

WILLIAM BINNEY

‘We Are Watching Our Democracy Go Down the Drain’

Jason Ross of the LaRouche PAC Science Team interviewed William Binney on May 5.

Jason Ross: Hi, I’m Jason Ross, and I’m very happy to be interviewing William Binney, a former senior National Security Agency (NSA) official. Mr. Binney served in the NSA for more than 30 years, including as technical director of its World Geopolitical and Military Analysis Reporting Group. He worked on developing many of the technologies still used by the NSA, and he resigned in 2001 over the potential for a totalitarian, as he put it, Orwellian state, in which the technical means to spy on every American were being developed.

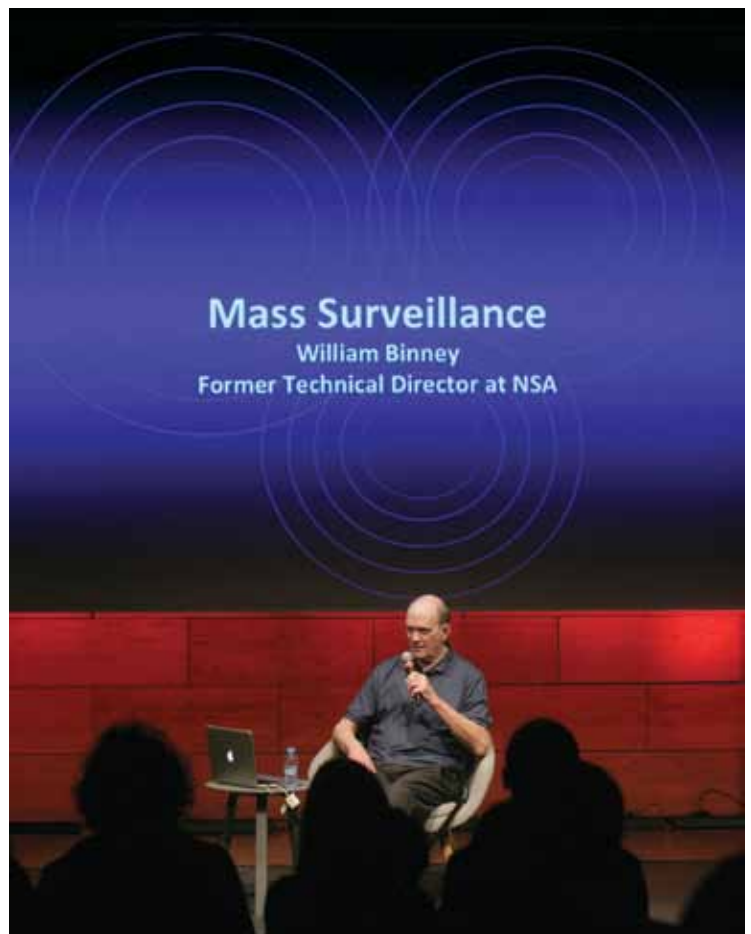
Let me ask you: Ever since Donald Trump won the Presidential election, there has been a drumbeat of attacks, stating that Russia threw the election to Trump, by hacking and releasing emails, by hiring Internet trolls, by collecting blackmail material, and other means. These claims have come from political circles, intelligence circles, former British MI6 agent Christopher Steele, and others.

Let me ask you, Mr. Binney: What do you think about these claims? Did Russian hackers elect Donald Trump?

William Binney: I wrote an article that was published in *Consortiumnews* on Dec. 12th of last year that said this was all a big fabrication, simply because they weren’t saying exactly where the hack came from and where the data out of the hack went to. That’s the whole point of what NSA has set up, in terms of copying and collecting everything in a fiber network inside the United States, and virtually everything in the world on those fibers.

