How The NSA Tracks You: Former NSA Technical Director

By William "Bill" Binney

Former NSA technical director on how NSA track you. From the SHA2017 conference in Netherlands.

Transcript

I am very honored and proud to present you Bill Binney on the stage and he will be telling us the perspective from the inside of the NSA because he was the Technical Director of the NSA for many years and worked in the intelligence services for more than thirty-seven years. He is a child of the Cold War and worked throughout the Cold War decrypting and breaking cyphers from the adversaries of the US and back then he used to call himself the "Technical Director of the World, in a sense." So please give it away for 'How the NSA tracks you' with Bill Binney…

[applause]

NSA Whistleblower William "Bill" Binney

Thank you, thank you. I'd like to say it's nice to be back with large numbers of people with character and integrity, which, when I worked at NSA, not too many people had. And I could get into some of that story…

I didn't work on the programs that Phil Zimmerman was talking about, the commercially available stuff, I was all looking at military and governmental encryptions and codes and activity but the same techniques apply to any crypt system. And I was on the offensive side not the defensive side. I knew Snow[den?] and the defensive people and I went to talk to them once to say "Here, I have all these solutions on the offensive side" and "can you tell me how you're designing the defensive side?" because I thought that they should be parallel. What we were doing, they were doing—and they wouldn't tell me. There's that kind of communications [problems] now, like, for example, for cyber security. All the [offensive] attacks that have come out of [WikiLeaks'] Vault 7 and the NSA exposures; hundreds of millions of lines of source code on attacks on firewalls, switches, servers, operating systems, all of that. There's thousands of attacks and we've only seen a few of them so far used in the world [i.e. WannaCry] and you can just be ready for a much rougher ride because the offensive side knew all these things were weak and existing; the defensive side didn't and never fixed anything so we were all vulnerable, so we all got attacked. Now everytime you get attacked, they say **"We need more money, more people, more empire." It's a swindle, we're all being swindled by our governments.** If they would only fix the things they knew that were wrong, we might have some security. But instead, they don't.

When I left NSA, I did that at the end of October 2001. Because they started spying on individuals and not groups of bad guys. So that meant they were

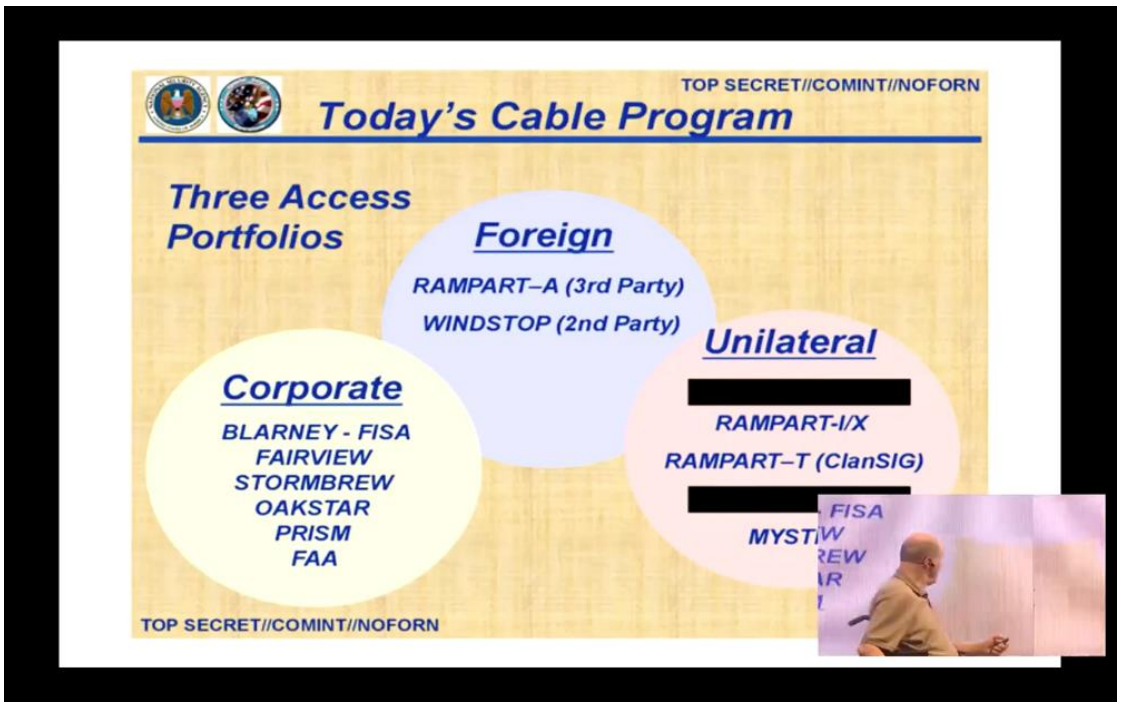
scooping up everything from everybody in the world and it's much more extensive than anybody thought, it's more extensive than even these slides show. And in order to store all this material they had to build the Bluffdale [Utah] 1.0 million square foot facility for storing data and last year they broke ground for a 2.8 million square foot facility on Ft. Meade [Maryland]—they took out a 36 hole golf course to do it. The point is: If you collect everything, an ever-increasing amount of data year after year, means you need ever-increasing data storage facilities to store it all. The way we found out about this was to look at the… Everytime the government wants to build something, they have to file an environmental study. So when they wanted to put in this very large building, they had to also submit an environmental impact statement and study to do it before they did it. So we're looking at those and seeing what they're building. So when they do that, we know this is on Ft. Meade and it's NSA doing it so… virtually everything on Ft. Meade is NSA anyway. That gave us the knowledge of the scale of what they're collecting and they're assembling. For example, Cisco, who sold them routers to route data to the Utah facility, estimated that by 2015 the amount of data going into the Utah facility would be 966 Exabytes a year, that's about a Zettabyte. That's why, originally, years ago, I estimated that the capacity was 5 Zettabytes. It's my guess, it's a lot of bytes anyway.

I felt I didn't have to take anything with me [Snowden-like] because everybody in Congress when I left [NSA], they all knew me: they knew what I was doing. Most of what they're doing to spy on everybody I designed anyway or had a hand in it. They knew all that so I felt I didn't have to bring any material out to validate anything I was saying because they all knew I did it. I naively thought that I could do that and go complain through the [proper] channels—the intelligence committees and the inspector generals—and they would all take some action on it. Well, what it really meant was when it came time to actually hearing what I had to say, Congress never invited me in. I testified in the [German] Bundestag; I testified in the House of Lords in the UK. **But the [US] Congress would never hear me because then they'd lose plausible deniability. That was really their key. They needed to have plausible deniability so they can continue this massive spying program because it gave them power over everybody in the world.** Even the members of Congress had power against others [in Congress]; they had power on judges on the Supreme Court, the federal judges, all of them. That's why they're so afraid. Everybody's afraid because all this data that's about them, the central agencies—the intelligence agencies—they have it. And that's why Senator Schumer warned President Trump earlier, a few months ago, that he shouldn't attack the intelligence community because they've got six ways to Sunday to come at you. That's because it's like J. Edgar Hoover on super steroids. They have the same kind of data that J. Edgar Hoover had—on *everybody*. So it's leverage against every member of parliament and every government in the world.

