Retired NSA Technical Director Explains Snowden Docs

Posted on September 30, 2014 at 6:49 am

I had an opportunity to attend a presentation by a retired technical director at the NSA, William Binney, which provided context for some of the published documents released by former NSA contractor, Edward Snowden.

Because of the public value of Binney's expertise on the subject, I decided to publish his presentation and comments on my website.

Binney also mentions how the current NSA mass surveillance regime differs from aspects of an earlier less expensive program, called THINTHREAD, which both he and the former NSA senior computer scientist, Edward Loomis, invented.

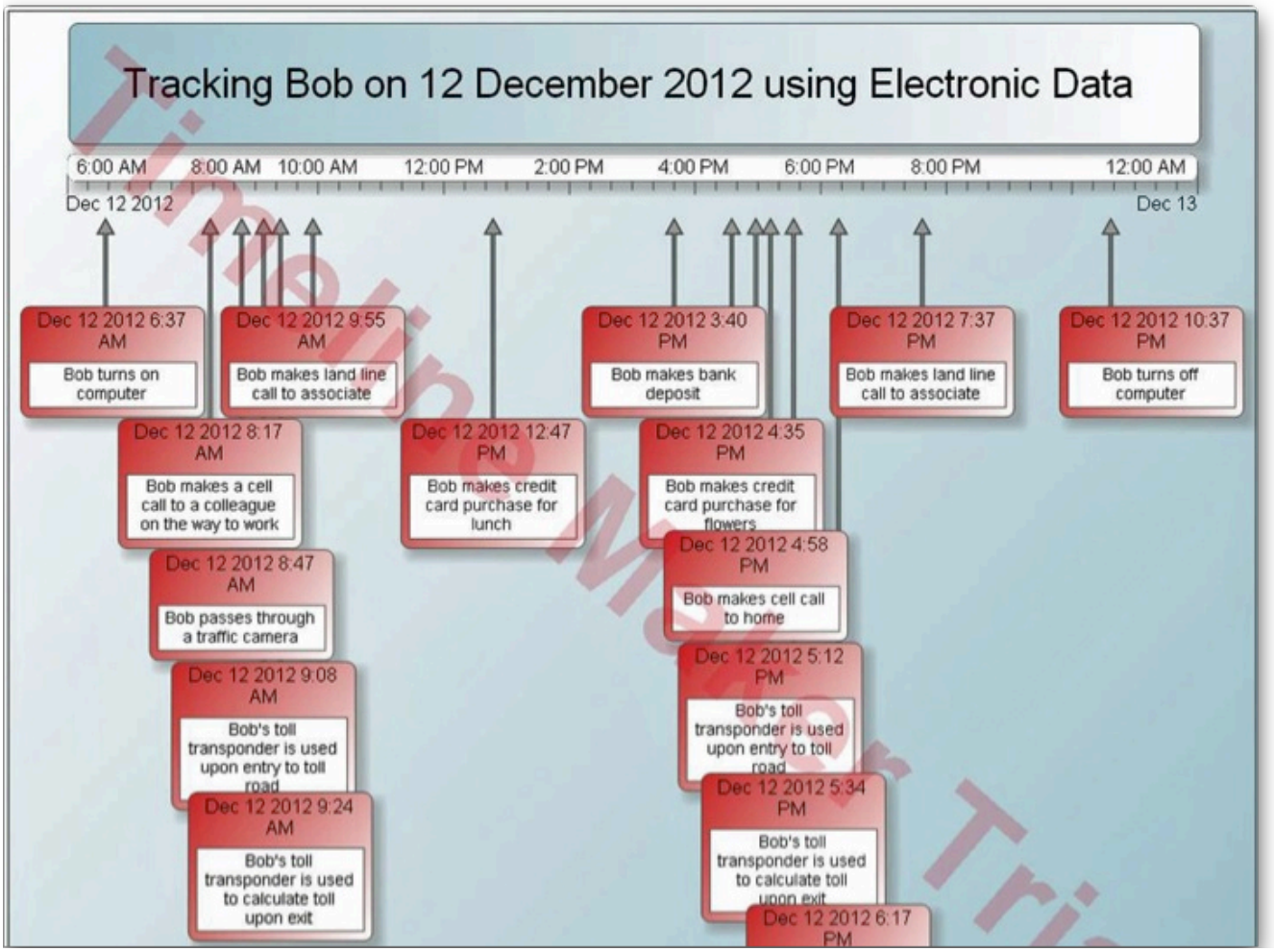
As Tim Shorrock has already reported, the back-end of THINTHREAD was used by the NSA in a later program called STELLARWIND (thereby forgoing front end privacy protections both Binney and Loomis built into their earlier, less expensive system). NSA then "illegally directed" STELLARWIND en masse sans privacy protections on Americans and the rest of the world.

The presentation began with a cursory display of the first three slides. Binney then explores the remaining slides in greater depth.

The presentation contains Binney's own slides and published documents released to journalists by Snowden.

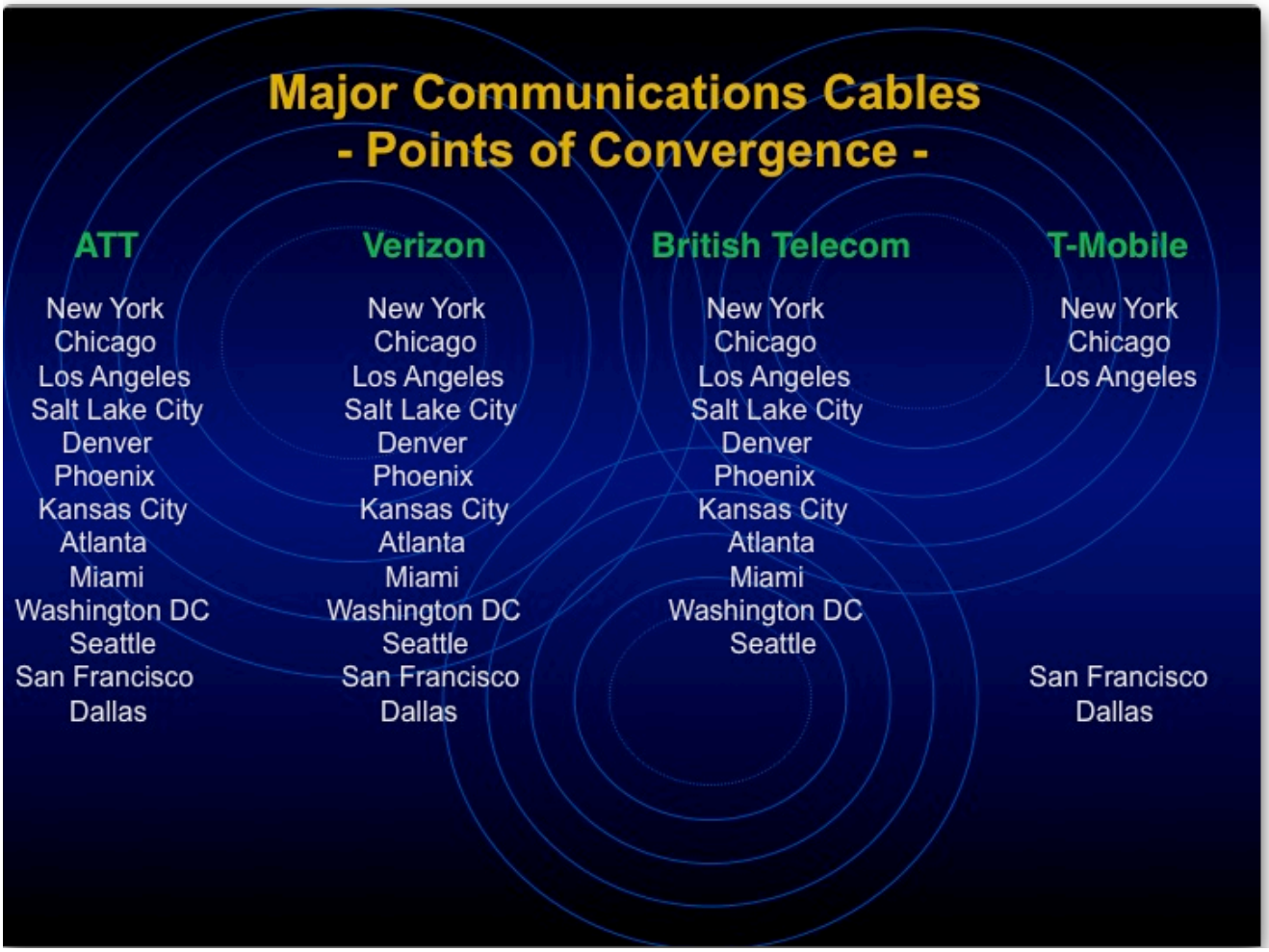
The presentation begins below:

(*Binney Slide*)

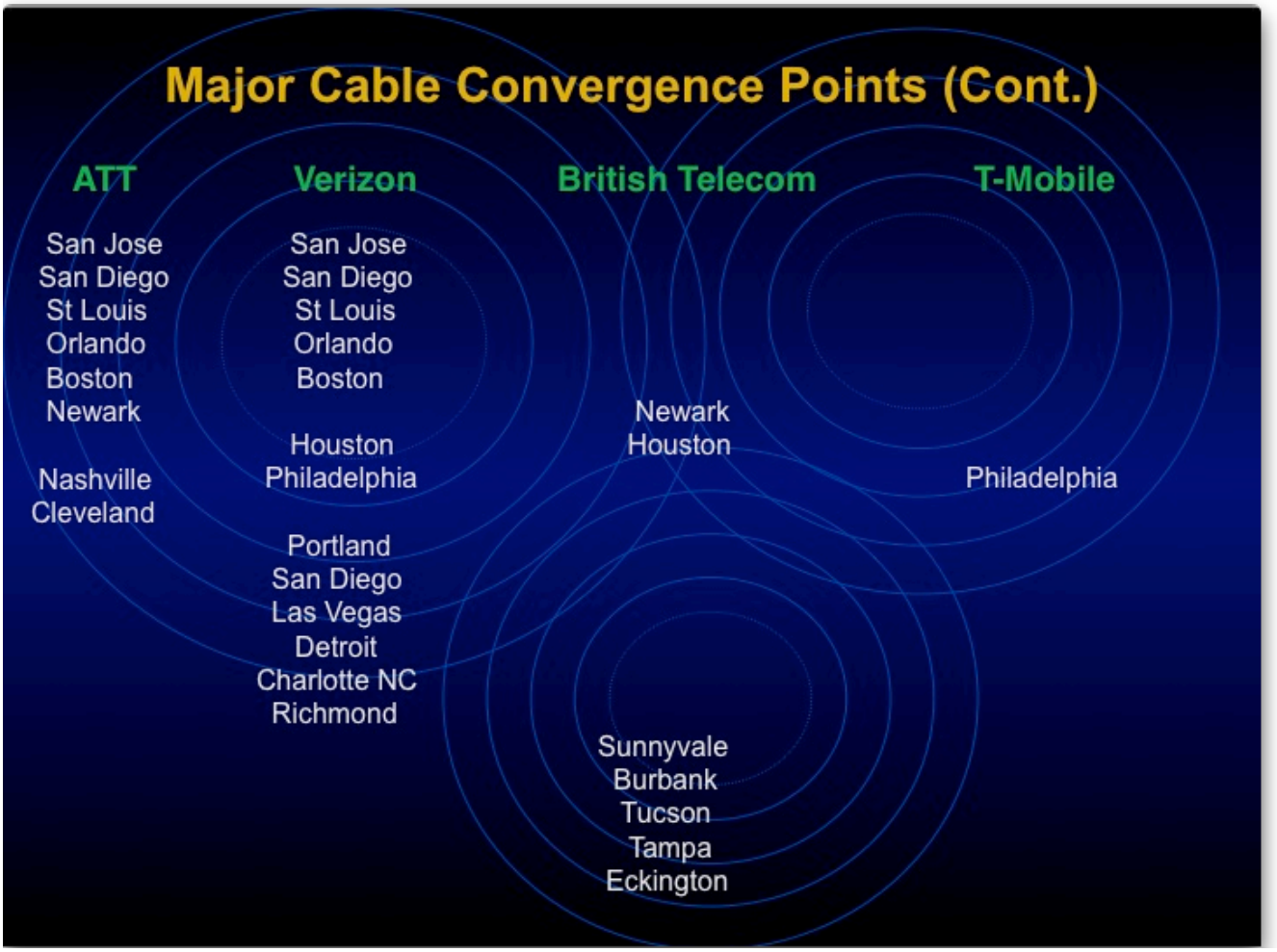


William Binney: Next slide.