That means—and they’ve got trace route programs by the hundreds, scattered all over the world—that means that they can follow the [data] packets as they move through the net-

work. Now, if somebody hacks into the DNC [Democratic National Committee] or Hillary [Clinton’s] or [former Clinton campaign chairman John] Podesta’s email or something, and they want to find out who it is, all they have to do is use the IP address with XKey-score, as Edward Snowden said, and they’ve got all the data to find out where the packets went. But they haven’t done that. Even NSA, which is the only agency that can do this—the rest of them are meaningless—if NSA says they’ve got data on it, then it’s meaningful. If the rest say that we have “high confidence,” that’s just pure



Miquel Taverna/CCCB

William Binney

speculation, that's just pure garbage, that doesn't mean anything. Produce the evidence! They haven't produced any at all. So that's what I called it back in December of last year.

Ross: More recently, about a little over a month ago, you co-authored [an article](#) with Ray McGovern in which you wrote about Trump's response to this, that "his choice may decide whether there is a future for this constitutional republic. Either Trump can acquiesce to or fight against a deep state of intelligence officials who have a myriad of ways to spy on politicians and other citizens, and thus amass derogatory materials that can be easily transformed into black-mail."

That's a strong claim. Tell us, how do you see the Trump response to this attack on elected government? And what should ordinary people do, to prevent such a policy coup?

Binney: First of all, I think President Trump realizes what's been going on. A recent statement he made about, "there's an awful lot of spying going on [against] U.S. citizens, and we really don't know the extent of it, and we really have to find out what the heck"—he used the word "hell"—"what the hell is going on." Well, that means they're even keeping him in the dark.

Now, as the President of the United States, he's supposed to know all the sources of information that the intelligence community is using to produce intelligence for him, and he obviously doesn't know about this. But I've made it perfectly clear that the "Fairview" program, "Stormbrew" programs, and "Blarney" programs for the tapping of fiber networks inside the United States are their sources of information on everybody in the United States, including representatives in the House and Senate; you know, even judges on the Supreme Court, Generals on the Joint Chiefs of Staff, all Federal judges, all senior lawyers in law firms all around, and all the journalists and everything; all that stuff is being captured and stored.

And what they're not talking about is—I've seen some arguments where they said, "Well, as long as we're only using it for intelligence, and law enforcement isn't involved, you know, it's okay for us to do that." That was the argument I think that Judge Napolitano put forward, that they were using with the FISA [Foreign Intelligence Surveillance Act] Court to dupe them into doing what they want.



U.S. Air Force photo/Staff Sgt. Jonathan Lovelady

U.S. Army Lt. General Michael Flynn testifying when he was director of the Defense Intelligence Agency, Feb. 4, 2014.

And that's really what's happened. They've been duped, and so have the Congress, most of Congress. The intelligence committees, I think, were more aware of what was going on than the rest of Congress. But they duped the rest of Congress! They made them all just play along like a bunch of sheep—"here's the bell, follow the bell." So, our democracy basically doesn't really exist the way it was originally intended. And the law enforcement—FBI, DEA, and others in the law enforcement community, had direct access into the NSA data, they've had it all along! Director [Robert] Mueller at the FBI said he'd been using the Stellar Wind, which is the domestic spying data, since 2001, he'd been using that, and that's direct access through their technology data center in Quantico, Virginia into the NSA databases where they could look at all the content and meta-data of everybody in the country. And they could retroactively research them any time they want.

And they're using it to arrest people for common crimes inside the United States. So this is simply a destruction of the entire judicial process in our country, and it's a fundamental violation of constitutional rights. They've scrapped the Constitution, fundamentally.

That's why, when the Iraqis were struggling to put together a Constitution, I said, "Well, why don't we give them ours? We're not using it."

Ross: One specific example of that recently is [former DIA and former National Security Council Director] Michael Flynn, who, his conversations with a

Russian diplomat were recorded, which happens, but then the unmasking—it was reported that was done by Susan Rice, Obama’s National Security Advisor. As you put it, this sounds just like what J. Edgar Hoover used the FBI to do: collecting blackmail material to exert political control. What must be done to prevent such control, such blackmail potential through agents operating through the intelligence sector? What do we do about this?

