

The NSA Scandal: Economic Espionage against Germany? Is Germany's BND a Subsidiary of US Intelligence?

Interview with William Binney, former Technical Director for Intelligence at the U.S. National Security Agency (NSA)

By [Lars Schall](#)

Global Research, November 06, 2014

[Lars Schall.com](#)

Region: [Europe](#), [USA](#)

Theme: [Intelligence](#), [Terrorism](#)

William Binney, former Technical Director for Intelligence at the U.S. National Security Agency, talks in this interview with German financial journalist Lars Schall about, inter alia: NSA's digital surveillance as the STASI on super steroids; the relationship between NSA and BND; the fear-mongering of terrorism; and what went wrong when it came to uncover the 9/11 plot.

William Binney, who grew up in the US state of Pennsylvania and graduated with a Bachelor of Science degree in mathematics from the Pennsylvania State University in 1970, was a 36-year career official at the NSA. Having expertise in intelligence analysis, traffic analysis, systems analysis, knowledge management, and mathematics (including set theory, number theory, and probability), Binney has been described as one of the best analysts in NSA's history. He resigned in October 2001 as Technical Director for Intelligence at NSA. Since then, he expressed massive criticism of the monitoring programs of the NSA and the related violations of the US constitution. Moreover, he founded Entity Mapping, LLC, a private intelligence agency together with fellow NSA whistleblower J. Kirk Wiebe to market their analysis program to government agencies.

Lars Schall: Bill, you were invited this year as a witness by the NSA commission of the German parliament, the Bundestag. How has it been to speak there and what did you try to get across?

William Binney: I was there for about six hours testifying with a half hour break in the middle. So it was quite intense. There were so many questions. Some of them I didn't have answers for because I didn't have knowledge about it, and I tried to make those clear and tried to give them information about things I knew personally, so I didn't want to extrapolate beyond that. Initially, they were asking questions about my background which was, I guess, setting the stage for the follow on questions, but in the long run they were interested in the relationships with the BND and the NSA, and I think part of the break in the middle had to do with something that happened there and that was a BND person was implicated in spying on the commission when it was investigating the relationship, and they were also passing that information to NSA, at least that was alleged at that time, I don't know if that's true or not.

Anyway, it was quite lengthy and very thorough, and my whole point was to try to get across to them that what NSA and the intelligence community in the Five Eyes at least and

probably in some of the other countries, I don't know exactly which ones and I've made this clear, but I think they're not doing alone, and it's the idea of collecting massive amounts of data is just like the STASI – except this time I kind of tried to get across to them that it's like the STASI on super steroids. As Wolfgang Schmidt, the former lieutenant colonel of East German STASI, commented about NSA's surveillance program: For us, this would have been a dream come true. Well, that's the whole point of it, it's so invasive, it's digital surveillance on a massive scale, and I tried to get that across to them. Because this is basically a fundamental threat to our democracy and every democracy around the world, you know I call it over here in the United States the greatest threat to our democracy since our Civil War.

LS: Were there some questions that you would have expected that were not asked?

WB: No, I think they pretty much asked all the relevant questions, some of which I dealt with in close session, especially in dealing with the relationship between BND and NSA that I knew, I addressed those in close session.

LS: What's your view on how Germany is treating Edward Snowden?

WB: I think for the most part he got a lot of popular support in Germany. I think the government there is a little bit sensitive to it simply because of the close and enduring relationship between the United States government and the German government. So I think they're trying to balance an act there between support from the general populace and also support for the US government from the existing agreements and cooperation with the German government. They have to balance that.

LS: What's your overall view on how the German government behaves in the NSA scandal?

WB: My personal believe is that they only now are starting to get into it and only now they are beginning to realize, just as over here Congress is beginning to realize, how much they cannot trust our own intelligence agencies, and this is evident for example from last year when two representatives attempted to get a bill passed in the House of Representatives to un-fund the NSA activity. Basically, they just found out through the Snowden releases that a lot of the information they were been fed by the intelligence agencies and the administration was not true. And so they finally began to realize what was going on and tried to get an initiative to stop it, and that's when the president and the director at the time of NSA, Keith Alexander, lobbied the House of Representatives very heavily to defeat that bill, which they did, but the bill only lost by twelve votes in the House of Representatives – so that's not a bad deal, it was a fairly close vote, and still the issues are still going on over here and politically people are still talking trying to resolve it and we are trying to help them with that by publishing articles and things that we send over to Germany as well as the things that need to be done to ensure that these intelligence agencies are kept inline by their governments respecting the rights of their citizens.