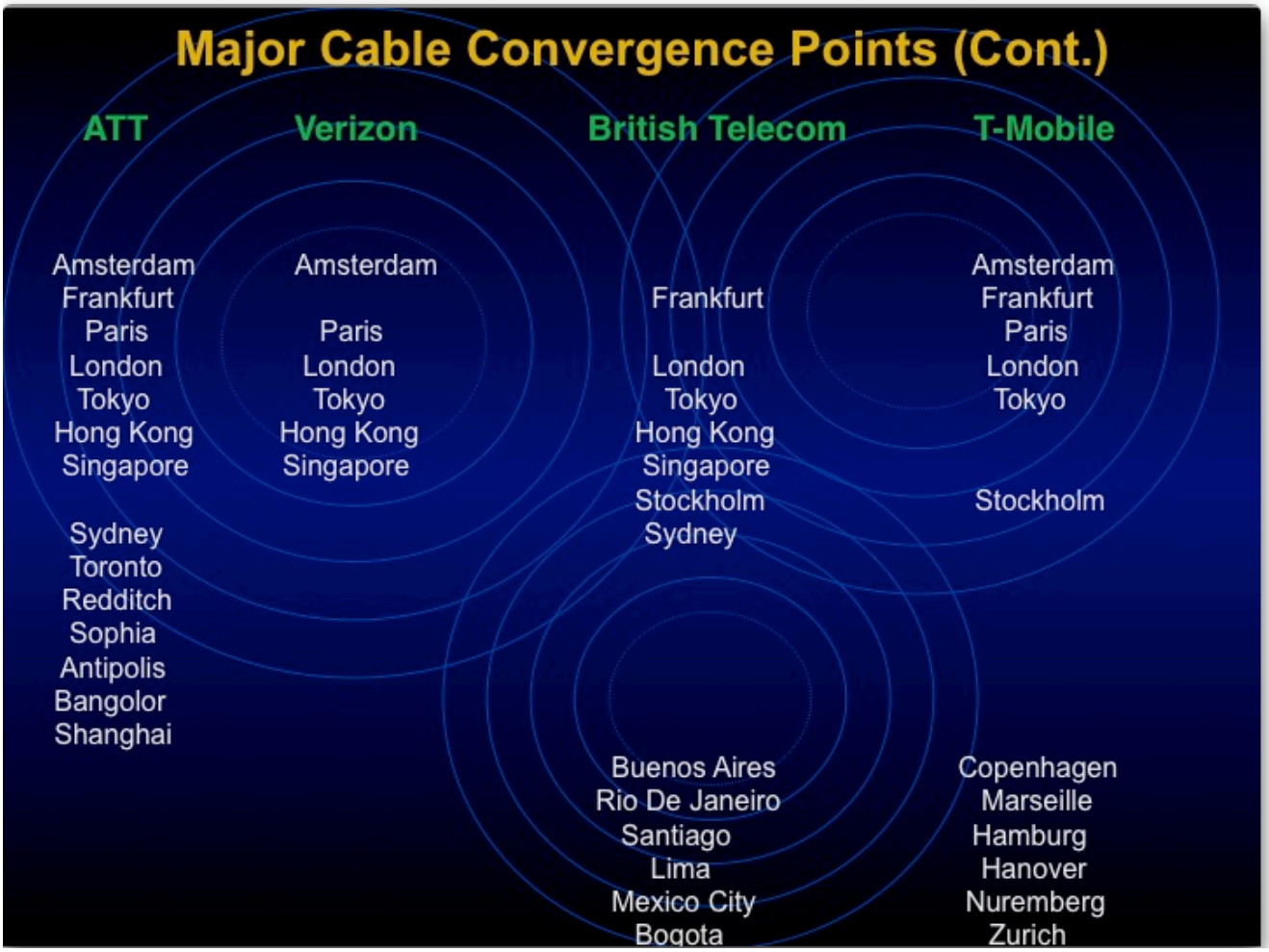
(*Binney Slide*)



(*Binney Slide*)



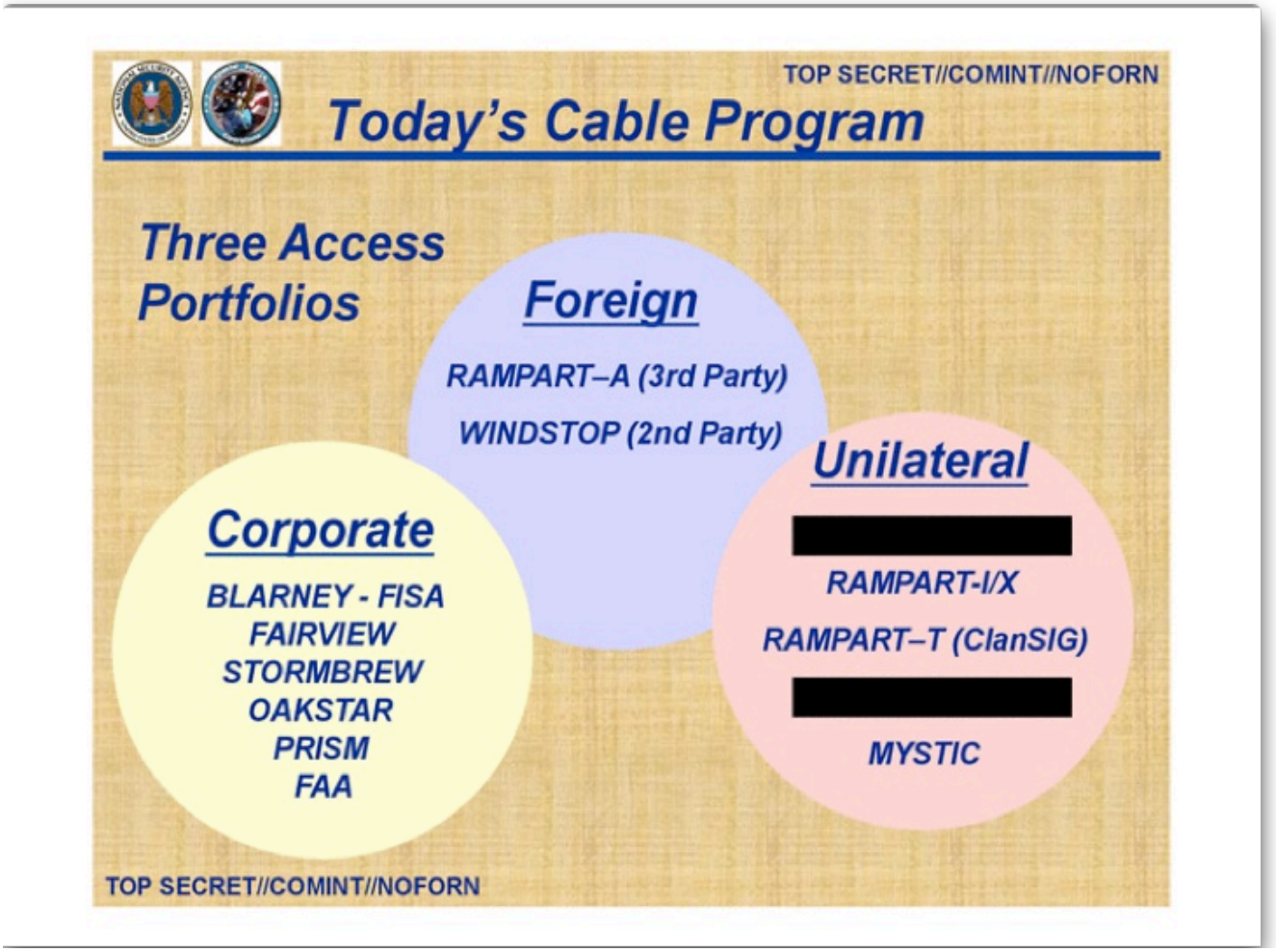
(*Binney Slide*)



There we go. Amsterdam, Paris, Frankfurt-- you know-- all the big points where they have fiber lines converging. So these were the major points to go after the collection of data. So how do they do it?

Next slide.

(*Snowden Slide in Binney Slide Presentation*)



There are three approaches.

One is you go after the corporations running-- I mean these are some of Snowden's slides. This is why I'm trying to find these slides, pull them together and put them in some sequence that'll allow everybody to understand what's going on. So there's three approaches to it.

One is the corporate one. This is where they go to the corporation and say, "How about cooperating with us? Give us access to fibers. We'll put taps on them and we'll duplicate the fibers-- you know, put a splitter on it."

Say, "Look. Send all the equivalent off the fibers into our Narus equipment-- or whatever other equipment-- the Verint kind of equipment-- whichever they have-- and you guys maintain it. We'll pay you to do that. We'll pay you for the access and we'll pay you for any data you give us." So that's the corporate cooperation.

And, those were separate programs that-- the one in particular that should concern everybody in the United States is FAIRVIEW. And we'll get into that one in a minute.

But the rest are OAKSTAR-- other foreign companies.

These are all corporate relationships directly with NSA.

No government-- 'other government' is in between.

And the other way is to go to the governments themselves and make arrangements with them to host their system and sponsor them with the local companies and fix-- and put the taps on the fiber lines inside those countries.

That's RAMPART-A-- is 3rd party.

WINDSTOP is 2nd party. 2nd party is Canada-- the other English-speaking countries: Canada, UK, Australia, and New Zealand. Those are those four.

And then 3rd party is everybody else, and there's like, 33 of them.

So, then of course-- barring no cooperation from the companies or no cooperation from the foreign governments or any of their sub-agencies, like the BND [Germany] or GCHQ [UK] or the equivalents-- then they'll unilaterally tap them.

What that means is they can-- like, if they have a submarine in, like, the USS Jimmy Carter for underwater stuff-- and then other covert or clandestine approaches to tap into fibers anywhere in the world.

That's how they got into Google and all their fiber lines between the centers that they had. This is where they did it.

Also, in there is-- they have over 50,000 implants in the switches and servers around the world on the internet. That means they own the internet. What that implant could do is mirror-image everything or extract data from servers or they can do--

Question: Software running in servers? Or is it hardware?

William Binney: It's software. In the switches and some of that's a mix of software and hardware.

For example, Jacob Applebaum at the 30C3 [30 Chaos Computer Congress] I think it was-- gave a list they went through and showed a slide where they had people going in where Cisco routers were being shipped.

In the middle of the shipment they delayed it-- and they put it on the side-- and these guys came in and put hardware and software in it to basically be the implant for that switch and then shipped it off to wherever it was going-- and whoever installed it installed the implants for them,

and you know, got it running.

Question: So these are not backdoors that are persuaded by American government-- NSA to Cisco. These are not backdoors that are deliberatley put into place by Cisco itself?

William Binney: No, the back doors are into, like, crypt-systems and other systems by other companies that are FBI-directed. There's a program called BULLRUN that they use to weaken crypt-systems and put back doors into them. So that's a separate program.