Binney: You have to have some Attorney General who will take action to stop this. This is a violation of the fundamentals of the Constitution and the Bill of Rights, and also a violation of the existing law. They tried—like in 2008 when Congress passed a retroactive immunity for the telecommunications companies. That was because these companies were giving them access to the fiber lines, and letting them take all the data off the fiber lines, and because they were also giving them all the data on all their customers. It was trying to retroactively give immunity to people who were committing an unconstitutional act—which is unconstitutional and therefore not a law.

That’s why I’m supporting four separate attempts to challenge that in federal court. We’re challenging them based on the constitutionality of what the NSA is collecting. Once that challenge gets up, and gets into the Supreme Court—it’s obvious that it’s unconstitutional, any idiot can see that. What that means is that once it’s declared unconstitutional, their whole house of cards falls. All those laws they tried to pass to protect people also fall, because they are not constitutional. You can’t authorize an unconstitu-



CC/George Rex

Sign in Britain referring to the UK’s Government Communications Headquarters.

tional act with a law. That law is not a law, because it doesn’t conform to the Constitution.

So, these are the things I am trying to do. I think everybody should challenge them in federal court, but also the political way to do it is you need to fire people on the intelligence committees, because they are advocates for this kind of crap. They are also part and parcel of covering up what they are really doing to the rest of Congress. You need to focus on them, and also in the courts, and get the courts to recognize what’s really been going on. They are so afraid of doing anything when it comes to national security, because it’s such an unfamiliar topic to them. But the Constitution is not an unfamiliar topic. All they have to do is pay attention to that and rule based on that. That’s the simple answer.

The British Police State

Ross: On the international side of this, according to recent reports, some of the initial launching of these investigations into Trump were sparked by interventions from the UK, as were the totally deranged reports coming from MI6 agent Christopher Steele, including salacious claims about Trump’s behavior. Under the “Five Eyes” arrangement a lot of intelligence sharing occurs between the NSA and, for example, the UK’s GCHQ [Government Communications Headquarters].

Let me ask, is having a foreign country with an unsavory and imperial history being so tightly tied to our intelligence services—is this a concern for you? How do you see this international partnership?

Binney: I think it’s gotten a little too involved, in my view anyway. For example, other than the





defenceimages.mod.uk

Aerial view of the GCHQ in Cheltenham, Gloucestershire.

law enforcement and now other intelligence agencies that Obama had opened up the NSA data to, the people with direct access to the NSA database are the “Five Eyes” countries [United States, Canada, New Zealand, Britain, and Australia]. GCHQ has had it since 2007 at least, and the others were following that probably in 2008 or 2009. So that means that they can go in directly into the database too. And when you do that, you can actually pick and put in place and select the kinds of information you want and ignore the rest.

In other words, if there is exculpatory data in there about the Trump campaign program or anybody involved in it, they may simply be ignoring that, and only putting forward something that may indicate that they were involved, might indicate a suspicion or something. So it’s a matter of selecting the data that you look at, instead of looking at the whole set of information to get an overall picture. That’s one thing I don’t trust them to do. First of all, they are even messing up their own country with their investigative powers bill. At least they openly admit they are going after everything everyone is doing on the web, and they are trying to get the companies, the Internet service providers, to provide it to them, and do a lot of work for them against everybody in the UK, as well, who are using the web and acquiring things on the web. They want them to create an Internet connection record, is what they call it. They were estimating about 60 billion records, Internet records, per day, for British citizens alone. But

they’ve got a large access to the transoceanic cables going from Europe to America through Bude [in Cornwall] and a couple of other places too. That gives them a lot more than that. The British part of it is just bad enough for them, but also they’re getting all the records on U.S. citizens that are routed through any of the access points that they’ve got. I think it’s really a situation that needs some effective monitoring. The oversight we have now with the FISA court and the intelligence committees is a farce, it’s a joke. They don’t do anything; they can’t achieve anything and they can’t verify anything they’re being told by the intelligence agencies. So it’s really a

sham, it’s a charade.

Ross: This might be asking you to speculate, but you had mentioned how there is a potential for spying on federal officials, judges, top level political layers inside the United States. The intelligence committees themselves I would imagine would be a prime target for this sort of compromising type of control. Do you think that is a factor in the cowardice being shown by the intelligence committees?