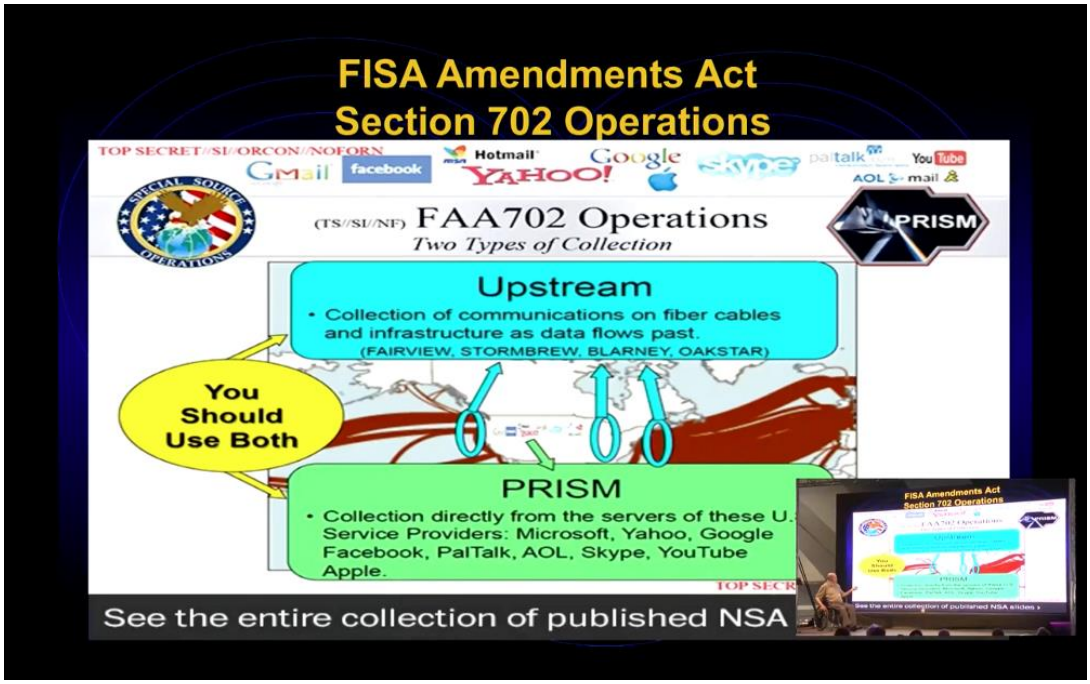
When Edward Snowden came out, he came out with material and slides and publications by the government about the programs they were running. And that was the stuff I left [NSA with] so it gave me all the opportunity to pull it together and say: this is what they're doing, this is how they're doing it, and this is what it means. That's what I've been trying to do.

So I've assembled some slides here to give you some idea, hopefully a *better idea* of what's going on. And I've also assembled some slides to show you what they *should* be doing. I have only one case of an unclassified version of big data analysis, which is what they should be doing and they aren't. That's why people are getting killed, that's why I said in the [House of Lords] that bulk data kills people. Because all the analysts in the UK in MI5 and GCHQ, similarly in the FBI and NSA, they're buried in data and they can't see what's happening because there is just too much data and they're using old techniques of word searches and stuff like that. That's not the way to do it at all. Social networking is the key to solving all of these problems, solving them quickly, and making all the data content problem a manageable thing.

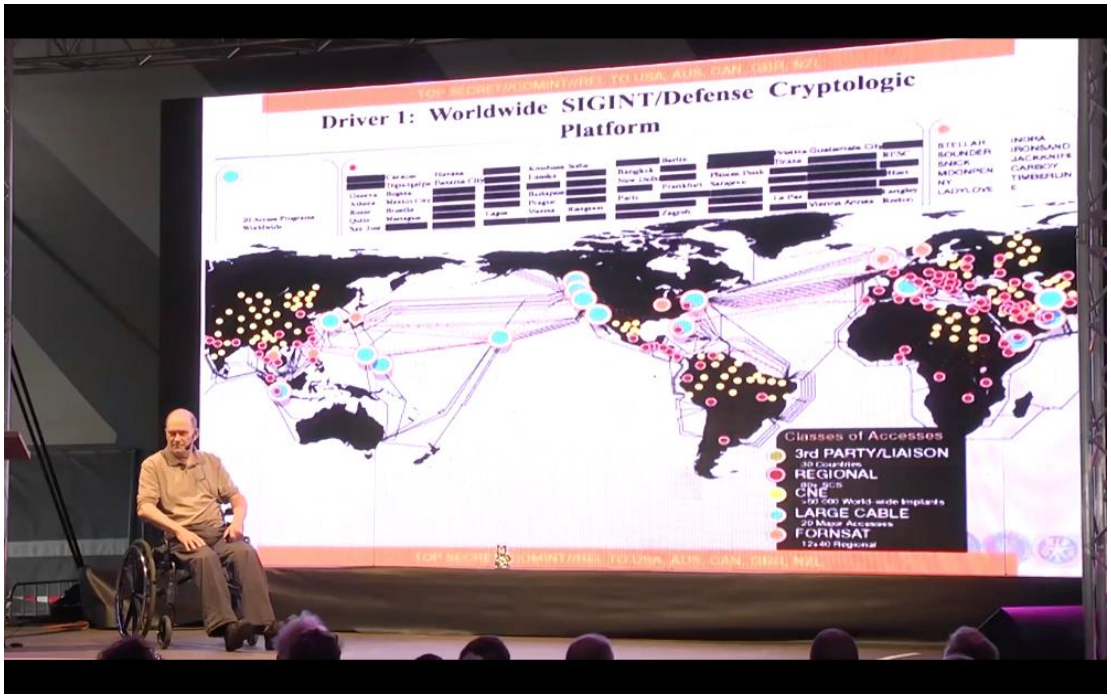
Now, I'll take you into that.



These are the ways that basically they collect data. First, they use the corporations that run the fiber-optic lines and they get them to allow [NSA] to put taps on them—and I'll show you some of the taps, where they are. And if that doesn't work, they use the foreign government to go at their own telecommunications companies to do the similar thing. And if that doesn't work, they'll tap the line anywhere they can get to it and [victims] won't even know it, nor their governments nor their communications companies will even know they're tapped. So that's how they get into it.



The PRISM program is really where they have the companies involved, that's down there and a list of them. This came out, it was one of the first things that was published out of the Snowden material, and it all focused on PRISM. Well PRISM is really the *minor* program. The major program is Upstream, that's where they have the fiber-optic taps on hundreds of places in the world. That's where they're collecting off the fiber line *all the data* and storing it. PRISM was simply their way of putting out something where Congress and the courts could look at it and say "Well, we're abiding by the law. See here, we asked these companies for this data and we have a warrant for that to do it. So you see, we're abiding by the law." When in Upstream, they were taking *everything* off the line. The MUSCULAR program was a parallel one which basically did the [mass collection] for Yahoo and Google and a couple others, [Obama's regime] unilaterally tapped the lines between their data centers—when they transfer data to back it up, and so on—they got everything they had and [Yahoo, Google, etc.] didn't know it. The MUSCULAR program from those companies, plus the Upstream is really the main one. And PRISM was only one small input to the data that NSA was collecting.

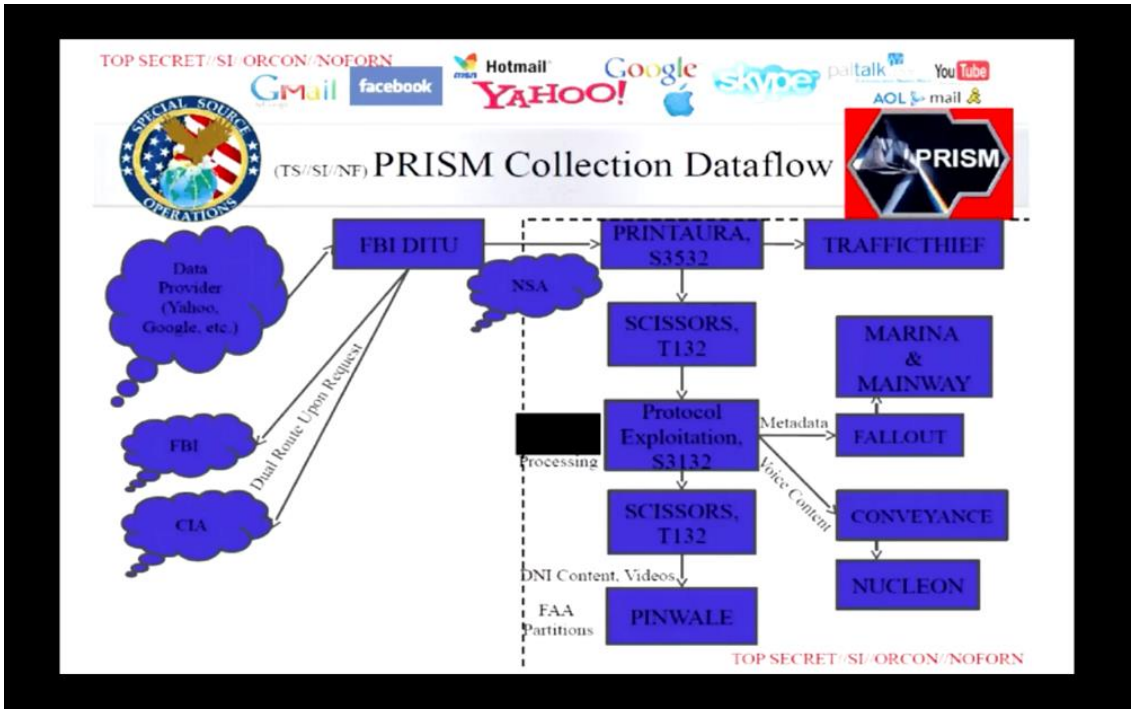


Worldwide, these are the kinds of things they have. It's all kinds of collection. The real big one is over there, it's CNE, Computer Network Exploitation. That's where they're implanting either with hardware or software or both into switches and servers around the world and [NSA] can make them do anything they want because they "own" them. So if you send data anywhere through those switches or servers—and there's tens of thousands of them in the world—[NSA] basically "own" the network. They have access to it and they get it.