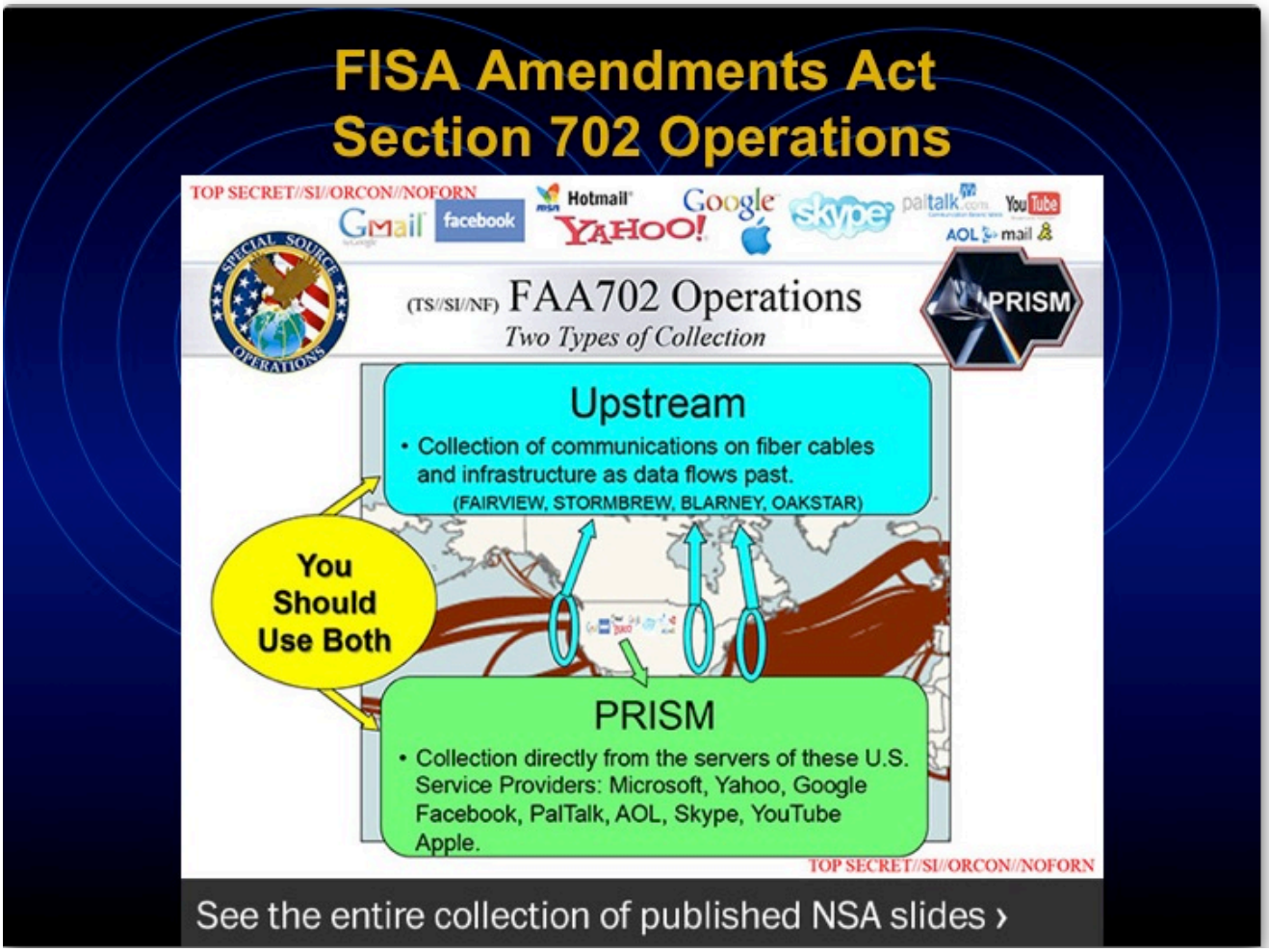
Question: In the same way what you were describing what occurred with Google? Which is it was essentially a physical hack into the lines that they thought were secure, and--?

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

The path the NSA would like to take would be the corporate first, because that's the easiest. The corporations will support it or do it with the foreign system, and you know, the foreign governments-- their agencies will help you.

So looking at the one slide that Snowden released on the PRISM program--

(*Snowden Slide in Binney Slide Presentation*)



It shows the UPSTREAM collection area and that's really where the major collection of data occurs and it's done under Executive Order 12333-- not under FISA 702 or the Patriot Act or any of that. It's all done under one -- Executive Order 12333.

And you see the names there: 'FAIRVIEW', 'STORMBREW', 'BLARNEY' and 'OAKSTAR'-- those are some of the major programs in the UPSTREAM collection. UPSTREAM means outside of the corporation, you know.

So now let's go to look at 'FAIRVIEW' that's the next slide.

(*Snowden Slide in Binney Slide Presentation*)

These are the tap points of the fiber line inside the United States. Okay?

The one in San Francisco was the one Mark Klein exposed, which was the one with all the Narus devices-- where they're taking all the data off the fiber lines. Well, these are the rest of them. There's between 80 and a hundred of them.

Question: What are the colors for?

William Binney: The colors. My estimate of that-- the dark blue ones are the major Internet sites. The rest of them are the telephone network. Okay?

This is where they record the telephone conversations and keep them stored for a period of time. That's how for example, Tim Clemente, the FBI agent that commented on CNN about the bombings in Boston. And he said, they had a way of getting back to the phone call that one of the Tsarnaev brothers made to his wife. This is how they do that. They record it here with these different places. This, by the way, maps very well through the heat map of the Internet activity of-- or the communications activity of the United States, also maps the population distribution.

Question: Cell phone networks? Because is it both data and voice-- are they-- is there like usually like a spoof tower or are they taken before or after?

William Binney: This is the AT&T network. So you're doing the AT&T switches.

Question: Everything in cell phone network dumps back into the primary phone--

William Binney: Right. It comes right back into the switches systems-- then goes, gets routed up to the local tower.

Question: Stingray devices. That are often used by local police-- sort of before stuff gets into the network.

William Binney: Yeah, I know.

This is done by NSA and NSA has access to the entire AT&T network.

Question: Why would the federal government also have these other systems? Seems redundant? Or is it because the police wouldn't have access to NSA information?

William Binney: Well, none of this is releasable or admissible in a court. We'll get to that later.

Question: The white sites there on the FAIRVIEW slide? They don't appear to have color.

William Binney: I assume the color has to do with whether or not-- they're variations on whether-- how much-- or maybe he extent of the ability to record and retain data.

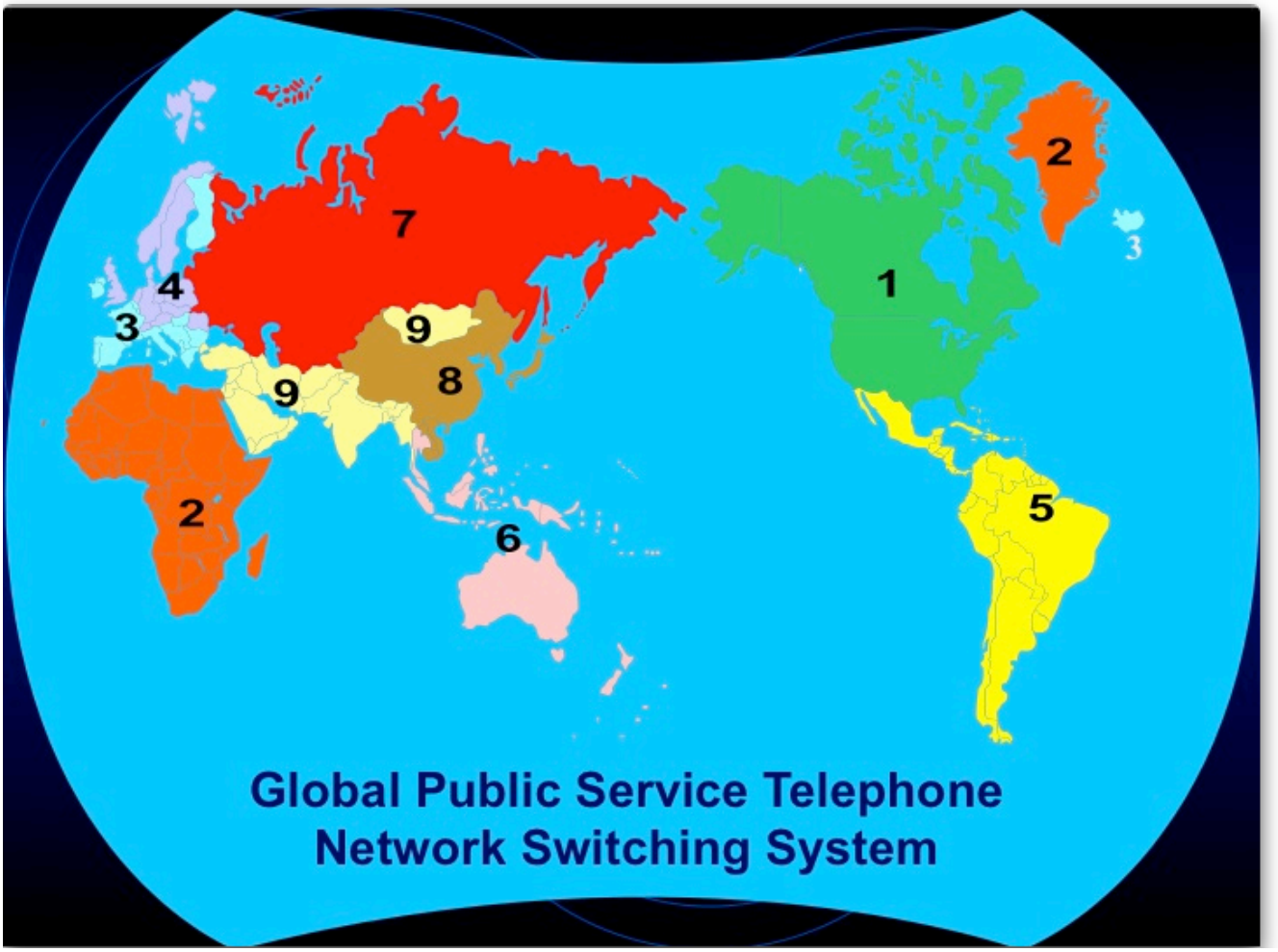
Because it looks like there is a gradient of colors. I don't have an index down the side to tell me what it is-- I just have to guess at it.

Question: For your concept of how to intercept with THINTHREAD are you against this kind of-- ?

William Binney: I would never be doing the United States, okay? That's what they're doing here. Only thing I would do is-- I would be looking only at foreign threats basically, which would mean I'd look at the transoceanic cables and the surface points along the coast of the east and the west. Nothing internal.

Okay. Next slide, yeah.

(*Binney Slide*)

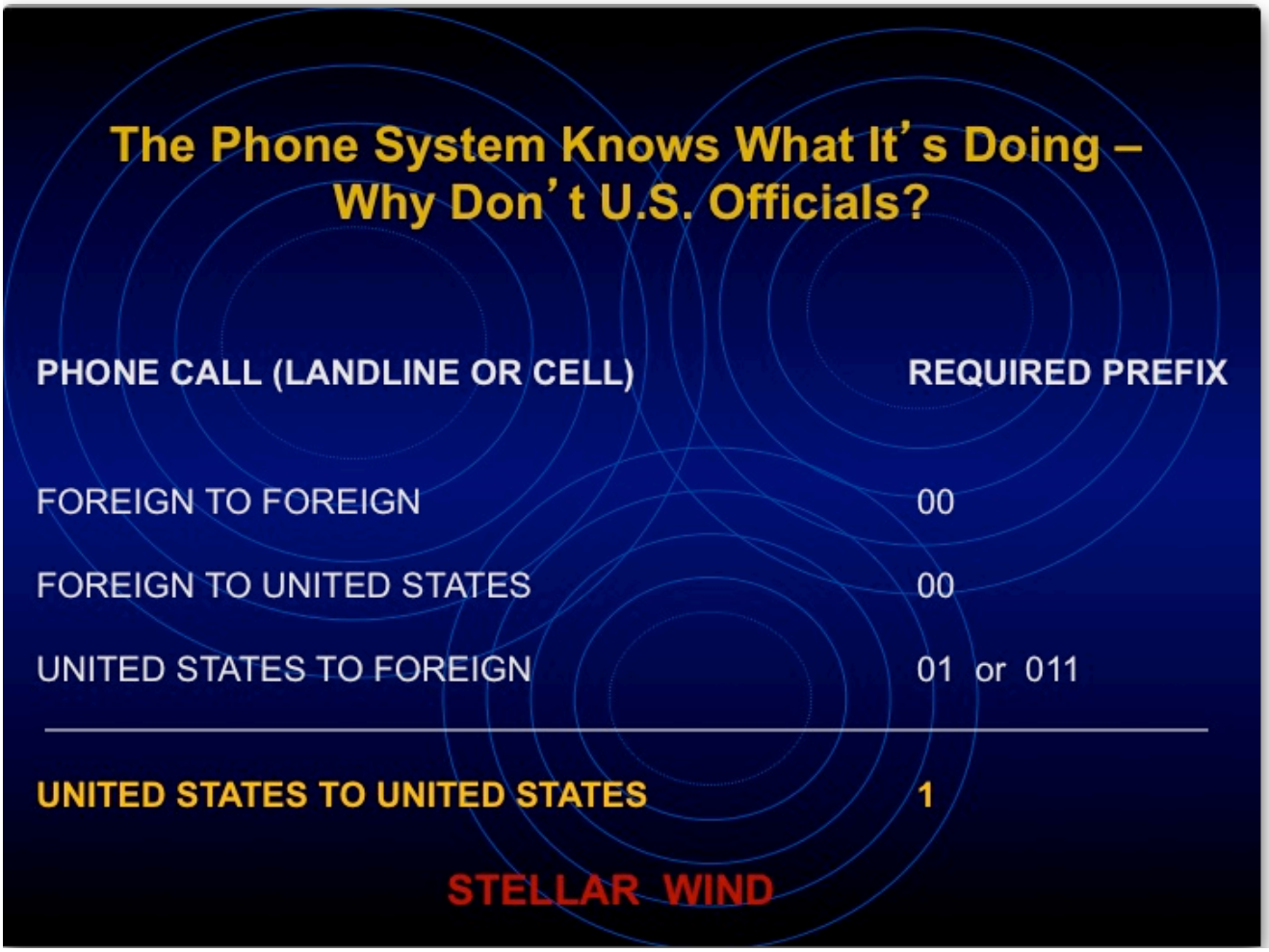


So getting down the phone network-- the phone switch telephone network. That includes satellite phones, and mobile phones, and everything, worldwide-- it's all numbered. There's a number scheme for it. The entire world is broken up into nine zones and these are the numbering schemes for those zones.