Binney: Yes, that’s part of it, because even when Senator [Chuck] Schumer [D-NY] warned President Trump that he shouldn’t go after the intelligence community because they’ve got many ways to get back at him, well, this is exactly one of them. What that’s really saying is that everything they’ve done electronically has also been captured, and they can go back and look at everything they’re doing, and everything they’ve ever done for the past 10 or 15 years. That’s definitely it. We had another whistleblower, Russell Tice, who had made it perfectly clear that this is the kind of activity that is going on. He even said that in some of the areas he was, where he saw this data, he saw the transcripts of phone calls of the then-Senator Obama.

I’ve been calling it the imperial guard—for the Roman Empire their imperial guard basically determined who the emperors were and what they did. That’s what is happening here with the intelligence community.

Ross: Do you know if there was a lot of push-back or fight around the Five Eyes sharing, around giving access to such sensitive material to foreign governments?

Binney: I've never heard any opposition to that at all. Because fundamentally the Five Eyes are the ones that are doing this worldwide bulk data acquisition. They are the core of it. There are about eight or nine other countries around the world that are also participating, and they've got limited access to that data. But the core is the Five Eyes, and I believe they have almost unfettered access to it.

Ross: You had mentioned that you are pursuing lawsuits as a way of challenging these activities through federal courts. How are those proceeding?

Binney: They are still going, but the Government is trying to slow roll them because they know that when it comes to the Constitution and what they are doing, that they are actively performing unconstitutional activities, and they don't want it exposed in federal court or to the public because all of those activities are fundamentally impeachable offenses—that's what we impeached Richard Nixon for, violation of constitutional rights of U.S. citizens. That's exactly what's going on now, except now it's involving everybody. Back then Nixon could only handle a few thousand people. With the FBI, NSA, the CIA—all of them are doing it now. You had the CIA break into the Senate when they were writing that summary paper about the torture; you had them break into their servers. They got caught at it anyway.

Ross: And didn't exactly receive much punishment for such a brazen act.

Binney: Well what can you do when people have the goods on you? Who is going to do anything against them?

Spying and Blackmail

Ross: This is something that people have to be aware of, understanding the potential of the use of blackmail, and certain agencies that are collecting the material for it. That makes it possible, I suppose, to inoculate or immunize against the effects of being able to bring out a scandal on demand, if people are aware that's used as a political technique and its origins.



CCBY/Timothy Krause

Eliot Spitzer, former New York Governor and prosecutor.

Binney: Yes, and they use it internationally too, it's not just in the United States. They used this against Jim Rosen, the Associated Press, other reporters, the Tea Party, the Occupy group— anybody who is doing something that they don't particularly care for, they go after and try to get rid of them, like General [David] Petraeus, General [John] Allen, and also [former New York Governor] Eliot Spitzer. They went after Spitzer—he was going after the bankers for defrauding people. The problem is the way the banks were packaging the deals. They were forced by Congress to approve loans that couldn't be supported by people getting them. That made that a bad investment, so they had to package it. Then they sold these packages around the world, and they fraudulently advertised them. That's what Eliot Spitzer was going after them for, for fraudulently soliciting people to buy these packaged deals, and they had to stop that because it would lead back to the Congress of the United States. That would expose them, so they had to stop it. So they got rid of Eliot.

What was the probable cause for anybody to investigate Eliot Spitzer? I can't think of one except, "Oh, he's going after our bankers."

Ross: In the aftermath of the revelations of the spying on [Martin Luther] King, there was the Church Committee [chaired by Senator Frank Church (D-ID)], there was the efforts of Congressman Neil Gallagher [D-NJ]; this is when the intelligence committees were

created. Was that an effective push-back at the time? What would something like that look like today?