So all of that is feeding another program that they call TREASUREMAP, and this one just says, well, we want to know where everything is in the world, every minute of every day. So it's not just collecting what you're saying—encrypted or

not—but it's also monitoring where you are when you do it. And that's basically done by… This is a kind of the geography of the world, then there is the physical layout of the fibers and the microwaves and the satellite towers and everything, and then that maps to a physical network, and then logical network is who's communicating across them, that maps to equipment which in turn maps to people and that's how [NSA] follow everybody [everywhere all the time].

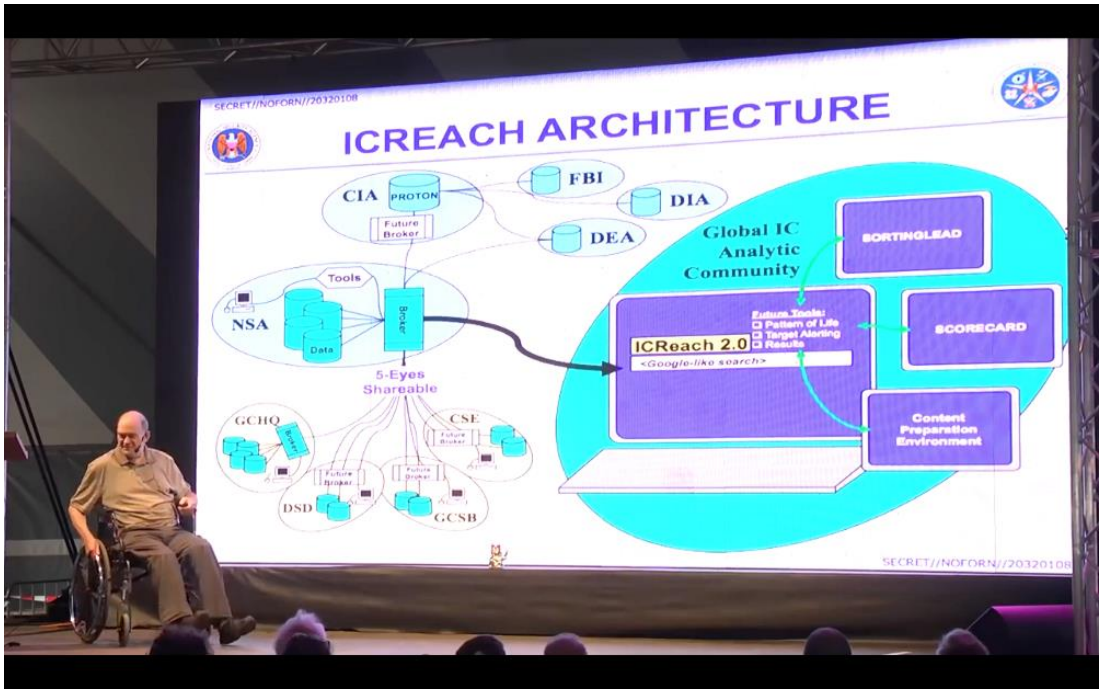
This is also when you have cellphones, for example, how they take the GPS and use the drones to target people. I think Jacob Applebaum was the one who said "NSA tracks them and CIA wacks them." And there's 1.2 million people on the drone list according to the last number I saw. I mean, that's crazy. *(Note: I'm unsure where this information was sourced from, I think he may have confused the Terror Watch List [which years ago was already over 1.1 million people](). And the No Fly List, per that Washington Post article, draws from that watch list. It is guaranteed that at least some designated terrorist targets of drone strikes would also be listed in that same watch list.)* They aren't verifying who they're hitting, they just go out and kill people all the time. This is insane. *(Note: That is true. For instance, [they're hitting cellphones through NSA's SIGINT](), killing tons of non-terrorists because they don't know who is using the devices targeted. And because it's with flying robots of death, they clearly don't care either.)* I call that [drone] program "Random Slaughter" because that's about what it is. This is why I get in their face every time I possibly can in the US because they're doing stupid stuff that's hurting a lot of people. But any rate, that's the TREASUREMAP.



All the material they collect from all the sources goes back into these programs back inside NSA—over here in that rectangle over there, basically a square fundamentally. These programs, MAINWAY and MARINA, are basically the graphs of social networks that map into the databases in PINWALE, the

Internet, and NUCLEON—the voice—that are basic to the two systems they're following: public switch telephone network, which is all the phones—fixed, mobile, satellite, any kind of phone; and all the content data then goes into NUCLEON and it's indexed up there by the MARINA program so that when they want to see who did what, they have an index all to everything [YOU!] ever said in their database. This was the whole design I left them and they haven't changed a damn thing in fifteen years, sixteen years. So that's real "progress" for ya.

But any rate, one of the things to look at over here in the side is that both CIA and the FBI, through the FBI center in Quantico, Virginia, have a direct access into these databases in the entire graph. Not only that but they also use that for police around the world. So it's a straight violation of everything, all this data's collected without warrants so it's a basic violation of the rights of every human in a court of law and that's what they're using it for. They're using it to arrest people and then they pull a *substitution* [they "reconstruct" information through "Parallel Construction"] and I've got some slides on that too.



And these are other people who have access to it. The Five Eyes group over here (US, Canada, UK, Australia, New Zealand), they have direct access into the NSA database here and so do the Drug Enforcement Administration (DEA), Defense Intelligence Agency (DIA), the FBI, CIA, all these people have direct access to all this data and it's children's data as well, it's *everybody* on the line because they take it all. So there's no distinction, they don't filter anything; it's just capture everything. This is what Gen. [Keith] Alexander said in Menwith Hill station a few years ago, he said: "All we have to do is collect it all" and that's what they're doing. The problem is, once you collect it all… And they have the impression, or they give the impression that "data is intelligence." When you collect more data, you have more intelligence. It's not. The point is, you have intelligence when you *understand* the meaning of what you've collected. If you

can't do that, you have nothing but a bunch of data. And that, unfortunately, that's the perspective they have. So they think collecting more is better.

Instead what happens is it buries their analysts and buries both the police and the intelligence people and they can't figure anything out so what the consequences [are], planned attacks happen because they don't see them coming and they can't prevent them. And so, that's why I said—when I went to the UK [House of Lords] to try to stir them up, I wanted to get them upset because they were getting ready to pass the Investigatory Powers [Act of 2016] bill, the bulk acquisition of data on everybody in the UK, as well as everybody they can possibly get in the world—I said: "Bulk data kills people." And the reason I said that is because of the inability to stop terrorist attacks, for example, we continue to see these [failure] things today. Nothing has changed, they're still going after more data, more people [hired], more of an empire, and they still can't figure out what they've got. But they're really good after the fact. After the fact, once they know who did it, they've got all the data on them and they can go directly at them.

The other thing it does give them, though is the power to manipulate anybody they want or do industrial espionage or if somebody is getting a political group together or getting politically active and they don't want them they have the ability to target them here using this data. It's just there, all they have to do is go at it.