If you dial a number from the U.S.-- '01' or '011'-- then the zone of the world you want to call. If it's 3 or 4, you're going to Europe-- 7, Russia, and so on.

So I mean, the entire number scheme tells you exactly who you you have on the line-- these are machines passing it, so they have to have this data both ways, so they can route to and back. The machines do this. So if the machines do this, you know?

(*Binney Slide*)

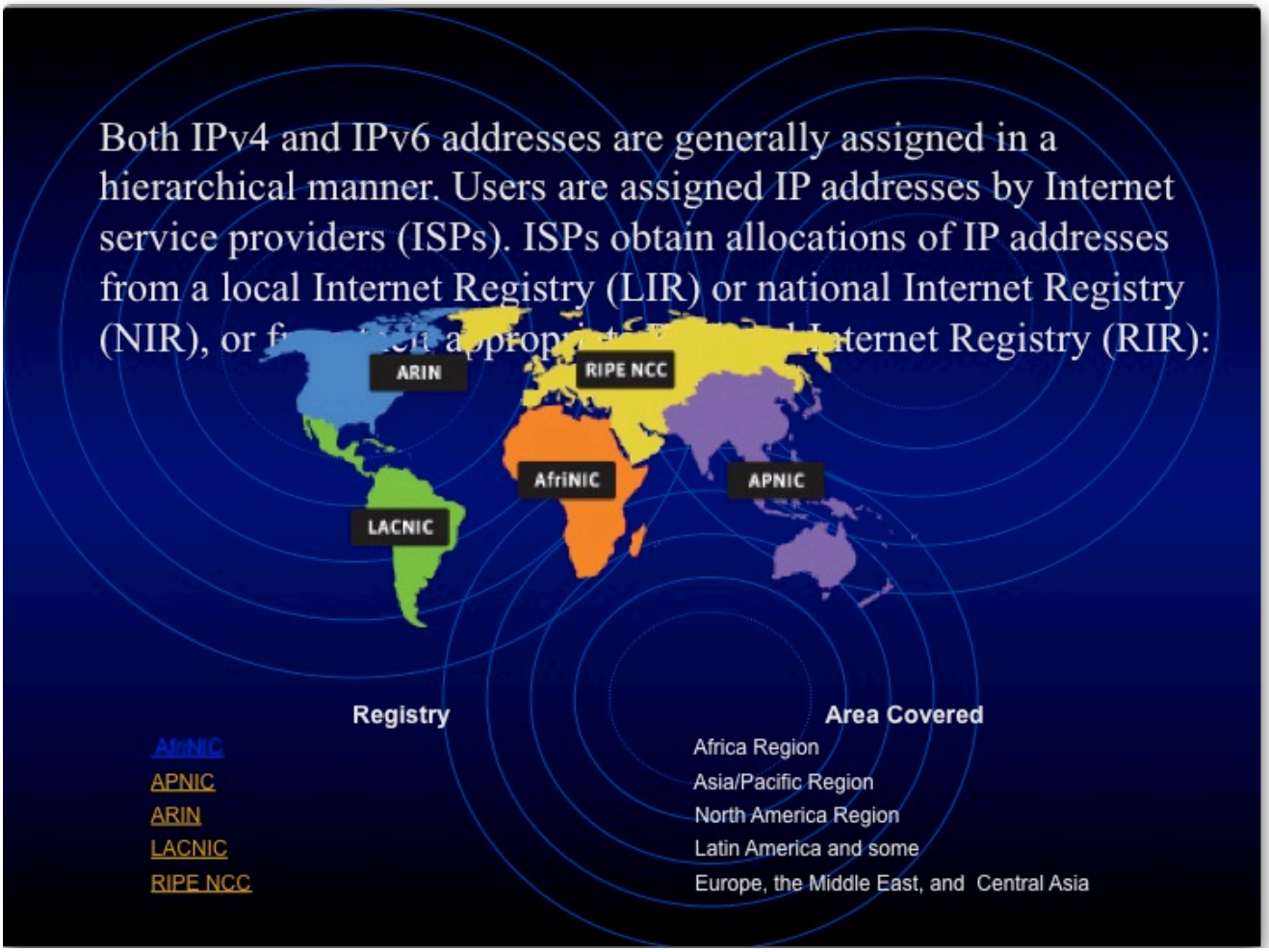


I mean, how could [Keith] Alexander [former director of the NSA] come up and say, "I don't know if it was in the United States." When in fact, the machines have to know, okay? You have to, or it doesn't get through.

So if you wanted to eliminate everybody in the-- STELLAR WIND is doing the U.S. side of it. That's that program. But you could pick that up. Everything but the '1' is obviously and currently in the U.S. or in Canada-- could eliminate that, and then you could delete that-- as you saw-- as they went across the line. That's how we did it.

Then of course, the next slide.

(*Binney Slide*)



Slide is the same with the Internet.

Question: Well, what is their answer to that?

William Binney: They lie. It's a way of trying to avoid a nasty issue for them.

They're really smart people. I mean, they have to make the job look complicated. It's not complicated at all. They're real simple. And in the Internet world, it's-- you know, IP address out of the IANA [Internet Assigned Numbers Authority] or the ICAAN [Internet Corporation for Assigned Names and Numbers], you know.

So, I mean-- the Internet world is divided into five zones, right? And you just block assign different number blocks to these different zones. Then it's subdivided down from the regional authorities-- down into the country authorities-- down into the service providers in local areas. So even if they want to assign an arbitrary number, that arbitrary number still tells you what zone of the world it is. And even if you look at the assignment and sub-assignments, you can get even further down in that.

Question: In 1999, there was a review of the NSA as it was moving from-- basically analog to more digital and there were recommendations made by corporations. Do you know anything about that?

William Binney: Yeah. They all wanted to kill THINTHREAD because it stopped them from feeding on $4 Billion. And then a following $4B. Their whole objective was to-- and they lied in Congress about it, too. And we had evidence of that, too.

Question: And those were--?

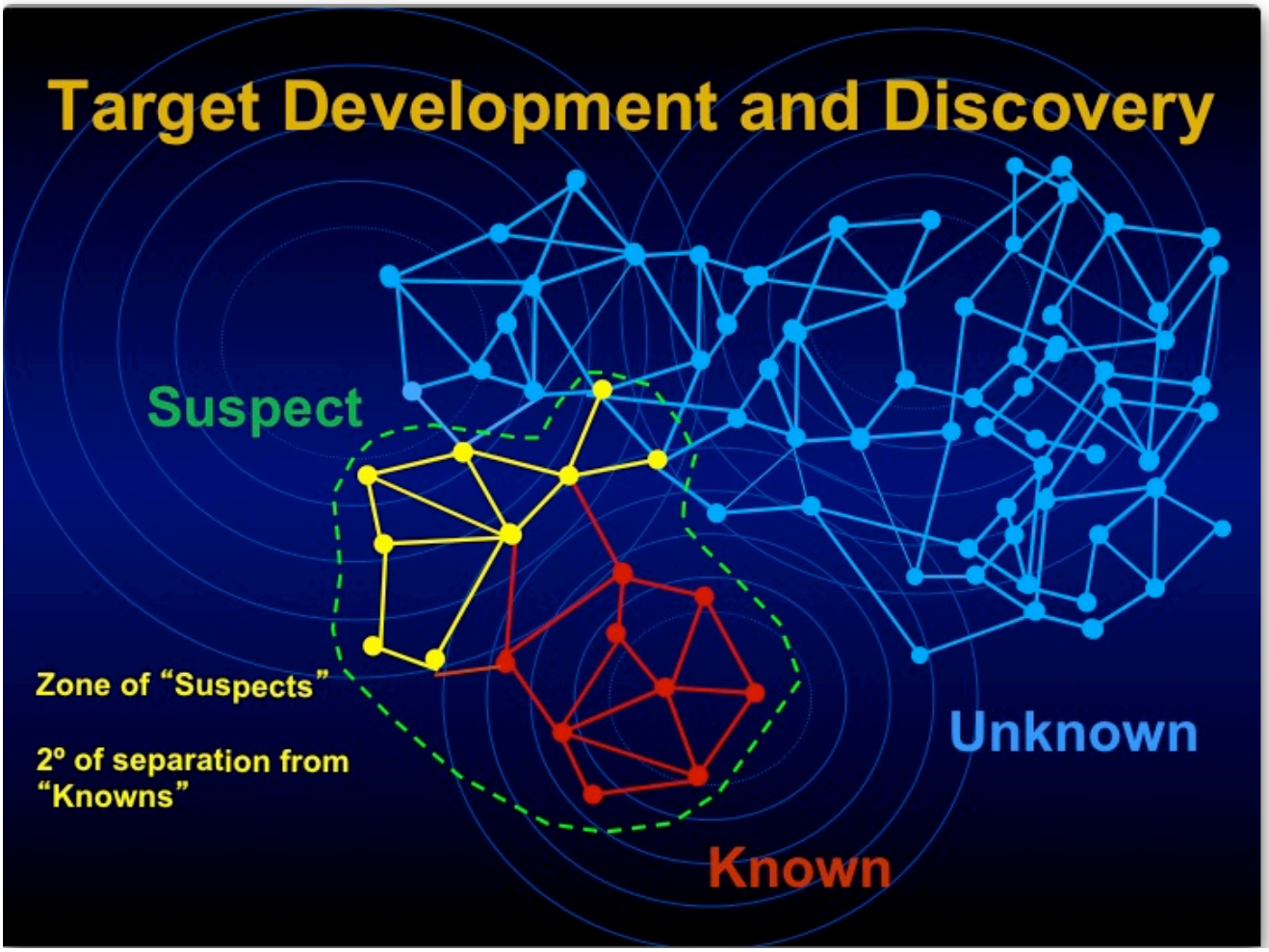
William Binney: TRW, Booz Allen and all the big guys. There were like 15 different companies that were involved in the thieving.

Question: Just to put the question out there, I'm curious of how much influence these large corporations also had in shaping NSA policy?

William Binney: It was directly. Yeah, it was directly influenced. I mean, they wanted to feed on all this money and they had all this influence and they used it with [Michael] Hayden and Bill Black from SAIC. SAIC was the major contractor for TRAILBLAZER right up front. They were the ones that got the multimillion dollar contracts right up front-- multi hundreds of millions, sorry.

So can we have the next slide?

(*Binney Slide*)



At any rate, this was the whole idea of target development, and how we-- this is how we eliminated the analyst getting involved at all with THINTHREAD. We wanted them not to be involved, because they make mistakes.