LS: A few months ago it was revealed that the NSA could have had access via the Bundesnachrichtendienst (BND) to data at the DE-CIX internet hub in Frankfurt. If this was the case – the DE-CIX Management GmbH Frankfurt denies that this took place (1) –, the BND would have violated German law. Can you tell us, please, how such arrangements between NSA and BND come about that are including breaches of law?

WB: The agencies like NSA and BND would set up a separate international agreement

between the two agencies that would have to be passed and approved by at least some portion of the government, that is your government would need to agree to it and so would ours, and that's starts with the agencies agreeing on what to cooperate on and how to cooperate and what the ground rules are for that cooperation, and that's then passed to the House and Senate Intelligence Committees or very restricted numbers of people in administration would also be able to see that kind of agreement, and the same would be true I assume on the BND side and the German government, there should be some small subset of the German government that's aware of these agreements and is monitoring them, though I don't know what the conditions are there within the BND and how they do it, within the United States it's the House and Senate intelligence committees and the FISA court that is supposed to oversee that these things don't violate US law, but in fact, what they have been doing over here is advocating violation of US law. They are enabling that - it's not the question of them doing oversight, they aren't doing it, they are enabling it.

And of course they are all doing it on the basis of fear-mongering of terrorism. They try to get everybody afraid so they will do whatever they want, that's the kind of leverage that they are trying to use not just against the public, but also against Congress. It's just all based on fear-mongering. The whole point is to get more money and build a bigger empire which they have done. Over here, we've spend for all the 16 agencies close to a trillion dollars since 9/11. That's really been a money-making proposition for them, this fear-mongering. Now they are doing it with cyber security. It's how you control your population, how you manipulate them and how you let them pay for things you want done.

LS: Is the BND merely a subsidiary or branch of the US intelligence apparatus?

WB: I wouldn't call them a branch, but they are certainly a cooperating partner. Again, it's all written out in agreements as to what the efforts are that they jointly share and work together on, that's all written out in agreements and approved again by their agency's heads and then it goes to certain parts of the governments for approval also. That's all laid out and defined in those agreements. I wouldn't say that they're working totally for them, they have their own agenda and own priorities. The cooperation occurs where there's common interest and common concern about given activities, like terrorism or maybe dope smuggling and things like that.

LS: Is the NSA engaged in economic espionage related to Germany? And if this was the case, wouldn't it be the task for the BND to prevent this from happening?

WB: You would think so. I can only assume from what it's been printed that this is happening, but the question really becomes whether or not it is shared with US companies to give them advantage in competition. I am sure that all governments around the world do this to some degree, depending on their capabilities and resources primarily. The question becomes whether or not it's shared outside of the government channels to industry for example to gain advantage. You would expect that government people are keeping it within, but the problem here is in NSA: a good many of the people who are managing all the data that would contain that kind of information are in fact contractors working for other industrial partners in the United States. Some of them like Boeing have many interests and so does Lockheed Martin and so on, these are corporations where people are running that data and managing that data for NSA. So they have access to it. What they are doing to it, is another question, but it's a very risky situation in terms of industrial espionage.

LS: Your own career at NSA culminated as Technical Director for Intelligence in 2001. The

very same year you retired. Why so?

WB: What happened after they wanted us to stop doing the ThinThread program, which was the one that solved the massive data problem related to the internet communications, and so it was a cheap solution and they had to get rid of us, so that's what they did, and as part of that process they had to remove me from that rather high position I had and put me into a smaller position which was out of sight basically. They didn't want Congress or anybody else be aware of what I was doing or have access to me. That's generally what they do when they don't want people doing things, they move them out of their way.

LS: What did NSA wrong when it came to uncover the 9/11 plot? Edward Snowden "suggested that the United States had the proper intelligence ahead of 9/11 but failed to act." (2)

WB: Yes, that came out of Tom Drake's use of ThinThread to go through the entire data base at NSA, he went through the data and analyzed it after the fact in early 2002, I believe, and he used the ThinThread program. He found out that NSA had in fact in its data base prior to 9/11 all the information necessary to find out who was involved, where they were - you know, to put the whole thing together and be able to stop it.