So they can target people and use it against them but they can't look at all of it to figure out who out there is planning an attack on us or is going to smuggle weapons or smuggle dope or any of that. They can't do that because they've got too much data and they're using stupid searches, like word searches. If they use the word "bomb," if they're looking for somebody planting a bomb or building a bomb, if you say in an email to anybody "The quarterback threw a bomb at the last to win the game," your email is going to be picked up by that word search and it's absolutely irrelevant to anything they're looking for. That's the point. That's why social networking, of focusing in on those networks that are involved in terrorism or the ones you know of with the seeds you have, you can focus in on them.

And I would point out that all of the terrorist attacks that have ever happened, before or after 9/11, have been by people who were known by either the intelligence or the police or both. So why weren't they focusing on them? If they were, they have a chance to prevent the attack; instead, they're looking at this bulk [collection] stuff. It does spend a lot of money, it employs a lot of people, so it's what I call a "Happiness Management Program." But the point is, to keep it going [and billions flowing] sometimes [innocent] people have to die. And that's just un-American, first of all. No [regular] American would do that; no one would sacrifice the lives of anybody for this crap. But *they* [military-intelligence-industrial complex war profiteers] do and they do it because there is a big empire behind this. To collect all this data, the intelligence community—mostly NSA—has spent somewhere close to two hundred billion dollars since 9/11 just to get the data and they built an empire worldwide to do it and they've got all these countries that are participating in that.

I should point out, you see this date over here down at the bottom-right, 20320108. That's the eighth day of January, 2032. That means it's the first classification review for this slide [to see if it is safe to declassify]. Twenty-five years. So if you subtract twenty-five years from that it's the eighth of January, 2007, that was the date the slide was created. So this was the state of things in 2007. If you look at all these slides, many times you'll see a date there and you can figure out, well, this is the date of that program.

This is where they use the [data] for the SOD, it's the Special Operations Division of the Drug Enforcement Administration. The police, they have also the FBI, CIA, NSA, the DHS, the IRS, all have representatives on the SOD and they all look into the NSA data. IRS is supposed to be there for fraud and things like that but they used the data against the Tea Party, and the FBI used it against the Occupy [Wall Street] group, and other political parties were attacked similarly. And, of course, people looking to unmask information about individuals, that's done through these kind of organizations or they can request that directly to NSA.

The problem is the human failing here, people given the power over others eventually they [ab]use it. That's historically true, it's a weakness in humanity. That's the real problem here and there is no way of checking… there's no checks and balances involved in this at all. The Congress and the courts say they have oversight, that's a joke: they don't have any oversight. Even after the Snowden material came out, the head judge, Reggie Walton, on the FISA court, he came out and tried to make an excuse for his court and the judges on it that they really didn't have a lot of capability to verify anything that NSA, CIA, or FBI were telling them. In fact, he doesn't have *very little*; he has *none*. He's totally dependent on them telling the truth and they only tell him what they want to tell him. Same is true with intelligence committees in Congress, and the same is true in every country of the world. No government of any country in the world has any control of their intelligence agencies, they do not know what they're

doing. And they have no control, really, of any of them. They can't stop it. They would say they go to oversight but when they go in all they're told is what the agency wants them to hear, so they get the story *du jour*, the story of the day from that agency. That's the problem I see.

So in order to do this, they don't tell any of the attorneys, the judges or anything, you never sign anything, never put it in affidavits, there is no documentation that they used NSA data or NSA-collected data from all their collaborators to do any of this. And so, what that means is they have to do a "Parallel Construction": they reconstruct data or go out and get data that they could substitute in a court of law for the NSA data because then they could use that as a justification for the warrant—which they didn't get in the first place. So that basically means that they're perjuring themselves in a court of law. This is not just for us in the United States, anybody who has any relationship with the FBI or the DEA worldwide, they're all getting insight through these programs. And so, whatever actions they take are based on the unconstitutional collection of data by the NSA and the CIA. But they're still using it. In fact, one of the federal agents using this data commented to a Reuters reporter—this is a Reuters slide. He said, you know, this is such a great program, I just hope we can keep it secret. Well, what does that mean? It means we have a secret government. When you marry the intelligence agencies with the police, you have a secret police. In Germany, they called that the Gestapo, or the Stasi. So I refer to NSA as the "New Stasi Agency."

Unfortunately, we haven't been able to do anything [to stop them]. I am attempting to do everything I possibly can against these people. **I'm supporting four separate lawsuits against President Trump—previously against President Obama—and the intelligence agencies of the United States for unconstitutional collection of data.** We have to do it for our laws—our constitutional governance, violation of privacy rights of US citizens. So we're attacking them that way in a court of law and I just got my first chance with the Third Circuit Court of Appeals to submit some of this NSA data about their own programs into the court of law, now it's going to be tough for NSA to deny it because it's in the federal courts. This is the court that's one level down from the Supreme Court in the United States, and it's at four separate circuit courts—one in the Second, one in the Third, one in the Ninth, one in the Eleventh. So I'm coming at them from as many directions as I possibly can and, hopefully, one of them will get through to the Supreme Court and when it does, we'll get to them. And if we fix it, why, hopefully that'll spread around the world to the rest of the countries who've adopted this from [us] because *we* started it: we Americans were the first one in the bulk collection pit, the rest of you came along a little later. That's only because we were close in and it was convenient, so we got it first.

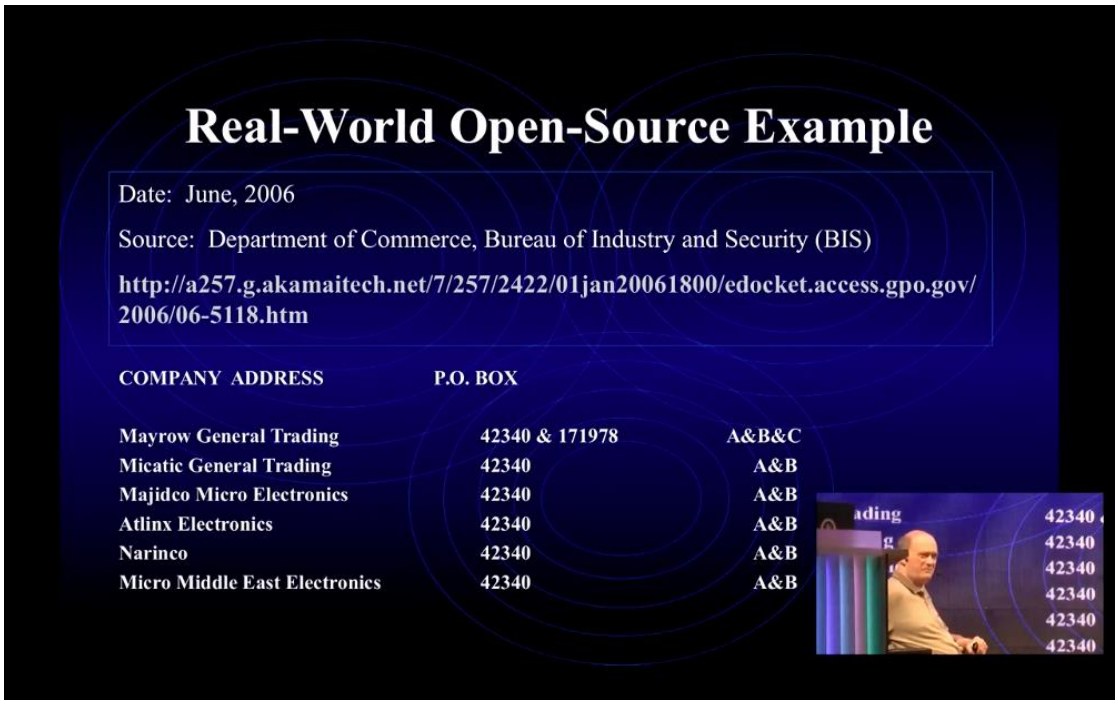
The point is, they're all doing the wrong thing. For two basic reasons. Number one, it buries their analysts with too much data, they're totally dysfunctional so they can't figure out anything and they're just "losing it." And, by the way, I provided from Edward Snowden's material copies of memos written by internal analysts in NSA and MI5 and these other places, saying that they are buried in data—they just can't figure out

anything, they've got too much data. I gave that to the House of Lords as documention of what I was saying was true and they simply ignored it. But the main problem I had from the very beginning was it was a total invasion of the privacy rights of everybody on the planet, starting with us in the US. It took me one week to get out of NSA when I found that out.