So, we designed this approach that said, for target development, you have a zone of suspicion around the known targets, the red there basically is the known targets and the zone of suspicion goes out two degrees.

And you look at the commonality for that. For example, we were trying to look at the content being passed out in that zone, to see if it actually compared to the content internally in the known zone. They're using latent semantic indexing, those kinds of things, to try to do that.

And the idea was if you had to kind of match, then you could say have an analyst look at it then, because we didn't want to waste their time. You don't look at anything until it looks good. So all this is done by software. Okay. And then you say, "Okay, here you go, take a look at this." Then that's where you build probable cause.

Question: What do you do about pizza joints?

William Binney: That's easy to eliminate. And you do that right up front. Very simply, because any company or department of a government has many, many subscribers. You look at simply the relationships and you can tell right away whether or not it's a company.

Question: So do you end up with false negatives there sometimes? There's some questions in the Boston bombing case, that the pizza joint-- some of these folks may have actually been a criminal front. And involved in some of the Russian Mafia stuff.

William Binney: But you could see that if you have--

Well, yeah, but you have to show-- you have to build probable cause on that. That would require more than simply one person calling them.

Question: Oh, yeah, yeah. No, I mean--

William Binney: Then everyone then has--

I mean, you look at that kind of thing and you record it, but you don't go through that as a second degree. You stop there.

The point is, if you had a pattern in which multiple suspects-- all were ordering from the same pizza place, despite the fact, you know, at a rate and frequency that would be much higher than one would expect for simply a distribution within the geographic area, that would be an indicator of like, oh, that pizza joint seems to be a nexus. Why is that? That would raise its profile within--

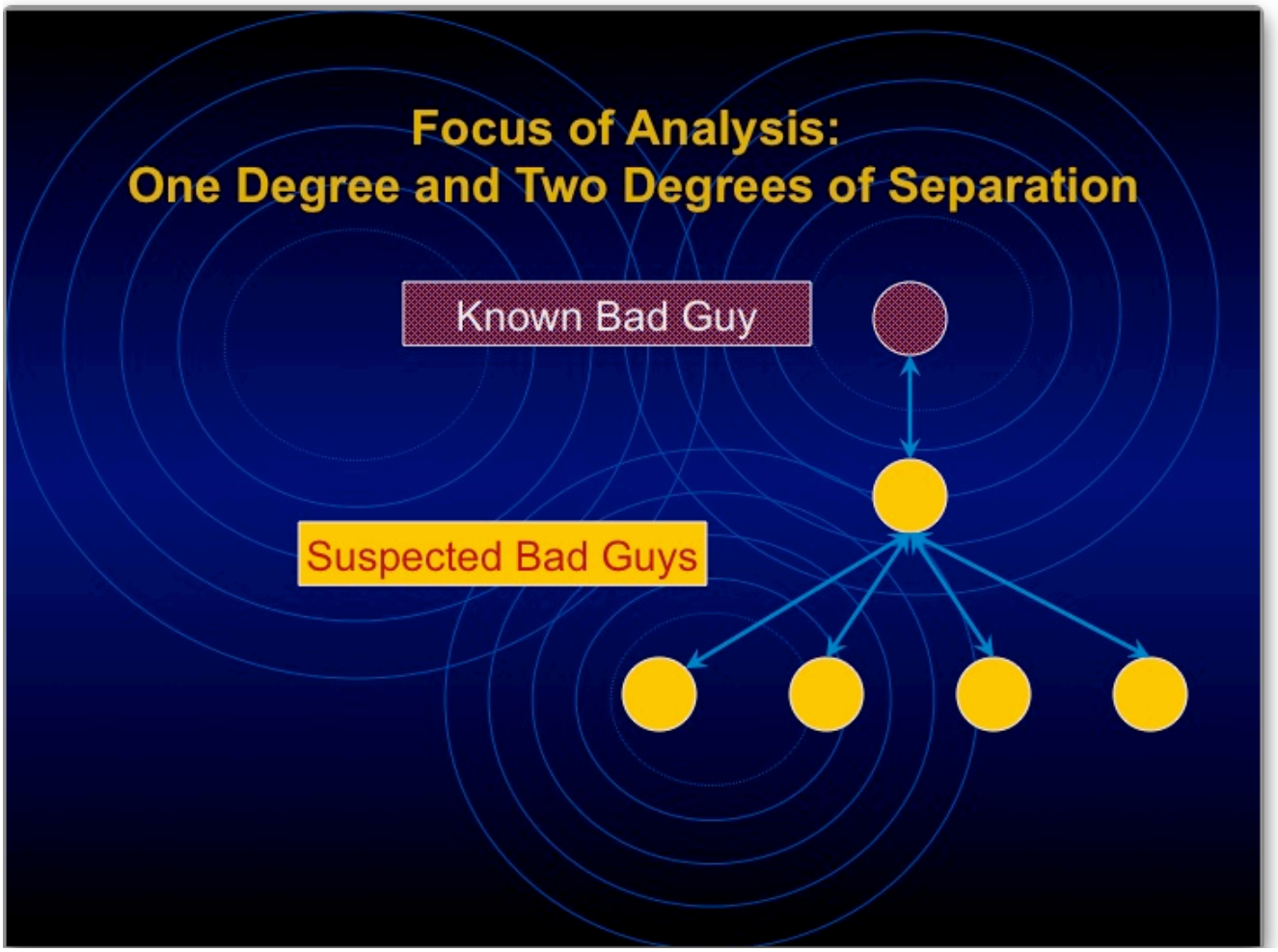
Question: So that average pizza joint would not fall into it, even though it receives lots of phone calls, including perhaps from some terrorists within the area? If they're phoning at a rate which is consistent. But if multiples are calling, then it shows up within the data.

William Binney: That's building probable cause. But the other point is you can also see, like, relationships, if it is a front company. And you see a relationship that calls to-- and then calls from. So you can build a relationship that way, too. So you'll see that kind of company would be suspicious in terms of building relationships like that. If it was a pizza company, "Why is a pizza company calling somebody, you know?"

Well, but that's how you would filter this out. I mean, you look at those patterns, what we're talking about.

Next slide.

(*Binney Slide*)



When it comes to putting data in the target list or list of things you want to look at, you don't have to go beyond the first degree [with THINTHREAD]. Because if you go beyond the first degree and put data in for the next three down, you get the next degree down from that. That's what you don't want to do. This thing goes up exponentially. So that's why they're getting buried with data. They don't do that.

Question: This, 'known bad guy' how is that defined?

William Binney: Let's put it this way-- we have been on the terrorist network worldwide for 30 years. So we have been developing these targets for that long and we know exactly who these people are.

Question: But so-called 'eco-terrorists' or eco-activists, depending on how you look at it? Is it people actively threatening to harm individuals, or?

William Binney: Yeah. Well, these terrorists were like Al-Qaeda, Hezbollah, Hamas, FARC. I mean, we had their entire networks.

Question: So with THINTHREAD, for someone like Jahar Tsarnaev, would you be able to look at that person and say-- he actually didn't have anything to do with it? Would you be able to exonerate him?

William Binney: Well, I mean, except for the fact that he got caught in the act. But no--

Question: Would THINTHREAD tell the level of his implication?

William Binney: Yeah, the question whether or not we'd be able to pick him out before the event? I mean, intelligence is supposed to be predictive in terms of intentions and capabilities. After the fact, figuring out how much data you had in your database about people, that's a forensic situation, that's a police issue.

We may not have been able to associate him, if his brother was the main point. Right? I mean, and he was depending on his brother to do whatever he wanted done. So we may not be able to pick him out that way, but we've certainly would have got his brother.

Question: So these people are identified in terms of the metadata-- where the connections are made back and forth? It's not so much about the content?

William Binney: It's a little bit more than that, because when-- THINTHREAD had other criteria, too, like if you were using a satellite phone and you were in the mountains of Afghanistan, or the jungles of Peru--

Question: There's also a metadata, but it's a certain type of metadata?

William Binney: You became suspicious right away. But just from the properties of knowing the geopositioning of satellite phones, you knew who would be candidates for looking at. So that would be another set of the data. Or for example, somebody who was, frequenting sites advocating jihad, that would be an indication of maybe being radicalized.

Question: What would you do with agents of a foreign target, you wouldn't put them through two degrees of separation?

William Binney: We would do that with everybody.

Question: Including foreign leaders?

William Binney: Not foreign leaders, no. Those would be pretty much known.

Question: So then it would just be assigned to an analyst?

William Binney: They are on the target list all the time anyway.

Question: Would Putin be in non 'bad guy'? (Laughing.)

William Binney: No, he would be a target.

Question: That's a serious question.

William Binney: It is.

Question: I mean, a year ago, ISIS was the 'good guy', okay? They were the guys that were anti-Assad and now they're the 'bad guy'. So when do you? I mean, so sometimes the bad guy is perceived-- I mean, the bad guy doesn't walk around with a bad label on his head that's written in indelible ink, right?

William Binney: Well, that may be true in some cases, but in most cases, I think that's just wishful thinking on a lot of people's part.

Question: No, come on. We supported Saddam, then we hated Saddam.

William Binney: I know, but-- you would never say ISIS, for example, because the connections they had, were far beyond, you know, what was going on in Syria. I would never consider them. I never would.

Question: So the question is-- how do they stop doing what the CIA trained them to do, and-- ?

William Binney: I will not account for the CIA.

Question: (Laughing.) Those are policy decisions, though. You are talking about capabilities? Yeah, that was the question. How much does policy or politics affect the target list? Like how much of that is constant and how much depends on, you know, the policy of the day?

William Binney: I'm trying to think of an example. I don't know that any policy decision has taken anybody off the target list. I don't know of any case.

Question: What about ending up on the target list?

William Binney: I can't account for that for the present day.

Question: So anybody 'good' or 'bad' is being tracked if they are at that level?

William Binney: Yeah.

Question: How about monitoring of allies. For instance if you have allies on the list. What are you

looking for on the list? Angela Merkel--

William Binney: No, you see the difference now-- what I am explaining is what we were doing in THINTHREAD. What they've used-- is they've taken this program-- they have taken all the rules off and they're spying on everybody.

Question: We have a problem with inference. Guys do not run around with a 'known bad guy' or 'known 'good guy' tag on them. Getting from what's the data to what you can infer from the data is a really hard problem. That slide treats it as if it's already a solved problem, but it isn't already a solved problem.

Look, two years ago, they thought they had a particle that went faster than the speed of light. The whole physics community and physicists are by definition not especially dumb, spent 18 months or two years looking at that data, trying to figure out whether a particle could go faster than the speed of light. They finally concluded it was artifactual and thet convinced their colleagues and they decided it was artifactual. But it took the whole physics community 18 months.

Your profession, seems to me, already 'know' who's 'a good guy' and who's 'a bad guy'?

William Binney: I agree with everything you said. That's why THINTHREAD has a section called target development. That's why I was mentioning the idea of satellite phones coming up in Afghanistan or in the jungle. That's the developmental target.

They're always changing and then for example-- to take it literally-- with the terrorist program, you kill some. They recruit some. You kill some. They recruit some. You always have to look at new targets being developed. We don't know everything by any means, but we had their whole network of connections, because we can see people coming in and going out.

Question: But you can make mistakes, right?

William Binney: Yes, we can. So that's why you have to take a close look at them every time.

Question: And even if you take a close look, then you're wrong, right?

William Binney: It's not an automatic decision, no.

Question: But so where are those criteria set, in terms of what the targets of interest are?

William Binney: Those are basically set by the analyst for that specific target.