See, the problem with industry so involved in this and so inculcated inside of NSA - I mean, they are inseparable, they work in the same spaces, and when you do that they have a vested interest in continuing to get the next contracts so that they can keep getting more and more money. So what happens is, they try to keep the problem going instead of solving it. So they only do incrementally improvements over time, that keeps them in the primary position to get the follow on contracts to keep working on it. That's basically how they've been doing it, and they've been doing it for decades, by the way, it's standard practice that they use.

LS: Do you think the expansion of various NSA programs in reaction to 9/11 is justified?

WB: Absolutely not! That's what I opposed right away. They should have stopped it by using automation against a focused target set for acquisition of information. In other words, they knew the basic targets and people connected to them or those that were in close relationship with them, and they could define that and pull that data out and focus their analytic effort on that and solve that problem, but they didn't. Instead they decided to build a bigger agency and that they wanted a much larger budget and a much larger set of contractors and contracting agents. That was the path they took. I called that sacrificing the security of the people of the United States and of the people of the free world for money.

LS: NSA whistleblower Thomas Drake stated also in an interview with me that the nexus 9/11 - War on Terror is used as an excuse to expand programs that were existing pre-9/11. One example, I think, would be Echelon. Could you tell us about the development of Echelon, please?

WB: I don't know too much about what happened with Echelon, because that didn't really deal with the fiber optic lines, and that's really where the explosion occurred. The explosion in communications was occurring with the fiber optic lines. There are three types of attacks on it: Either they get corporate cooperation with the telecom companies or the companies running the fiber lines, and if they have that with or without the government's knowledge, local government if it's foreign, they may or may not let them know, in that case they can

go directly to the company to get an agreement, and if they do that, then they can tap the lines there and do the acquisition there. On the other hand, if they don't have a company doing that, then they can go to their counterpart in the government to try to get an agreement like in Frankfurt to try to get taps on that line or in other places, and if that's agreed, then there's a governmental approval to do that, at least in part by the agency involved, if not by the government itself too, I don't know that – I mean, that would be the part that would have to be investigated. And the other possibility, if they can't get a governmental cooperation or corporate cooperation, then they can unilaterally do it – that means they have ways and means to get access to the fiber lines without the cooperation of the government or of the company involved. That's like the taps that they put on the lines between Google and all the major internet service providers when they are transferring data from their major storage centers back and forth, they put taps on those lines without the knowledge of the companies. That's the kind of thing that they would do with anybody else that wouldn't cooperate. In other words, if you want to find out if your lines are tapped, you would need to trace the line all the way through.

LS: On August 17, 1975 Senator Frank Church stated on NBC's "Meet the Press":

"In the need to develop a capacity to know what potential enemies are doing, the United States government has perfected a technological capability that enables us to monitor the messages that go through the air. Now, that is necessary and important to the United States as we look abroad at enemies or potential enemies. We must know, at the same time, that capability at any time could be turned around on the American people, and no American would have any privacy left such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyrant, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology. I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That is the abyss from which there is no return."

How do those words sound today?

WB: They were right on the money. Frank Church captured it right away. The point is that they are in the process of perfecting this whole operation, and the point is that now that everybody has a greater capacity to communicate the invasion of privacy or the intrusion into what people's lives is all about is even worse than what Frank Church could have known. Back then he was only thinking about and looking at the landline telephone calls, where now it's not only that but also mobile phones, satellite phones, the internet, the computers, the tablets, and so on. All the networks people are carrying around. There are at least over three and a half billion phones in the world, and something very similar in terms of computers. The explosion has been tremendous both in terms of volume and in terms of numbers. Frank Church couldn't have dreamt about that in his time; he was just talking about a smaller segment of what was available that time. And now the intrusion is even greater.

And I would also point out that those were part of the fundamental grounds for the impeachment of Richard Nixon. They were preparing to throw him out of office, when he resigned. But at that time under the programs MINARETTE at NSA and COINTELPRO at FBI and CHAOS at CIA, Nixon was only spying on a few thousands of people. Now they are doing hundreds of millions in the US, there are almost 300 million US citizens, not counting the billion plus in the rest of the world. If you're just talking about the US, they're now doing virtually everybody. If you use a phone or a computer or any kind of bank card or if you're writing a check or do any kind of that thing, you're being spied on. So the intrusion is so much greater and so much more encompassing today.

But we are not even thinking about impeaching people. We should have impeached George W. Bush and Richard Cheney for doing this to begin with, but we didn't. And that's why they kept it all in secret, by the way – they knew that they were violating the US constitution and they knew they were also violating the laws. That's also why they had to give the telephone companies retroactive immunity, because they gave them access to the telephone lines and to the fiber optic lines that carried not only the telephone but also the internet. And they also gave them all the records of their customers, which all were violations of the laws and violations of constitutional rights of US citizens in the First, Fourth and Fifth Amendment, at a minimum.

