binney:** They keep talking about Julian Assange and all these people who are exposing all the crimes they're committing. The only reason they are doing it is because they are playing the *Wizard of Oz*. "Don't look at the man behind the curtain; focus over here at the bad guy. Here's the bad guy. Don't look at what I'm doing; look over there."

That is fundamentally what they are doing, and they use an old sophisticated technique of repeating a lie over and over again or an assertion over and over again, expecting that after so many repeats it will be believed as truth instead of actually looking at it with a critical view as to what the founding basis of making those kinds of assertions or allegations are. That is one thing that they are doing, primarily with the Russians and some of the other things currently happening in this country.

**C. Austin Fitts:** Before I litigated with them, I thought that they were far more powerful than they are. I underestimated how the rules of civil and criminal procedure require them to show evidence. There is a lot to be said for our legal system.

**William E. Binney:** Absolutely.

**C. Austin Fitts:** When you get them in court and they have to pony up, it's pretty interesting. I agree with you. We're going to have to find many courageous attorneys, and the more we can pile into court, the harder it's going to be for them – especially if we're all coming up with private encryption systems. I like that!



**William E. Binney:** Be creative, and have fun at the same time. It's like, "Aha! I got you."

**C. Austin Fitts:** Previously, you would be able to see on your website the specifics of who was coming in and reading the documents. I ended up putting many of the legal documents on our website. It was part of the way we did the public relations by making it all accessible.

Over time, some of the attorneys on the other side got lazy, and would come in and use our website. So by watching what they were reading, I could tell what they were up to. It was quite remarkable. So they spied on us, but we spied back on them; it was good.

**William E. Binney:** That's what I did internally at NSA, also.

**C. Austin Fitts:** Really?

**William E. Binney:** Oh, yes! I would give a talk on technology or what our developments were at that time, and then I would go into the network – my monitoring network. I had a record of everybody who came in and what they did and how long they stayed and where they went. So I would go in and look at that and say, "Oh, I know what they are about. I know what their entire objective is."

That's definitely a good technique.

**C. Austin Fitts:** Bill Binney, you are truly a national treasure. I can't thank you enough for everything you've done. I really appreciate the opportunity to have you on The Solari Report.



If there is anything we can do to support your work, please keep us posted. We would be delighted to do so.

**William E. Binney:** Thank you, and thank you for having me.

**C. Austin Fitts:** Have a great day. Goodbye.

**William E. Binney:** You, too.

## MODIFICATION

Transcripts are not always verbatim. Modifications are sometimes made to improve clarity, usefulness and readability, while staying true to the original intent.

## DISCLAIMER

Nothing on The Solari Report should be taken as individual investment advice. Anyone seeking investment advice for his or her personal financial situation is advised to seek out a qualified advisor or advisors and provide as much information as possible to the advisor in order that such advisor can take into account all relevant circumstances, objectives, and risks before rendering an opinion as to the appropriate investment strategy.