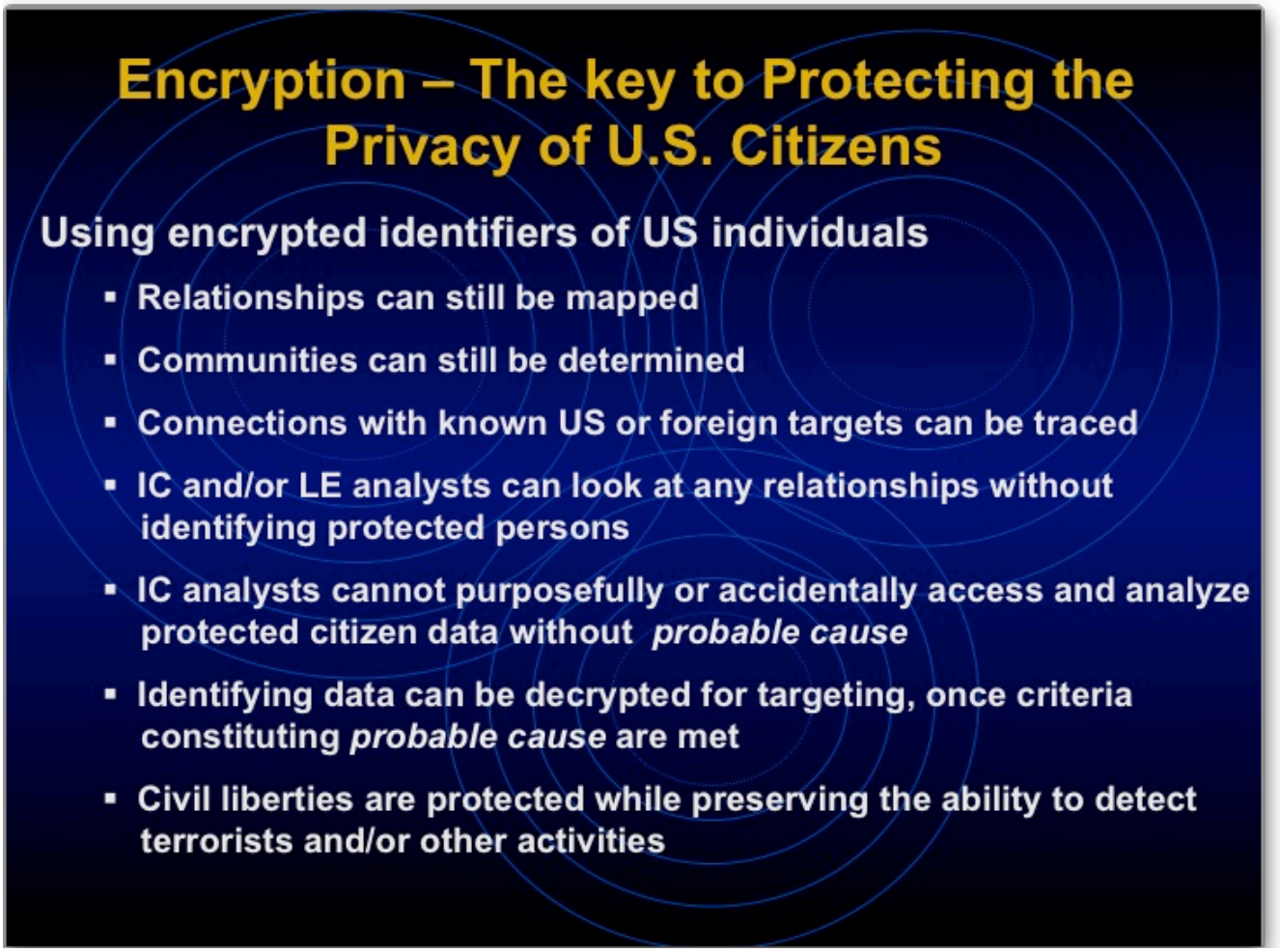
Question: And they always come up with the right--?

William Binney: And they're fallible, too.

Question: They come off of the State Department terrorist organization list. That is a policy issue as well-- in terms of who the enemy is? In the Manning trial, for example, the government had to come to court and say, "This is the list of Foreign Terrorist Organizations. They've been on this list for this amount of time and they link up to who is defined as an enemy in terms of U.S. policy."

William Binney: Next slide.

(*Binney Slide*)



This is what we achieved with encryption, you know, we would do all these things. You could still do all the things that analysts wanted to do and protect people. That's all that says. Okay?

THINTHREAD required a specific list of reasons why you're making people targets. So in this list, you would have to sign up-- you are the analyst-- and this is why this is a target. And you put down the reasons. This could be reviewed. So it would be a review process. Right now, as far as I'm aware of, there is no review process at all.

Question: If you look at the 'no fly list' and why people end up randomly on the list?

William Binney: And you don't have recourse-- there's no way of challenging.

Question: Yeah, due process. Now, is there any reason that that protection of the privacy of U.S. citizens, that same standard couldn't be extended to everybody in the database?

William Binney: It can be. But that was the first thing they got rid of after 9/11.

Next slide.

(*Binney Slide*)

This is showing how it would-- if you did one step at a time, you have to really step through this, or skip this slide. This steps through, every bit of information coming in.

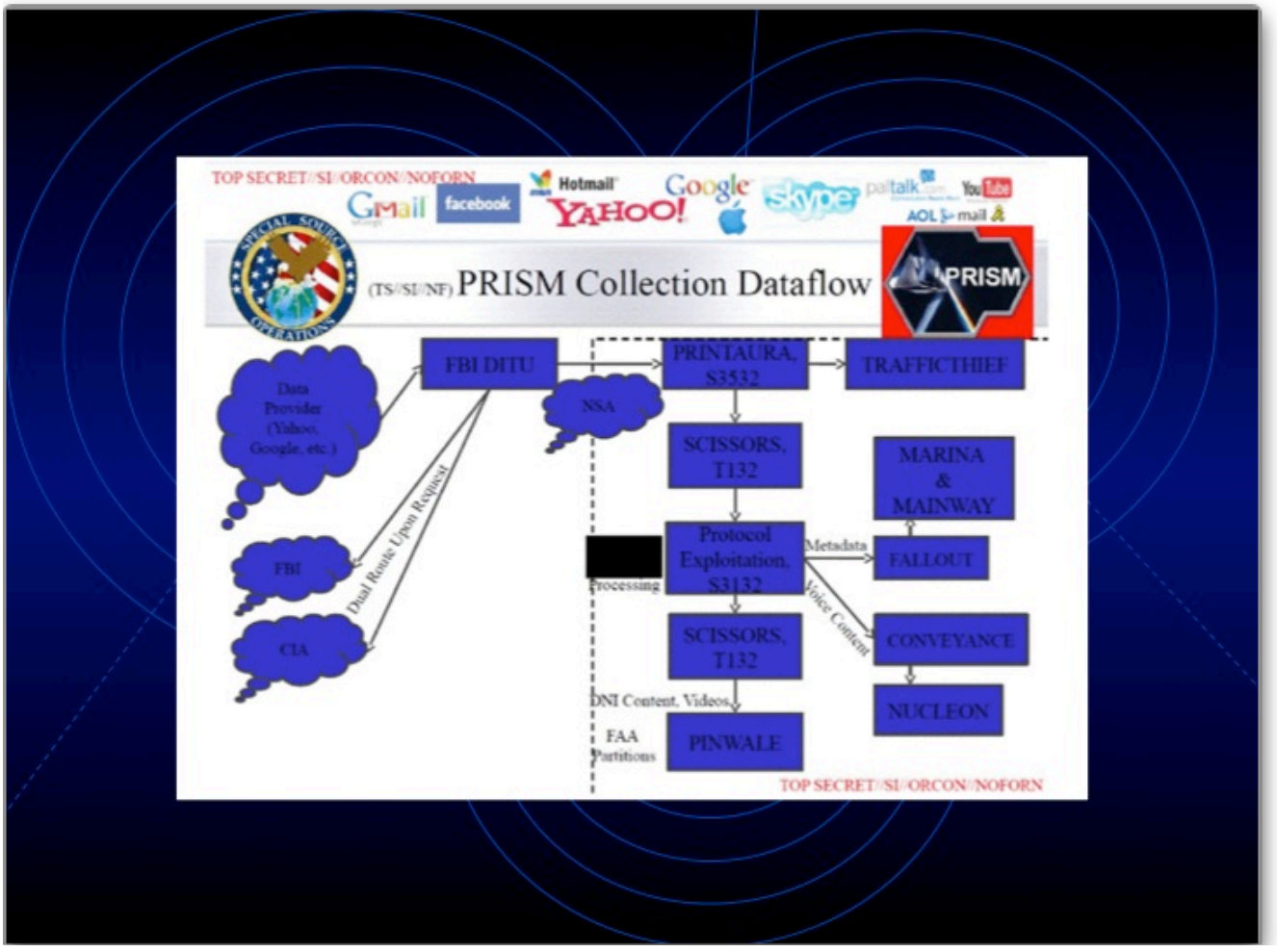
You first get it, things encrypted or not. Depending on who they were and where they were. And, as you went through, like, pretty soon we go to a now it's in the U.S.-- so you encrypt it, it's in Florida. Now you get some data on it, now you can decrypt it.

Like you have probable cause based to do this. That's the whole point, every time something happens, you have to have probable cause, according to the Fourth Amendment of the Constitution of the United States. So at any rate, that's how that would work. This was the data from 9/11, by the way. That's on the open source.

Question: So you get from 'protected' to 'wanted' just by association?

William Binney: No. You have to have multiple factors, in some cases, here we had telephone calls that gave you content that you could look at and say, yeah, they're participating in it. So they can develop probable cause.

(*Snowden Slide in Binney Slide Presentation*)



Then it all gets fed back into NSA and this little bracketed area over here is NSA. And those are the programs.

Basically the MARINA, MAINWAY, or the indexing. The graphing of phones and e-mails and things like that.

And then down in PINWALE, the database for the digital network, and NUCLEON is the voice stuff, encrypted and not.

And, then all of that is indexed back to MAINWAY and MARINA program, so that when analysts look in there, they can pull that out-- any community. They pull out of those spaces and with it comes index of all that data that's in the PINWALE and the NUCLEON base. So then that allows you to timeline everything that everybody did and everything they've said.

Question: Can you explain what SCISSORS are there?

William Binney: SCISSORS is simply a holding program that sorts out the metadata, sending it out through FALLOUT and indexes to MARINA or MAINWAY. So it's how it separates that out, but also continues to give the index to the data. It's the content data down below.

Question: And what is that S3132?

William Binney: That's the organizational designator inside NSA. They are handling that. But SCISSORS, you see, is those three blocks in the middle.

They shouldn't have laid them out that way, but it's really the same program. It's all within and the protocol exploitation is done within SCISSORS.

So these are the central programs. Now all you have to do is change PRISM input there to UPSTREAM, or you put in ECHELON or any other input source at all. And it goes into these programs or a similar kind of program for money or travel or whatever.

Question: What are the different attributes? I mean, money, travel--?

William Binney: Well, for money it's credit cards, account numbers, you know. And the transitions are transfers of money or purchases of stuff.

Question: And travel would be obviously whatever the TSA would take-- probably have that time?

William Binney: TSA, it's all reported as the people, names, and passports and stuff like that, that are coming in on a plane, or traveling on a plane. So all that goes into a database, and then you do comparisons of who's traveling with who. Right? Like can you group multiple people traveling on the same planes multiple times.

Question: It was said at the recent Aspen Security Conference, that basically the TSA knows everybody who is coming in-- and everybody the location of pretty much everybody in the United States on a day to day basis. They have it graphed out.

William Binney: NSA knows that, but I don't know if the TSA does. I mean, NSA gets five billion

records of GPS data on cell phones every day, so according to the Snowden material.

Question: Right. I'm sure the NSA knows more because they have more data points. But the TSA basically gets an intelligence brief every morning, at least about the people who are coming in and expected to come into the U.S.