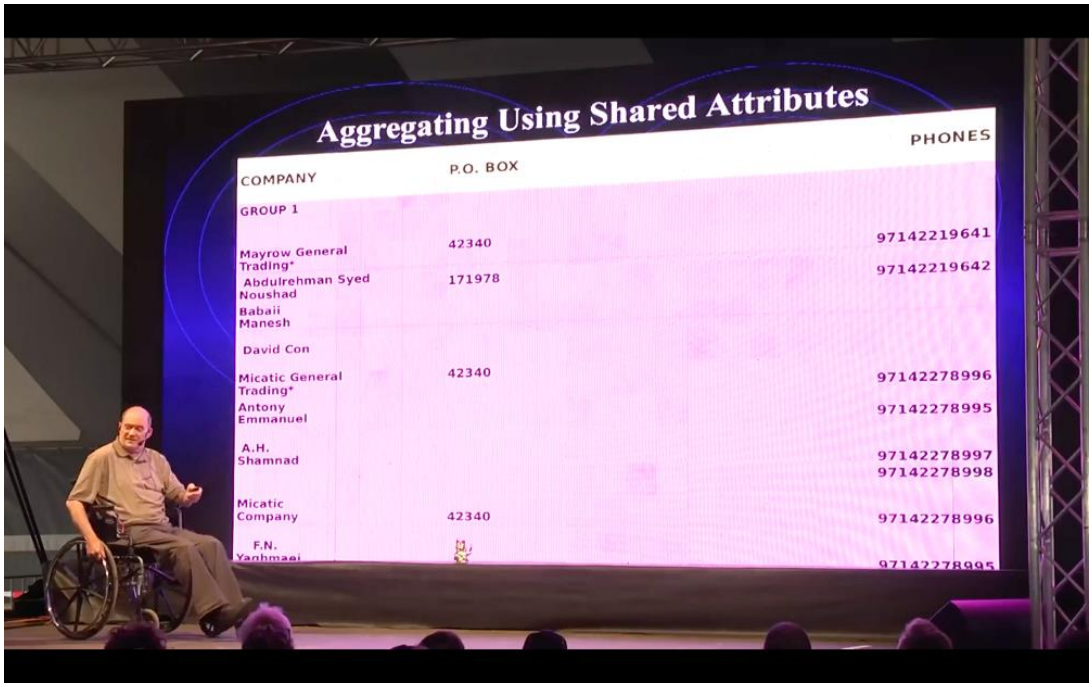
They were using the programs that were developed in the Signals Intelligence Automation Research Center, which I was founder of and the people I had building those things were the people they had to depend on to implement them worldwide on a scale that is still growing, there was no limitation to the scale. We did B+Tree file indexing schemes, which meant, if you needed more space you simply added another server, spread out the graph. So we saw no limit to anything we could do. We'd already taken in trillions of transactions and that wasn't a [system] problem at all. Once I found out that they started taking in everything that the telecommunications companies were having in terms of US communications, principally starting with the public switch telephone network and then starting very shortly after that the Internet and basically the worldwide web, I found that out in the second week of October 2001 and it took me a week and a half to get out of the place. So I got out Halloween Day, 31st of October 2001.

And since then I've been trying to advocate internally in the intelligence committees and inspector generals of both the Department of Justice and Department of Defense to have them… I mean, obviously this is totally unconstitutional violation of the Pen Register [Act] law, Electronic [Communication] Privacy Act, Electronic Security Act, any of the laws in place to cover FCC regulations governing any of the telecoms—that's why the telecommunications companies had to get *retroactive immunity* in 2008 because they had so many laws that they were violating everyday and they're still doing that. So the point was that [they] were all in it together and each one of the committees and the courts had to protect one another, it was a coverup because they were all involved in this. And the White House was the starter, it was actually started by Darth Cheney—I call him Darth Cheney because he went to the Dark Side. That's what he said anyway.

In the meantime, we had been advocating for a targeted approach where you went after groups of people that were doing bad things and you can easily define that by social networks in the world, either in the public switch telephone network or even in the Internet. We had no difficulty doing that at line speeds—fiber-optic rates. We were able to sessionize fiber-optic rates at stem-level transmissions in 1998. So from there on, we were able to do deep packet inspection on all that stuff and reconstruct everything on the lines. And so, we were able to see networks and we built all these social networks—transmitting the routing data, the IP's and the addressing schemes of the Internet as well as the phone networks—and we had no difficulty doing a targeted approach then of using that data to filter out what was relevant to targets we were interested in—or should be interested in—out of the flow of information around the world at whatever rate they were doing it. We simply subdivided and conquered it by divide and conquer approach. That was our way of doing it.



And our targeting approach we even took to [US] Customs and Border Protection (CBP) after we left NSA. And one of the ways we did that… this is the only unclassified version I can take of big data, it's the only thing I have. So we went down there and we had a Bureau of Industrial Security of the Department of Commerce publish this alert because some military in Iraq overran a bomb making factory and they found some parts in there and they traced the part numbers back to companies in the US selling them to Iranian companies in Dubai. The reason they're located in Dubai is it's outside of Iran, it's outside of the exclusion for trade so operating out of Dubai they can order these parts. So the Bureau of Industrial Security (BIS) had to alert everybody in the world that this was going on.



So we took that and used Google and went on the web—this was some more of the data they had, but we used it and Googled all the things and started looking at the data. What we did, we went out and added all kinds of information to that. We added fax numbers, phone numbers, addresses, more data on people involved, and more company names involved. And then in the end of it, just after the BIS report came out, they [Iranians] took all the names of the companies they had off the web and then kept that data out of the way becaue they thought BIS and CBP were still looking for the old data—they didn't have that confirmed, so they removed it and they changed the names. In the process of changing it, they used one of the new phone numbers with some of the old data. So that gave us the "in" and we then traced all to the new data and as they went we followed them and we didn't lose a thing. Of course, the CBP and the Pentagon and various other people in the intelligence community, they did lose it. But we used Google and followed them.

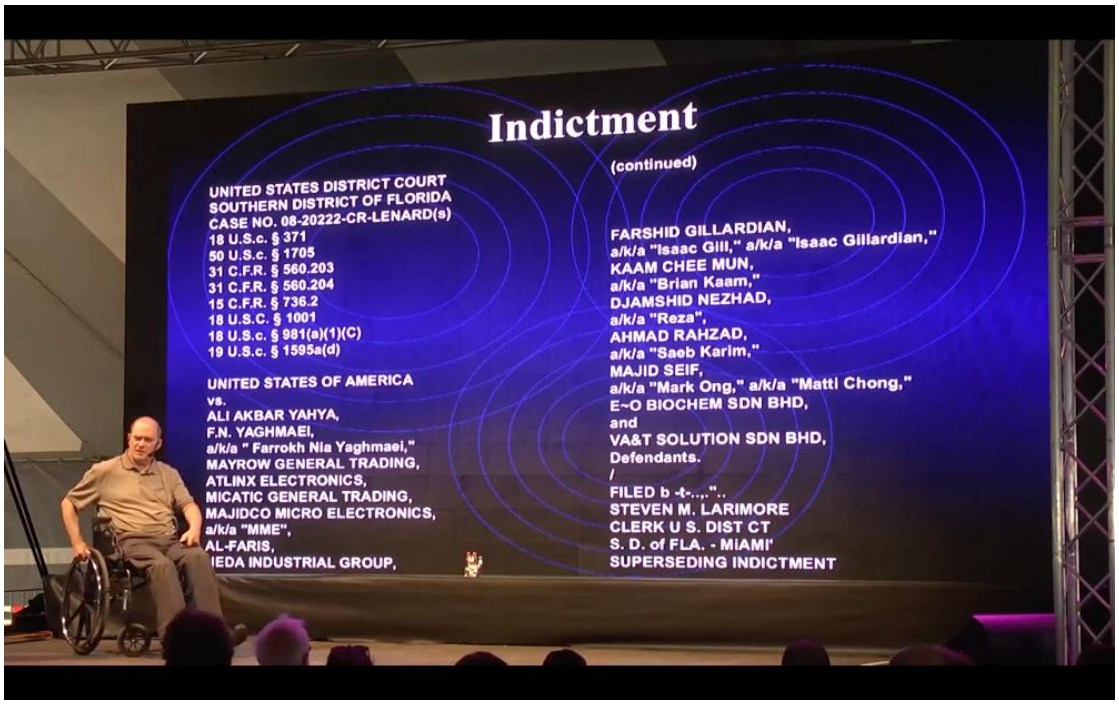
So we provided all that data to them and, since we didn't trust the U.S. government to do the right thing, we also gave it to our counterparts in Canada because they were losing people to IED attacks too. We didn't trust our government to the right thing, so we passed it up there too. [Canadians], of course, did the right thing. [Americans] didn't, of course. The whole idea was, we compiled all this list of information that we got from them—from those approaches—and gave it to Col. Woody at the Pentagon, he was [leading] the group that was looking at the prevention of IED attacks, and so on. So we passed all this data down to try to cut the supply of parts going into it.