LS: Bill, hearing that I have to ask: Are you disappointed from the reaction of your countrymen related to those NSA revelations?

WB: Yes, but I think that most of them still don't understand what that really means. I do have some hope here from some of the initial feedback to "CITIZENFOUR", the movie by Laura Poitras on Edward Snowden and some of the whistleblowing that we did. That's been very positive, and I think it's helping to educate the population here as to what that really means. I think once they really understand what's going on and what their government is doing to them, that they do will in fact react to that and react in a positive way and force the government to change, which they should.

LS: I would also like to discuss some questions related to PROMIS, a software for data mining, that was developed by Bill Hamilton's software firm INSLAW and stolen by the US Justice Department / US intelligence agencies. Dr. Norman Bailey was the Reagan National Security Council staff person in 1981 responsible for the new Signal Intelligence mission for NSA known as "Follow the Money." According to my information, Dr. Bailey told INSLAW that NSA briefed him on the fact that it had obtained the PROMIS software from the U.S. Department of Justice and used it as the principal software installed on computers of wire transfer clearing houses, commercial banks, investment banks, credit card companies, and international financial institutions for real-time surveillance of electronic fund transfers through the banking sector. Dr. Bailey also confirmed the use of PROMIS as "the principal software element" of "Follow the Money" later on publically in 2008. (3) Were you aware, while an employee at NSA, of the use of PROMIS by NSA for its "Follow the Money" bank surveillance mission?

WB: I was not personally aware of the program PROMIS or how NSA used it. I did know that there was an effort to look at money transfers, I mean, it was a matter of following that for terrorism, for dope smuggling, just international crime. But I wasn't aware of the PROMIS program.

LS: In retrospective, what would you like to say about PROMIS? I mean, the whole case still

isn't settled although it began in the 1980's and there's no doubt about it that the software was stolen by US intelligence agencies like CIA and NSA...

WB: I'm not surprised of that. I believe they tried to steal some of the intellectual capital we had after we had retired. The way they did it was to send the FBI at us to raid us ultimately. I had expected them to actively attack our computers and try to find the information there, we knew these people and so we never documented anything in a computer file anywhere, nothing was documented in the sense that it would be usable for them, either on paper or electronically – so we were walking around with all this knowledge in our heads and not putting it down so that anybody could have it.

There was a large intelligence company in the United States, they tried a kind of forced takeover of us, but what they didn't realized was that all the intellectual capital was in our brains and they could not take that over from us. There was nothing they could do to get the information from us. So they failed. And also the government failed when they were trying to get it from us.

PROMIS was a different story. They went into an agreement and my understanding is that they broke the agreement with Bill Hamilton. I think this is a court issue that should have been resolved in the courts a long time ago.

LS: So PROMIS has never been a topic among your colleagues at NSA?

WB: No, we never talked about it, and I've never heard about the program PROMIS at all while I was working at NSA.

LS: Is Wall Street a major player of the Deep State in the US?

WB: I certainly think it is politically anyway, because they do contribute a lot of money to the political campaigns. And of course they have their own lobbyists and all that. I can't imagine them not having some input in the process somewhere. It only seems reasonable.

LS: Well, the CIA for example was formed and launched by investment bankers and lawyers from Wall Street.

WB: Yes, and they of course got billions from us. And if you take the case of Elliot Spitzer for example, he was in New York and going after the bankers for all the defrauding of people. He was going after them in a criminal way, and of course they get rid of him. They had the FBI look through all the data, I allege, because I don't know where else they get it, the FBI had direct access through the PRISM program, they go into the name data bases at NSA, all the emails, phone calls and financial transactions in those data bases, and the FBI had access to that and could look at the data and find all the finance, phone calls and what have you for Elliot and find some evidence against him that they could use to leverage to get rid of him, which they did.

My question to begin with was what was their probable cause to do that in the beginning? I never really heard our government say anything about that, because they don't like the Fourth Amendment, because it constrains what they can and can't do. They want to have a free hand to get rid of anybody they want.