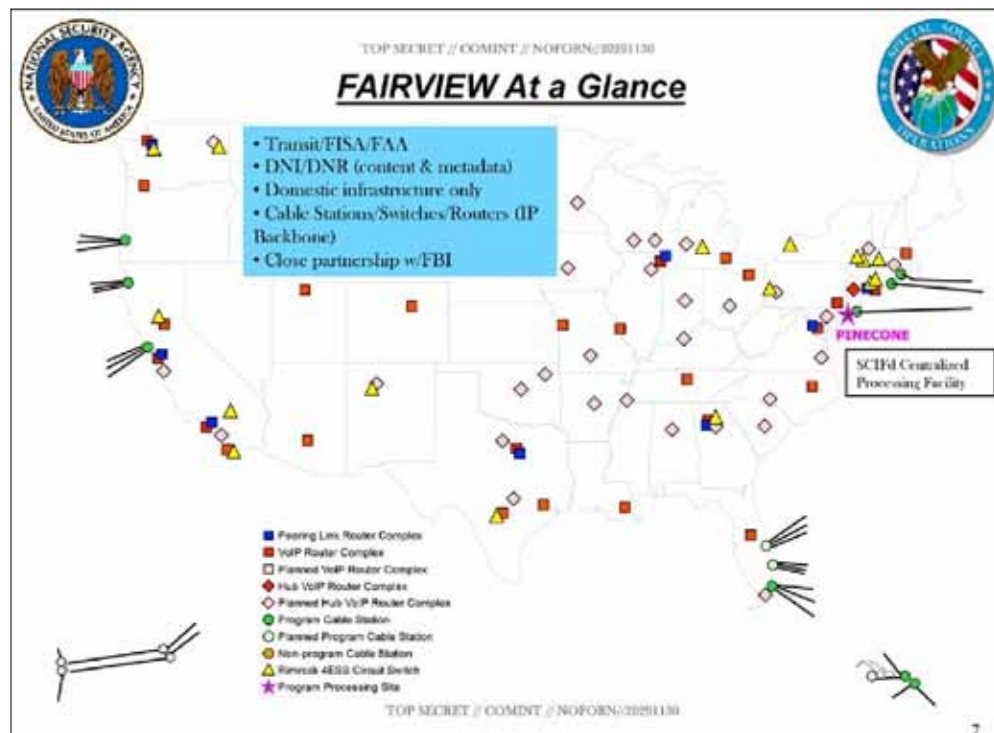
Binney: I think fundamentally we need another Church Committee that is open to the public all the way, that isn't hidden, no closed sessions at all, especially when it comes to exposing violations of our constitutional rights and the rights of people, period. I think that this needs to be out in the open and those who are doing it should be held accountable in the open. If it comes to indicting them, I think that that is a proper way to do things, that they need to be indicted, and the law should be adhered to—in my view anyway.

Ross: One more technical question before a summary. At the opening you had discussed how, if Russian hackers had really gotten these emails and released them, the NSA would have been able to find out about that given that the NSA sees all Internet traffic. Some people say, however, that Tor is something the NSA isn't able to unravel completely. Would that have provided a potential technical means to make it possible to hide the tracks, moving the data around?

Binney: No, I think they could have at least gotten some of the packets. That's one of the reasons they put all the trace route programs in hundreds of switches on the Internet around the world. That's because they are tracing all the packet routes to try to reconstruct Tor. That was one of the purposes of it.

Ross: Is there anything else that you would like to say to our listeners?

Binney: The law enforcement use of this data is just outright disgraceful, and I would also point out that [FBI Director James] Comey has known about all of this material and the use of it since at least the hospital visit in 2004 to [former Attorney General John] Ashcroft, when



Schematic diagram of the NSA's Fairview surveillance program.

Ashcroft was in the hospital and Comey was acting Attorney General, and he [Comey], at that point, refused to renew the program. He's known about it since then. All this business of saying, "Well, the Trump Tower, there was no wiretap directed at the Trump Tower." That's correct. Wiretapping is basically obsolete. That *word* is obsolete. Everything now is surveillance, and it is constant surveillance of everything. All of that data is captured and stored. So it's not a question of wiretapping any more but of targeting in the database that's been captured. If somebody wanted to go after then-candidate Trump, they would have gone into that database with his signatures and to go after all the data about him. That's targeting—once you've captured the data. Wiretapping is to get the data and capture it. The constant surveillance gets all that data anyway.