The reason [Iranians] used multiple company names to do the construction of the IEDs is because each company would order a different part and the idea was that if CBP looked at a given company—which is the way they do it—they would only see one part of an IED and never deduce that [they] were putting together an IED. So unless you collapse them down by a common attribute, like they're all sharing the same phone number or the same address or something like that to put these multiple companies into one place where you see the whole activity, then you sum it all together by their names and you see the IEDs. So you can see what they're doing when you do that.

And so, we proposed to CBP that we do this for them. They had a small data set of about half a billion records over ten years, of imports and exports—one import could be a thousand cars on a ship, so it was like half a billion records and they said it was a real mess because the data was "dirty" and all that. We looked at it and thought it was a goldmine: there's all kinds of information here, phone numbers on addresses, and so on. We could lay out all the entire world's phone numbering schemes and how they change—as they change since they put these things out there. So we proposed to them that we scrape the entire world's websites and pull together consolidated lists of however many million companies there were in the world—one to two hundred million, something like that—and be able to do a collapse on this and study all those and find those who were showing attributes of doing something "illegal." Which is what this [Iranian] multi-addressing scheme implies. So that would define a set of suspicion, zones of suspicion for companies involved in the world's trade. And we estimated that—from our study—we scraped the entire website. Pars Guide

was the website in Dubai, listing all the Iranian companies in Dubai: there were 5,032 of them. And when we did that we found 222 different company names that subgrouped into 55 different groups that were doing different nefarious things for the Iranian government. Smuggling dope, weapons, that kind of thing, buying equipment for IEDs and looking around for things that would help them with triggers and nuclear stuff.

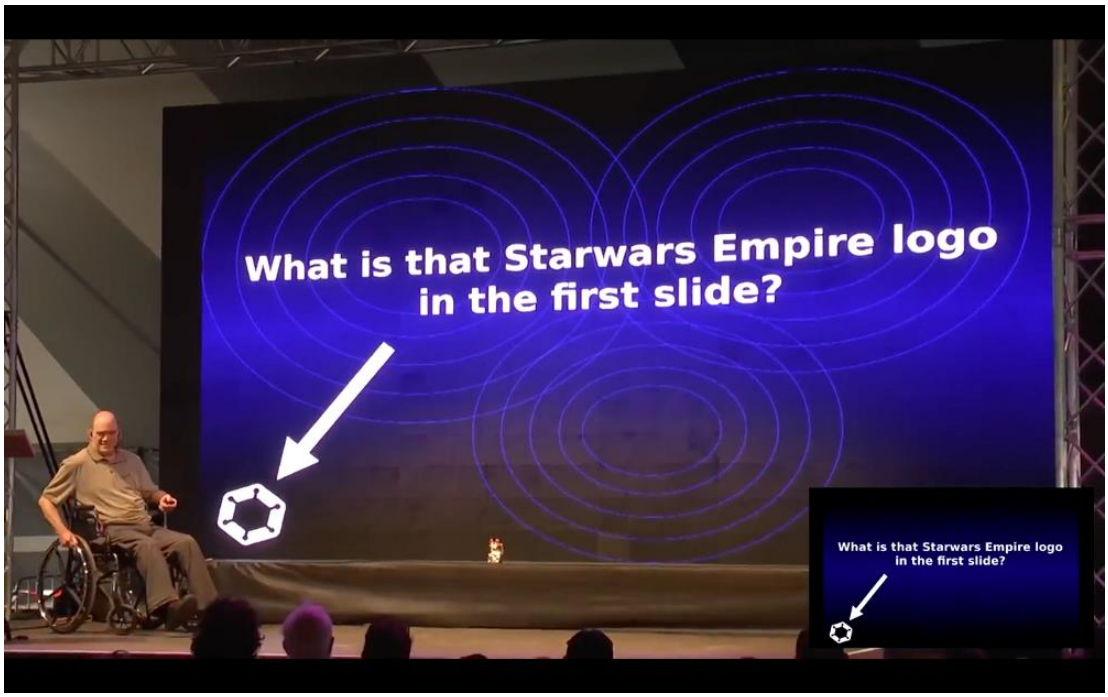
So we passed all that along, too. And, of course, our government is just too [stupid] to really do anything. Once we did that, we said we'd estimated that the entire world would produce perhaps forty thousand targets for you to do targeted selection of searching of incoming crates and don't do exports to these companies. So we thought we could do that in the first-run of our data and it would take us six months to correct all the data and make that happen. With Kirk Weibe and myself, and two programmers. But that [solution] was too cheap, they wanted to elect a $1.2 billion contract to IBM to do it. So they fired us and brought in IBM. And they *still* haven't done this, by the way.



The ultimate thing that came out [of this] was they indicted everybody that was involved in all the [IEDs], they arrested a few of them in Florida but some of them were back in Iran so they couldn't get to them. But they left the indictment out there. It took them two years to do the indictment from the time that we found all the data, that's a really "fast" judicial subprocess. But this is something that they could do worldwide on every possible criminal activity in the world by looking at social networks, looking at targeting approach, which would give everybody [innocent] privacy. If you use that as a filter right up front, nobody's data gets taken in unless they are a part of criminal activity or falling into a zone of suspicion around that activity. So it would give everybody in the world privacy. But that's not what they wanted, they didn't want privacy [protected]. They first removed our filter up front so they could take in everything; then they took away all the encryption we used to give privacy to people once we took the

data in—until we had a warrant—and they removed that; and then they removed the auditing routine in the back that looked at everybody that came in and what they did, when they came there, where they went, what data they looked at, what they did with the data, and they removed that because they didn't want anybody to know what they were going to do, they didn't even want internally anybody to know.

So it's not just that they're keeping secrets from us, they're keeping secrets from Congress and everybody else, even people inside their agency. Because the vast majority don't know, I think there's only about 3,000 people now inside NSA that really are involved in one way or another or know direct evidence about this program. That's the sick part of it, this is like a secret democracy that's not a real democracy. Johann Wolfgang von Goethe said it pretty well, he said: "No one is more hopelessly enslaved than those who falsely believe they're free." And that's us [America].



What's the [logo] doing here? Well, we have more details about our start-up soon. Kirk [Weibe] and I are in Europe because we can't get anything done in the US. So we're going to advise anybody, any organization or government, on ways you can do privacy and security by design. And we're going to help get one of those capabilities up and running here in Europe somewhere because obviously the US and UK are too [stupid] to realize it can be done. Actually, it's their agenda is the one that's driving them and that's one that means money, power, and control. And the way you get that is to take in data on everybody on the planet and that gives you that power. Then you can swindle money because you can let [terror] things happen because of the way you're doing business… things happen and that's more justification to get more money. It's like a swindle. I call the terrorism thing—trading privacy for security—a lie from the beginning and that's just the way they swindled everybody. Because the way they took in all the data, that meant they couldn't stop anything and then more

people get killed. They'd say they need more money, more people, more bureaucracy to stop it, they'd get that and more people get killed by another attack because they've got too much data and they'd keep dumping more and more on people. They're perpetuating the same problem; they're not facing the real issues. They don't understand what the problem really is and [innocent] people are dying as a result. So, we're over here to try to do something about that and, hopefully, we will get there.

Thank you.

Q&A

Bill Binney: "I guess now we can take some questions, anybody have any questions you want to ask?"

The introducer: "Yes, if you have any questions line up at the two microphones we have at the center there. Yes, please just go ahead…"

Audience member 1: "Hey, thank you so much."