Like in my case, in the case of Kirk Wiebe, or also in Tom Drake's case, they tried to get rid of us by falsifying evidence and drawing up an indictment against us. Well, you know, that

was falsifying evidence to submit to a court to put people away for decades, that's what they were trying to do to us. I caught them at it, okay, so they finally dropped all that. But I mean, that's our Department of Justice; that's not justice, that's criminal. So, the people down there what they're doing, the House and Senate intelligence committees, the FISA court, the Department of Justice and the White House, they are trying to cover up any exposure of this, and that's why they were really after Snowden, and that's why they wanted to stop all those leaks, because it's exposing them for the crimes they were committing against the people of United States and against the people of the world.

LS: Two other questions: Who are the largest private contractors who manage IT and telecommunication systems for the NSA, and what is their access and potential use of the data to serve their private interests?

WB: Well, you see, that's what I was talking about earlier: those who are managing the data for NSA are contractors and those are contracting organizations or companies that have many interests, not just in intelligence. They do have access there, and that's a real danger of whether or not they would use that for industrial espionage to give them leverage and advantage in a competitive bidding for contracts internationally. That's always a threat. I don't know how they are monitoring that, and I don't know what they are doing to ensure that that doesn't happen.

Also, I would point out that these kinds of data acquisitions are not just limited to NSA and BND, there are other countries involved that have also sharing agreements and have the ability, like through XKeyscore, to see these data sets. That just opens up an immense array of potential abuses. I don't know if they have agreements to monitor or prevent it or to stop it if they find it. I don't know what they're doing. (laughs.) They haven't made it clear. I mean, they are doing all of this in secret anyway.

LS: And it's quite a problem given the fact that roughly 70 per cent of the US intelligence budget is outsourced to corporate contractors. (4) — One more question, and I know it's hard to answer, but I think it's crucial: Are NSA systems used to manage the financial markets, for example related to the NY Fed, the operative arm of the Federal Reserve System?

WB: I do not know that the Treasury or any part of the Federal Reserve System is using those programs. They probably get the benefit of it from indirectly, but I don't know they are using them directly. They are part of the government, too, you know, they share knowledge across the government, how much of that I'm not sure. But again, whatever agreements were made, would be made within the US government as to what kind of sharing would go on and the level to get access to it, that would be defined in those agreements.

LS: How would you think the indirect use of those systems looks like?

WB: Here is what I think they would do: I would think that they would have the Treasury and all the banks report transfers of money in and out of the country. Also, I would think they would take cooperatively under the business records transfer all kinds of financial transactions, including not just credit cards, but also bank transfers of money back and forth between banks around the world. Also, all personal check-writing and transfers of money from individuals inside the country as well as anywhere else they can get it. Those are the kinds of transfers they would be looking for. They are looking for patterns of money transferring that would be indicative of payoff for dope or payoff for money laundering

operations or things like that. I would think they are doing that.

LS: And as you know the Treasury Department has this Office of Terrorism and Financial Intelligence as a Counterterrorism Finance Unit. Do you think the NSA works with them?

WB: I assume they do. The level of cooperation would be laid out in agreements again.

LS: Thank you very much for taking your time for this interview, Bill!

Notes:

(1) See the press release by the DE-CIX Management GmbH Frankfurt (in German) here:

<http://presse.de-cix.net/press-releases/pressemitteilung/article/statement-zu-den-medienberichten-ueber-den-de-cix-vom-25-juni-2014/>

(2) See "Read Snowden's comments on 9/11 that NBC didn't broadcast", Russia Today, May 30, 2014, here: <http://rt.com/usa/162576-nbc-snowden-september-attack/>

(3) See Tim Shorrock: "Exposing Bush's historic abuse of power", Salon, July 23, 2008, here: http://www.salon.com/2008/07/23/new_churchcomm/. For more information on NSA's "Follow the Money" SIGINT mission and PROMIS see Lars Schall: "Follow the Money: The NSA's real-time electronic surveillance of bank transactions", LarsSchall.com, February 2, 2014, here:

<http://www.larsschall.com/2014/02/02/follow-the-money-the-nsas-real-time-electronic-surveillance-of-bank-transactions/>

(4) See Tim Shorrock: "Spies for Hire: The Secret World of Intelligence Outsourcing", Simon & Schuster, New York, 2008, p. 6.

The original source of this article is [Lars Schall.com](http://LarsSchall.com)

Copyright © [Lars Schall](http://LarsSchall.com), [Lars Schall.com](http://LarsSchall.com), 2014

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

[Become a Member of Global Research](#)

Articles by: [Lars Schall](#)

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

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

For media inquiries: publications@globalresearch.ca