Ross: So there would be no need to have specific wiretapping of Trump, because everything is already collected?

Binney: That's right. It's a word game. Everything is a word game with these people now in the public. The public is being duped by this word game. That's all. And unless you know the ins and outs of what they do and how they do it, you think it sounds reasonable.

End of Constitutional Protections

Ross: It used to be that people were given the impression there was an absolute wall between intelligence gathering and criminal prosecution, where for example, there was a much lower bar for wiretap surveillance for national intelligence purposes. It seems like, from what you have been saying, that that barrier has been almost entirely eliminated. Is that true?

Binney: Yes, that's right, since 2001, according to FBI Director Mueller. He made that statement to Bart Gellman when Bart did an interview with him in 2011 for *Time* magazine. That's also on the web. The way he put it was we had been using the Stellar Wind program since 2001. You have to know what the Stellar Wind program is. That's the domestic spying data, the content and metadata of domestic spying. That's from the Fairview, Stormbrew, Blarney programs, where there are more than a hundred taps inside the United States are collecting all this data off the fiber network.

The Function of Intelligence Has Been Lost

Ross: You had proposed a different method of collection entirely, that you believe would have made it possible to safeguard privacy.

Binney: And also to succeed in stopping terrorism. Because now what they have is too much data altogether. They can't get through it in time to assess threats, so they can't stop the threats. People get killed, then they go clean up the mess. Then they go after the people they knew did it because they have lots of data already stored on them. From there on it's like forensics. Intelligence has become a forensics job, a police job, after the fact, after the crime, when in fact the purpose of intelligence is to predict intentions and capabilities of adversaries in advance so you can do something to stop it.

They've lost that entire perspective. We are paying tens of billions of dollars to capture everything (every year, by the way), and actually are not able to use it or do anything with it. That's the big swindle that we're all under now: We are doing this collection of *everything* for terrorism, and yet you can't do a thing to stop it because of all you've collected. Then a terrorist attack happens they say we need more data, more money, and more people. They are building an empire at the expense of the few people that have to die now and then, to keep the program going.

Ross: Do you see this as a funding or an allocation of resources issue? Also as a methodology problem, in

terms of the approach that analysts are taking to the use of data that we do have?

Binney: It's basically a combination of all of that. Fundamentally the motivation of these agencies is to swindle the public out of money, to build a bigger empire, intelligence empire, contracting empire, and governmental empire. It takes a lot of people to do all of this collection, and a lot of contracts and a lot of contractors to be involved to make it happen. So that's an empire you build and it costs a lot of money to do it. I reckon they're spending \$100 billion a year on the intelligence community, all 17 agencies. Whereas, if President Trump wants to build a wall, he can take \$2 billion out of CIA and \$2 billion out of the NSA program every year and they wouldn't miss it. It wouldn't affect them at all. They couldn't do any worse than they are doing right now anyway.

Ross: Is there anything else you would like to add to conclude?

Binney: No, except the law enforcement use of this data is corrupting our entire judicial process. It's really making a sham of it. I would add one case, "Amnesty International vs. Clapper," that made it all the way to the Supreme Court. When the Solicitor General of the United States argued the case of the Government against the Amnesty challenge—Amnesty charged that the Government was using data to criminally convict people without telling them the source of it, thus preventing any challenges under the discovery rules, as is their constitutional right in a court of law, to challenge any of the discovery material used against them in a court of law. But the Government couldn't confess openly that it all came from NSA because all of that data was acquired without a warrant that meant it would be thrown out, which meant that the Government had no case. So they had to do these parallel constructions, create the data, and use that as a substitute for the NSA data in a court of law. That's a violation of the principle of all the constitutional rights of citizens. And it really makes a sham of our entire judicial process. We are actually watching our democracy go right down the drain here.

Ross: Thank you very much. This is certainly a very sobering assessment. I think it's a good kick in the pants for people who aren't aware of this, and provides some opportunities, some avenues of what can be done about it. So, William Binney, thank you very much.

Binney: Well, thank you.