Bill Binney: "You're welcome."

Audience member 1: "One question comes to mind Being the Technical Director that you were, how did you end up noticing this rather than approving that or knowing of [unintellible] from the very beginning?"

Bill Binney: "As the Technical Director, I was looking at what is the biggest problem that analysts in the NSA had to solving problems and predicting intentions and capabilities of people who are going to hurt people, or criminal activity, and it turned out to be the digital explosion of communications—cellphones, Internet, and so on. And so, I had to design a way of getting into it. But it was pretty clear that in order to do that, we would be violating everybody's privacy unless we did something to eliminate that. So that's why I built in the social targeting and pulling out only that information and letting everything else go by. And that design is one of the things [NSA] didn't want, they wanted to take in everything—so they wanted to get rid of that filter. But, you see, in order for NSA to put that into place and get it running, they had to use the same contractors that I did to have my program built because they're the only ones who knew how to put it together and get it up and running, no one else in NSA did. And there were no other programs that could handle the massive amounts of data, so they had to use my program. It's when they did that, some of them came to me and said "you know what they're doing?" and said "they're taking in all this data on US citizens" down the hall from us and building these graphs and everything, and violating the privacy of everybody in the United States. Then, of course, after that spread to everybody else in the world. But that's how I found out about it and, once I did, that was the first sign to me I had to get out of here. I knew no one would do that in NSA without approval from above, and that came directly out of Darth Cheney's office."

Audience member 2: “Question: The filtering and targeting of social networks needs a lot of data and then you can extract patterns and then you can throw away the data because you don’t need it anymore. Is that right?”

Bill Binney: “There’s a couple ways to do it. One is you have a “seed.” That is, you know a bad guy. You could look at his social network and build from that and then you could say one degree [of separation] beyond that is as far as I’ll go to pull data in. It really ends up two degrees from the bad guy but you only pull data in from one degree from him. And so that means that you’re focused—all the rest of the world’s data goes right by—and that’s what you pull. And the metadata is the way you pull it out because that gives you the ability to… You’re looking at the data that’s required for the network to route data and, if you do that, then it’s easy to pull all that data out and that’s all you really get and it gives people privacy. You get a rich environment for your analysts to succeed and that’s what they don’t understand.”

Audience member 2: “I’m still curious. How can you get patterns from things you’ve never seen before? Unexpected stuff.”

Bill Binney: “We used actually two approaches out of three, but it was deductive, inductive, and abductive approach. The deductive approach simply said—it’s dealing with the graph: if you’re in the graph and you’re close to within proximity of two hops of a known terrorist then you’re going to be in a zone of suspicion. You’re going to be looked at, it doesn’t mean you’re guilty it just means you’re going to be looked at. And then a decision will be made, yes or no, if yes, then what’s the reason and if you get included then the entire graph will shift if you become a target at that point. And that was done by software. The other was the inductive approach, that was the main one: That if you are looking at sites advocating pedophilia or sites advocating jihad or terrorist activities or violence against the west and you keep repeatedly looking at them or look at multiple site advocating that, then that gives you the idea that you fall into the zone of suspicion and that means you get looked at. So at that point you get data coming in. But you can do it having all their attributes encrypted until you can prove that they are, in fact, a part of the illegal activity.”

Audience member 2: “Last question: Isn’t it handy that they do have a lot of data about the people who are now in the [Trump] White House?”

Bill Binney: “Yeah, they do. They have everything they do, including the codes to decrypt their communications.”

The introducer: “Thanks a lot for these questions. Please, next question.”

Audience member 3: “Hello. You mentioned the immense capacity to store all this data from everyone and, I was wondering: What companies [are involved] and did they cooperate willingly to create such a capacity to store all the data? And, in particular, IBM? And so, can we still trust our servers?”

Bill Binney: “No! That’s the answer. Everyone of them. And no. Because in the United States—if you’re a company in the United States—they can force you by

law to give them the data. It's only now coming out, they call it the Business Records Requisition. The first thing from Edward Snowden was the general warrant issued by the FISA court to the Verizon company to turn over all the information about their customers, over 110 million US citizens. And that was a violation of the Constitution, a direct violation. That's why the [FISA] judge, Reggie Walton, came out and tried to defend the court because of that. But they have the power to do that with all of the companies and, I would point out, that was B.R. 13–80, which meant it's the 80th order of 2013 to companies to give business records, which is the second quarter and it's issued every ninety-days. So every quarter an order comes out to each individual company. And, the way I reckoned, in the public switch telephone network the first two companies in line in the network providing data were AT&T and Verizon. AT&T would get order 1 in quarter one, Verizon gets order 2 in quarter one and then it gets order 80 in quarter two. That means there's 78 companies participating (in reality being forced into participating or be punished, possibly through being fined into bankruptcy). So that's 78 companies participating: banks, telecommunications companies, ISPs on the Internet, and so on."

Audience member 3: [garbled]

Bill Binney: "Could you repeat that, please?"

Audience member 3: "So did [these companies] get anything in exchange for all the information they passed on to NSA?"

Bill Binney: "Yeah, money. They get paid for it. There's a whole schedule on the rate of how much they get paid… It's true."

The introducer: "Thanks a lot. Next question, please."

Audience member 4: "Hello. Thank you for being here and everything you've done for, basically, all of us. My question is… When you see these testimonies from, for example, James Clapper, [Gen.] Keith Alexander, when they're being asked directly 'are you monitoring,' you can kind of see in their eyes and when you read other press that monitoring means a completely different thing for people within the NSA. So, my question is: How do we make questions more relevant to level the playing field to make sure that we're all talking about the same thing?"

Bill Binney: "Well, it's hard, especially when they lie to you. I mean, 'not wittingly.' *[physically mocking James Clapper's lying under oath]*

Audience member 4: "But how do we make the questions sharper? When we say 'monitoring'?"

Bill Binney: "Here's how. Senator Wyden phrased the question properly—I think is what you're getting at. He asked Gen. Alexander how many US citizens does he have in his databases? That's the right question. If you talk about 'collection,' well, Alexander, he uses a word game: collection means somebody looking at it at NSA. So it's not collected till somebody looks at it. Well, that's

horseshit. If I collect all your data, I've got it in my database. So he asked the right question: How many do you have in your databases? He said he couldn't answer him [then] so he came back in writing, this is on the web if you want to go look at it, it's really a joke. He said 'We can not tell you that because it would be a violation of the privacy rights of US citizens.'"

[audience laughter]

Bill Binney: "It's on the web, if you Google 'NSA answer to Wyden's question,' you should get it. You'll probably get multiple ones but it should be in there." *(Note: I did a cursory search for it but was unable to find it. I did find this written response from Gen. Alexander but it doesn't have said information quoted above. If I find that ata later date, I'll update this with it.)*

Audience member 5: "Hi. As an American, I'd like to say thank you for your service. And I also wanted to ask, as a citizen, if there is anything we can do to make it easier for agents to blow the whistle or to encourage them to become whistleblowers?"

Bill Binney: "I always advocate 'the squeaky wheel gets the oil.' So complain, bitch, moan, gripe, groan. If your congressman or senator comes out for a town[hall] meeting, confront them with it: 'Why are you backing this? This is obviously unconstitutional. You're violating your oath of office to protect and defend the constitution. And what are you going to do about it or should I work for somebody else? And if you aren't going to stop this, I'm going to work against you, give my money to somebody else, and vote to fire you!' And otherwise, sue the bastard [Obama, Trump, and others]. That's what I'm doing."

The introducer: "So, we do have some more time for questions. So, please, go ahead."