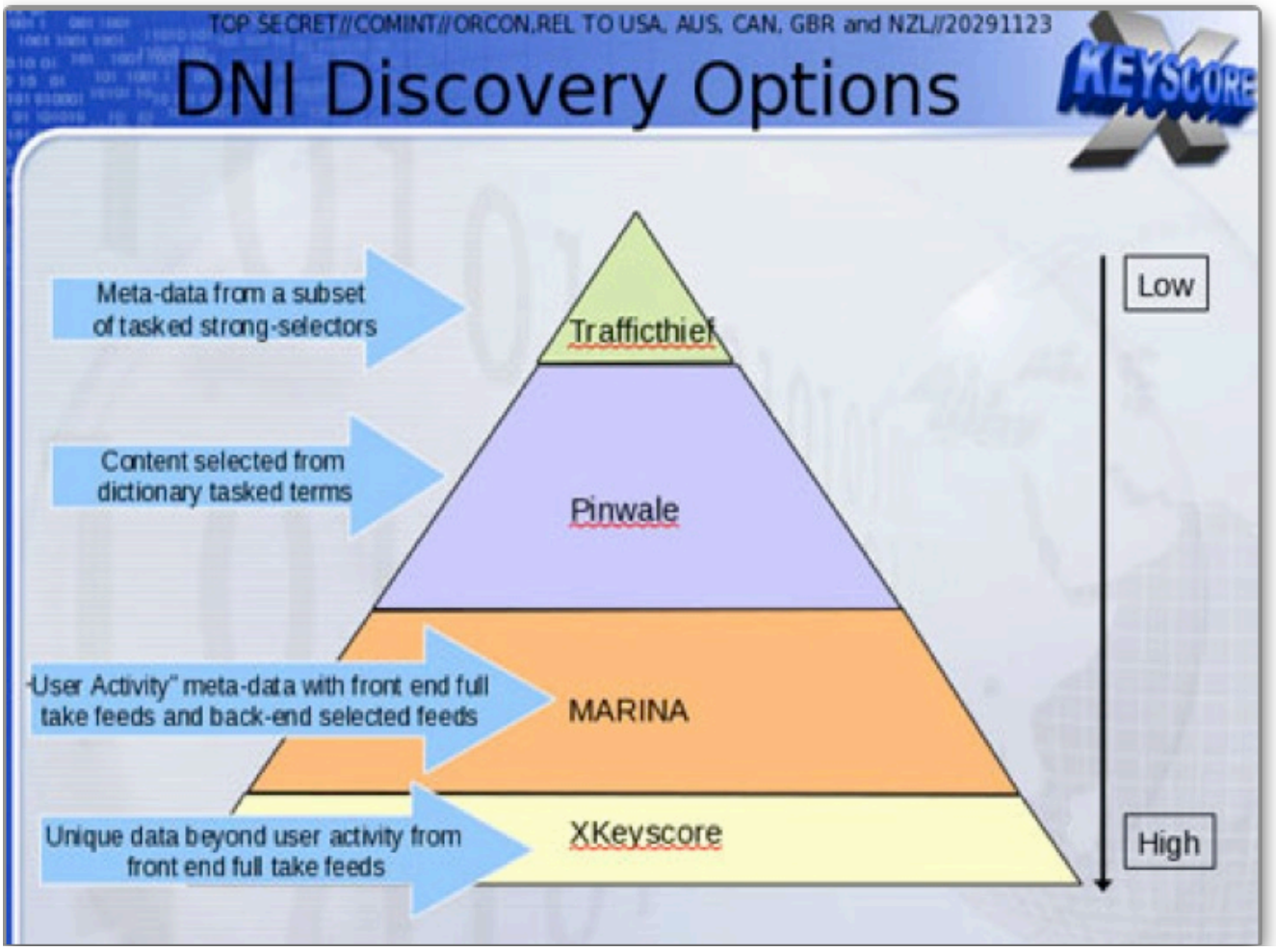
William Binney: But I'm talking about the whole population not just those traveling.

Question: So, for travel you are talking about GPS as a data-point generally in the travel attribute?

William Binney: That is what they are talking about doing.

Next slide.

(*Snowden Slide in Binney Slide Presentation*)



Then these are the analytics programs that they're looking at, the TRAFFICTHIEF-- it says 'tasked

strong selectors'.

An engineer did this, not an analyst, okay.

That means these are the specific targets that I want. And here is the metadata about those targets and take it out of the traffic.

So in this slide they're talking about discovering new things. So that's pretty low, you get what you know. That is what that says.

If I know these things, these are my targets, I get them. Then in PINWALE, they say, "content select from dictionary terms." This would mean, "My guys use these terms." Like if you remember the DHS term list of things, like "pork" was one word in there.

Idiots. So if you send an email home to your wife and say, "Honey, let's have pork tonight for dinner." You got sucked up by DHS. That's kind of idiocy-- it's called dictionary select.

This is like a Google search. This buries you in data, you can never get through this. It's a waste of time.

So but they're calling it getting greater or higher capability getting information, this is absurd. This is how you bury your analysts. And the same gets down here with MARINA and you know, and it's the same thing, and then down bar and the XKEYSCORE that means it goes into all the databases, pulling out the keywords and all that, everything all together. And so now you're really dumping on your analysts. So these are all idiots. And these are the engineers doing it, so.

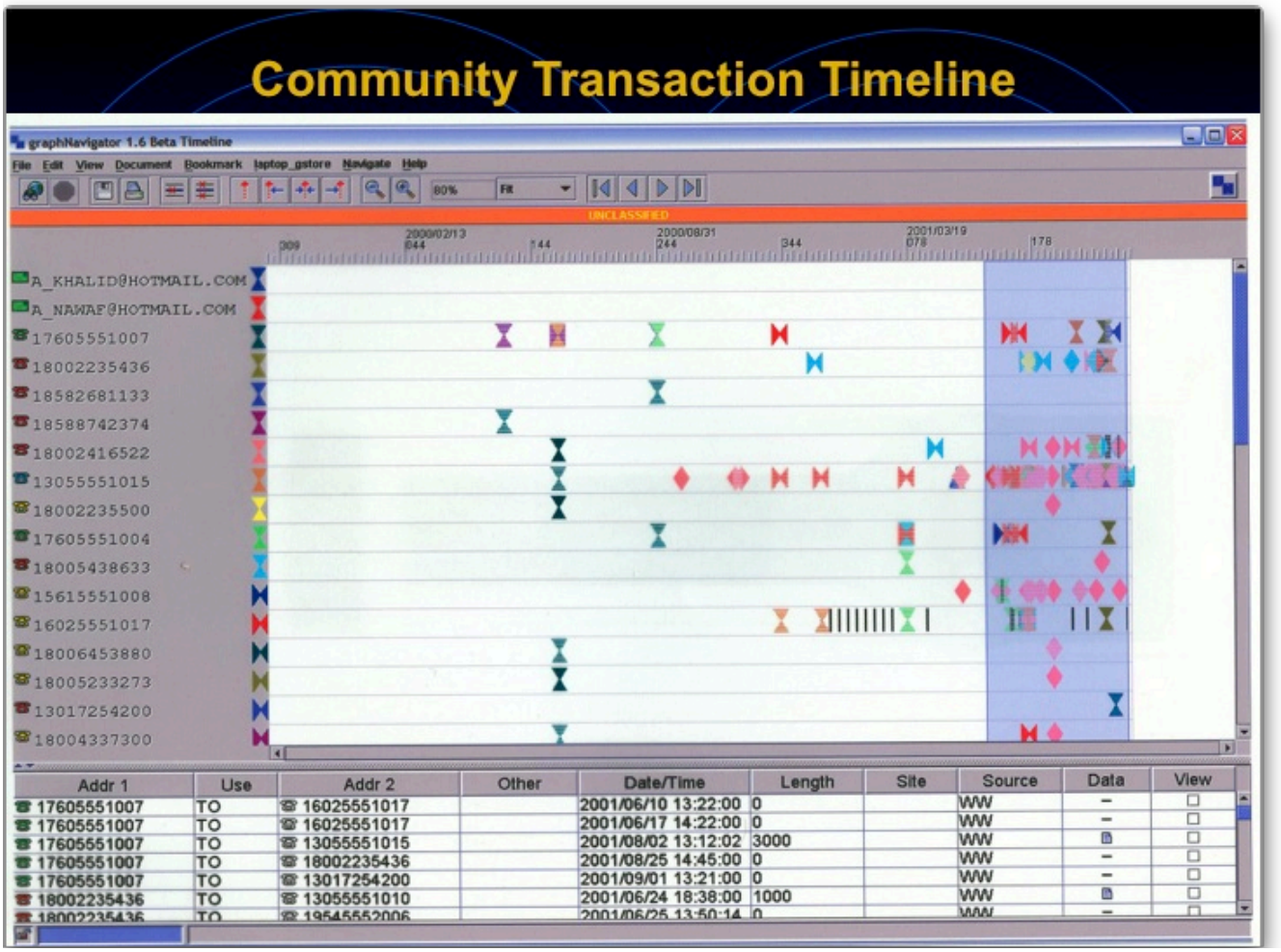
Question: Other than making money off of like these NSA contracts, what capabilities do these companies have, what other value are they generating for themselves?

William Binney: Nobody does return on investment at NSA. They don't.

I mean, if they did return on investment, they would throw away everything except TRAFFICTHIEF and maybe some graphing programs out of MAINWAY-- they'd throw all of this away. They wouldn't have built Bluffdale [Utah], that $2.3B or whatever it is-- facility to store data. This is all the data from PINWALE and MARINA and all that stuff is going out there, being stored. So they wouldn't have to buy that at all. They'd be more effective, because they wouldn't be buried. So at any rate, that's what they're doing.

Next slide.

(*Binney Slide*)

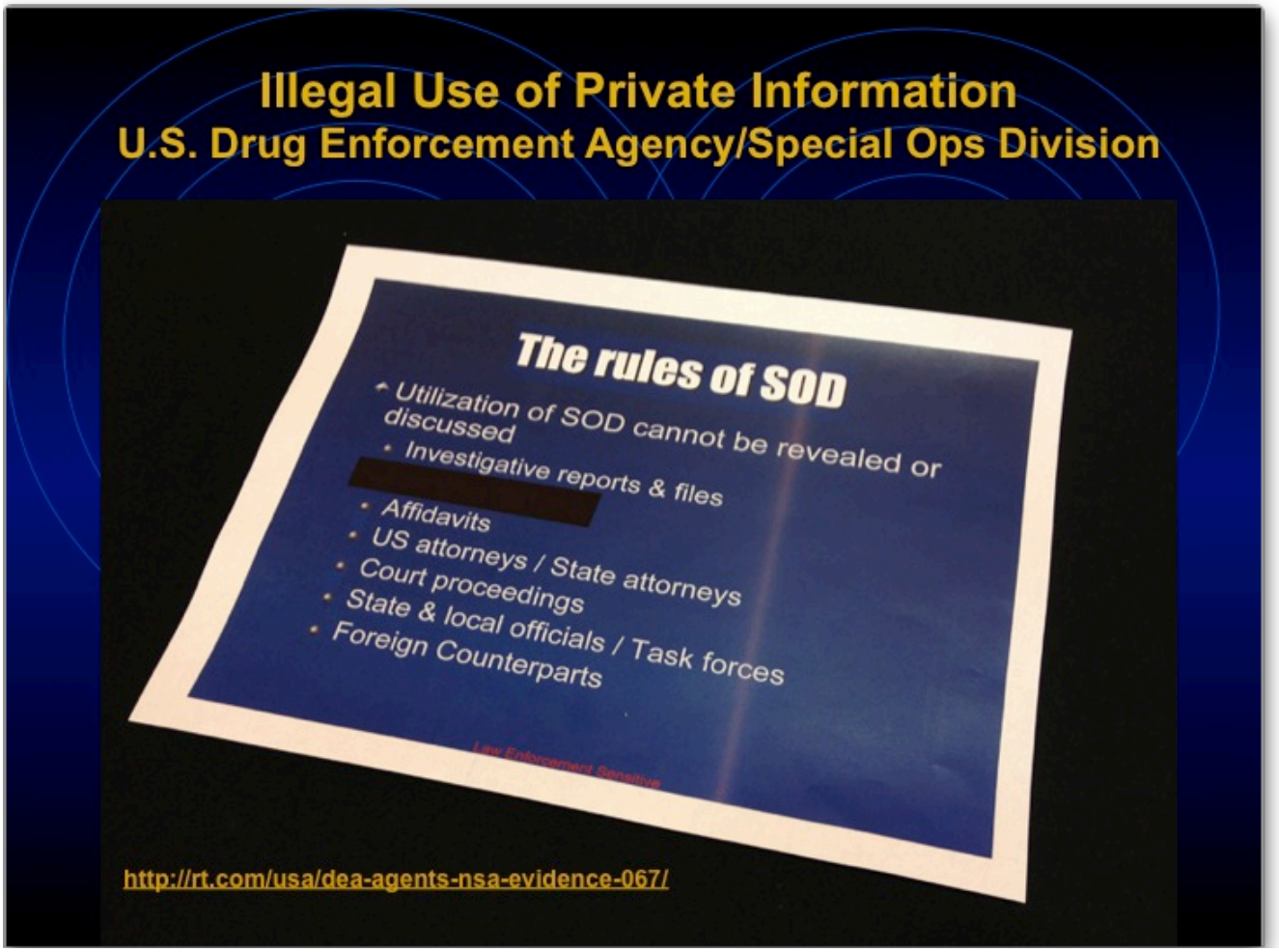


And then, once you do that, of course, you pull the data out from your-- take your graphing and then the MAINWAY MARINA program and then, when you pull this graph out and say, "I want this graph." Then you list the targets down the side. You highlight them, click, then you get a timeline of all their activity.