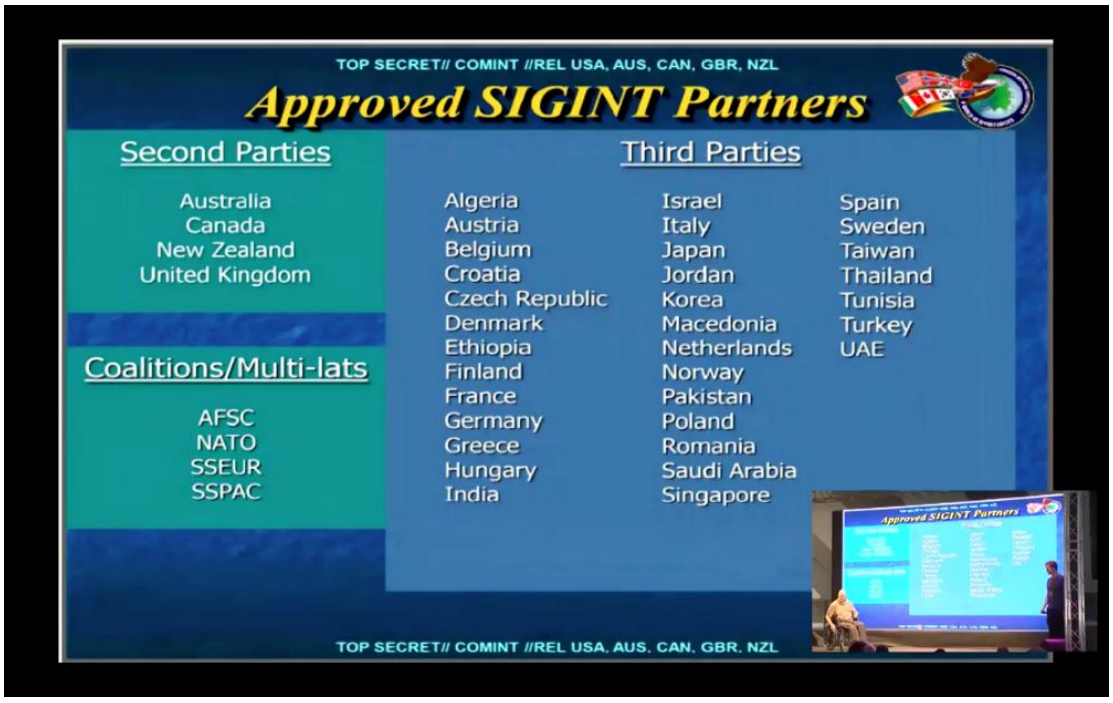
Audience member 6: "I was wondering. In NSA there have been several leaks to the public, which have helped us a great deal know more about the inner workings. Do you see a cultural change within the NSA that there may be more people who stand up and choose different paths, choose to reform the NSA from the inside?"

Bill Binney: "Yeah, I think that's probably happening, especially with the younger generation going into NSA [i.e. Reality Leigh Winner]. The older generation… We did a Myers-Briggs study of personal traits of people working at NSA in 1992 or something like that and it turned out that eighty-five percent of them were ISTJ's, so they're all introverts. You know, these are the people who like to work in their desks. Mathematicians are that way, they're very quiet people: give me a pencil, I'll figure it out. Go in a corner and [handing it back] here is the answer. That's all they do. But they're very easy to threaten, those are the kind of people you can easily threaten. And so, that's really what has been going on inside NSA. They have a program now called 'see something, say something' about your fellow workers. That's what the Stasi did. That's why I call [NSA] the new New Stasi Agency. They're picking up all the techniques from the Stasi and the KGB and the Gestapo and the SS. They just aren't

getting violent yet that we know of—internally in the US, outside is another story."

Audience member 6: "Hello. Now we know something about the US programs but do we know something about the other nations, like Russia? We know that China has some internal spying program but do they have capabilities of external spying?"

Bill Binney: "Yes. I had a slide there that I think they deleted, listing all of the countries cooperating with NSA. Let's see if I can get back to it… there they are. These are the countries participating with NSA. Of course, the rest of the Five Eyes up there, and everybody else is classified as Third Parties except for Fourth Parties which we don't talk about because we don't want anybody to know we have relations with them. So, you know, they're off the board but these are the countries and each country has a different relationship with NSA. I think eight or nine of these countries in the Third Parties category are cooperating in the bulk acquisition of data on the Internet with NSA and GQHQ and the rest of the Five Eyes. Is that the answer to your question?"



Audience member 6: "Yes, but the big one missing is Russia. So we should suppose that Russia has some similar secret programs we don't know about?"

Bill Binney: "Which one are you talking about?"

Audience member 6: "Russia."

Bill Binney: "Well, Russia does the same thing in reverse: they're looking at us the same way. Everybody's doing this to the ability and the capabilities that they have."

Audience member 6: “Thank you.”

Bill Binney: “This is standard spying. That’s why diplomacy was created—so we could spy on people.”

Audience member 6: “Thanks.”

The introducer: “So it looks like no more ques… oh, yes, there is one more question. Great, go ahead.”

Audience member 7: “Would you say that the way they are doing the wrong thing is incapability or not willing to do the right?”

Bill Binney: “You mean the other countries?”

Audience member 7: “No. The NSA, the US organizations. Are they not capable of doing the right thing or are they purposely not doing the right thing?”

Bill Binney: “Yeah, they *are* capable. You see some of these whistleblowers still coming out so there are people who understand that [they] are doing the wrong thing and they could create a way to do it like I did internally. The trouble is we have people managing these agencies who are fundamentally corrupt. Because there is so much money involved in this… money corrupts. [The] budget for NSA’s like $16 billion a year, and for the entire intelligence community it’s been close to a trillion dollars since 9/11. So that’s a lot of money and there is a whole intelligence empire that’s built up over the years in the United States and also in the UK—it’s spreading. Some of the testimony from BND [German intelligence agency Bundesnachrichtendienst] and what they’re doing with NSA. The Bundestag [German parliament] has found out recently many of the things [BND’s] doing. They’re all doing the wrong thing in terms of looking to stop things really; they’re not taking a targeted approach that’s a professional, disciplined look at your job and the targets you’re *supposed* to be looking at and watching instead of looking at everybody, spreading your effort across the entire planet. So they have to learn how to do the right thing, too.”

The introducer: “So, we have time left for about two short questions or one long question.”

Audience member 8: “One question, I don’t know if the answer is long. You just said that they are able to look at the right target but they collect information on everything, everywhere, anytime. It’s like they’re little kids—they’re distracted. I’m curious. All that information that is not related to the current target is related to a lot of other targets and power is to control what’s outside of your personal space. So the question is very big, I’ll try to ask about a specific point of view and maybe you can elaborate on that: How is it possible that we still have organized crime on a global scale—some of this outside the power of the United States or the direct influence—at least, I would imagine, organized crime from foreign countries should be the subject of this kind of information? Is it used and we don’t know? Or is it not used and why? Thank you.”

Bill Binney: "I would say they *attempt* to use it but if you look at… If you Google XKeyscore, which is the query routine going into the databases for most of the people, or ICREACH, I don't know if most of that's out there yet. But if you looked at that and you could see the way they ask the queries, about putting in words and phrases just like you do in a Google search. So in a Google search you get tons of material back so that [XKeyscore] approach gives you tons of material, which means you've got to go through all the items to try to find it and where is it in this list of, say you get 100,000 items back, where is it, is it 90,000, 80,000, can you get there? No, the answer is no. That's why they were failing."

Audience member 8: "So you're saying they're failing because they're not able to interpret the data?"

Bill Binney: "That's exactly right, they can't figure out what they've got. Because they're taking the wrong approach."

Audience member 9: "So, I was wondering. Someone like you, or for example…"

The introducer: "Get closer to the mic, please."

Audience member 9: "Someone like you, or for example, Thomas Drake—who was a previous version of this event, who came from the inside of the NSA and now is standing here. You told us about the NSA having a lot of data to use as leverage against people, how come you are able to be here… why aren't you dead or at least in jail for something wrong said or," *[audience laughter]* "if they've got so much power over everyone?"

Bill Binney: "Well, as I said in the movie about me, A Good American, I said: 'If they ever do anything like that, everyone will know who did it and why.' So, they don't want to expose themselves to that kind of political and reaction by the public in the United States and now I'm basically well known around the world so I don't think they… I want to get them in court any way I can, if they want to do [that], that's one of the ways [how], at least, if they don't 'terminate' me, I'll be able to do that."

Audience member 9: "So basically: By making it obvious they're your enemy, you're safe."

Bill Binney: "Yes, public exposure to a degree is security."

Audience member 9: "Okay. Thanks."

The introducer: "Thanks for this last question. Please give a warm round of applause."

Bill Binney: "Thank you. Thanks. Thank you."