And down on the side over here on the right, it says "Data". Well, you go to that particular point in the graph and you can pull up their email or transcribed phone call and read it. And so that's all done. This was done for profiling targets. How do they interact over time?

Next slide.

(*Reuters Document in Binney Slide Presentation.*)



That, by the way, can be done on anybody in the United States, because that data is in PINWALE or MARINA, or NUCLEON or both. And it's indexed.

Question: And is that what Snowden was complaining about?

William Binney: Yes. Now, it even gets worse, because once NSA has all this data, they have to have a customer for it, and it's now turned out to be law enforcement. Okay. It's the FBI and DEA and they're going directly into these databases and querying them and looking for criminal activity and then they use this data to go arrest people.

And when they do that, they can't take it into court, because it wasn't acquired with a warrant, so it's not admissible in court. And, these are the rules for the-- this is the-- in the DEA is this SOD, or the "Special Operations Division". It's specifically tasked to look at NSA data for criminal activity.

In the SOD is FBI, CIA, DEA, of course, DHS and the IRS.

People who can look at the communications connectivity in MAINWAY and say, "Oh, here's all the

people in the Tea Party. Or here's all the people in any religious organization or Occupy or any of it." They can see all of that. So I maintain that that's how the IRS is targeting Tea Party people. Then of course it goes down and it says you cannot reference this data--

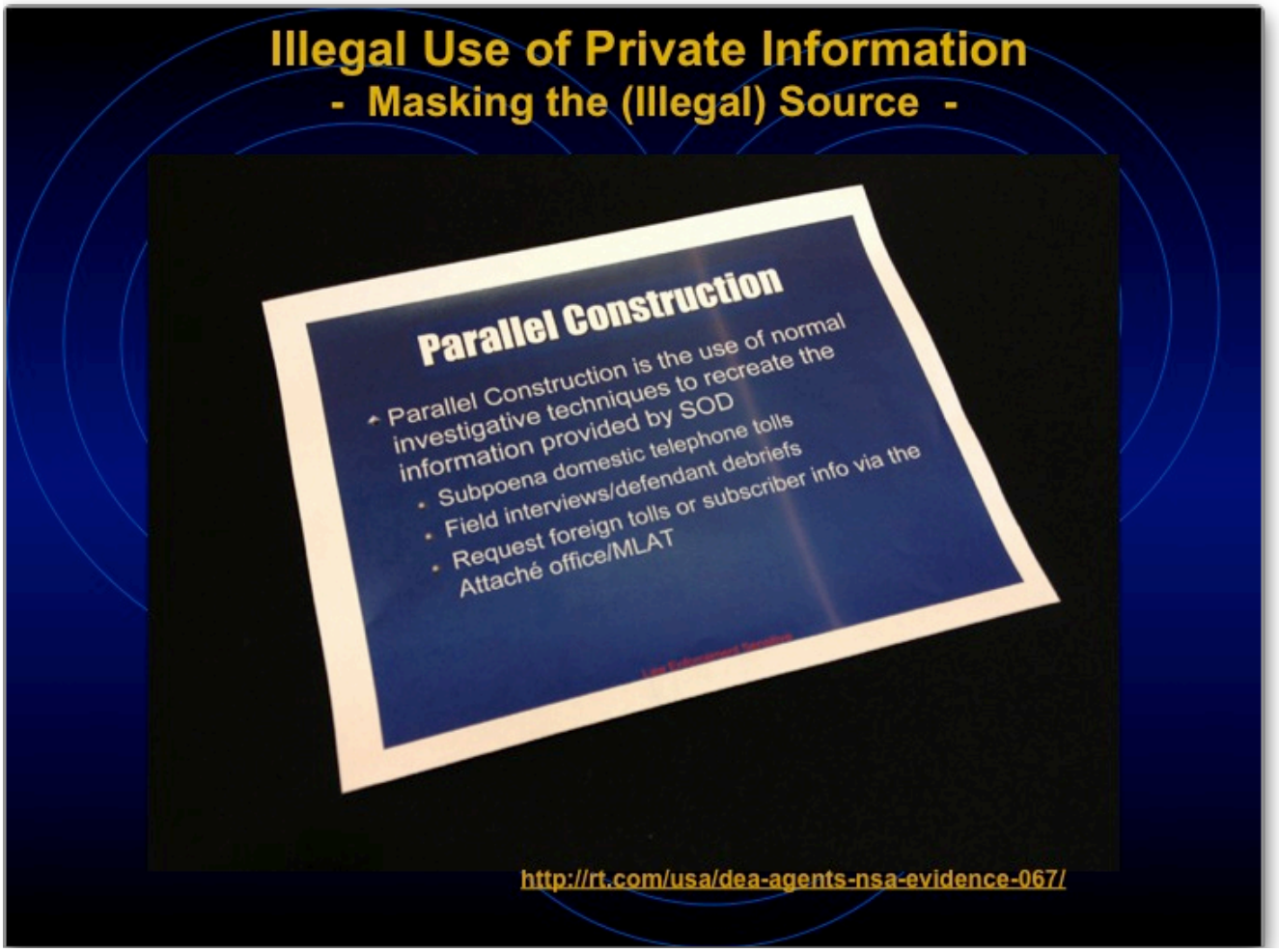
Question: Is that just your hypothesis?

William Binney: The only key point I have is the-- I can't remember her name, but I have it at home. She was testifying to the House Judiciary Committee. This was one of the people targeted by the IRS. And she mentioned some of the questions they were asking, she said, "They asked me a question about-- what's my relationship with this specific other person?" Well, my question now is (not what her relationship is) but how did the IRS know that she had it?

The only way they would know is looking right into SOD at the graphing in NSA. They would know that from that. That's how I put it down, that's why I made that inference. But at any rate, that means they can't take it into court, can't talk to the attorneys or state or local officials and you can't tell foreign counterparts. This is where it's the-- it's all the foreign police who have relationships with the FBI or the DEA, they're getting tipoffs through this system and not being given the data. So in other words, now to go into court.

Question: What's your guess on the part that's redacted there?

(*Reuters Document in Binney Slide Presentation.*)



William Binney: This is law enforcement, I really don't know. But, it may be connected with the MLAT [Mutual legal assistance treaty] procedures, I'm not sure. Okay. That's on this slide, so.

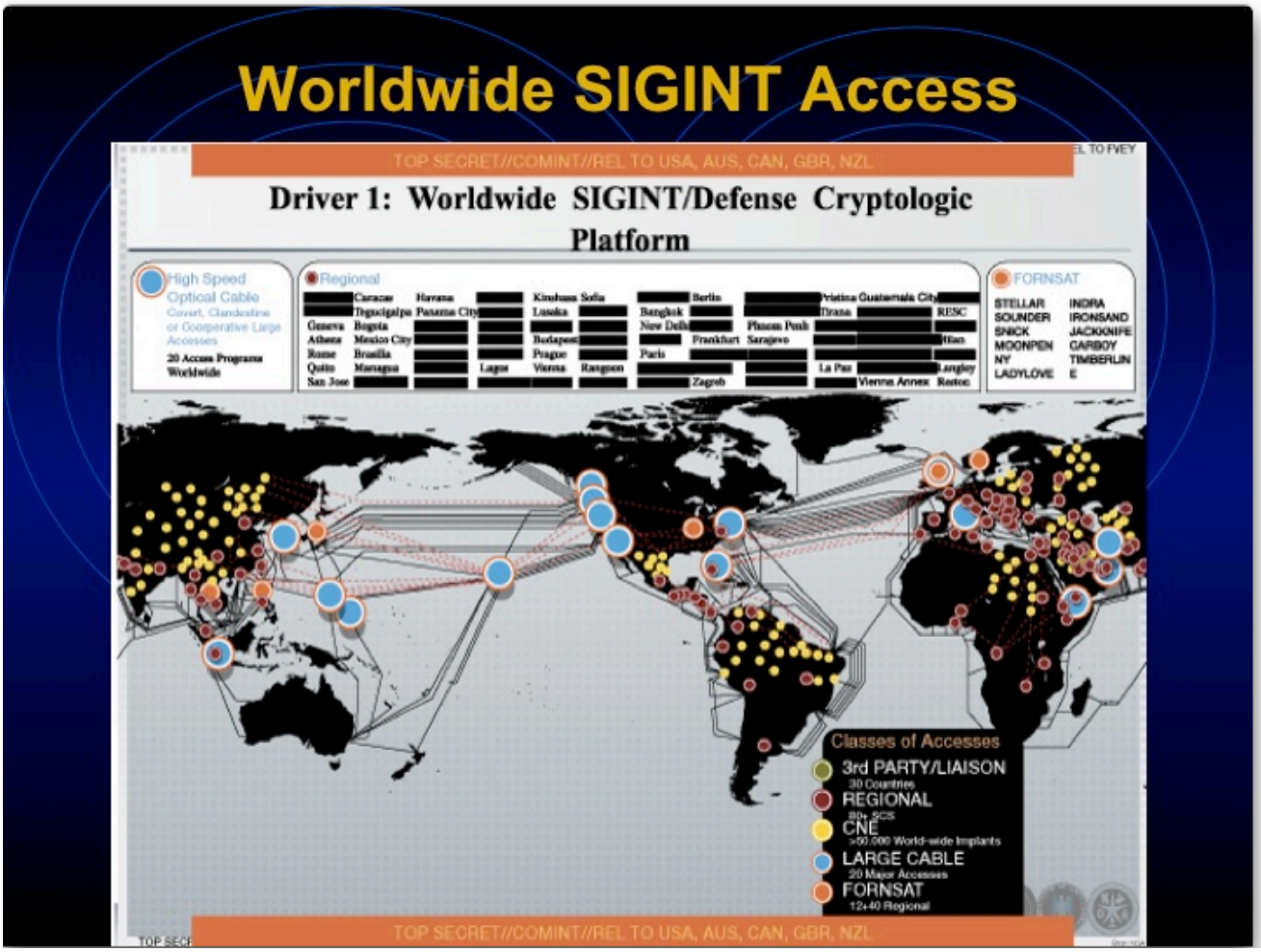
Question: Well, why would the MLAT--?

William Binney: Well, they participate in the parallel reconstruction. So, in other words, when you can't use the data, you have to go out and do a parallel construction, means you use what you would normally consider to be investigative techniques, go find the data. You have a little hint, though. NSA is telling you where the data is, it makes you look really good. If you have it quickly. So then you can justify, taking it into court and use that in court. And so I call that perjury.

In fact, I call this a 'Planned Program Perjury Policy' run by the Department of Justice of the United States. And, it's not just affecting our democracy, it's subverting our entire court system. It's not only subverting ours, it's subverting everybody's in the world that has a relationship with the FBI or the DEA. So this is infecting entire democracies, all of the world.

I think I have another slide.

(*Snowden Document in Binney Slide Presentation*)



Yeah, this is the one that shows, if you look down here in the corner, it says CNE, Computer Network Exploitation. It says greater than 50,000 implants worldwide. That means NSA owns the network. Not counting all the satellite or other kinds of communication access points.

Question: Note that there are no CNE points and FVEY on that chart.

William Binney: I mean, and if you go back to FAIRVEW, you know damn well that's not true.

Question: Well, on that chart.

William Binney: Yeah, that's right.

Question: Under this program.

William Binney: This is another engineer doing this. I mean, they're not telling you the total truth,

here, okay? Notice all the FVEY's. Yeah, right, that's right. And we know that's not true.

Question: I have one quick question. I've heard word that there's a set of internal morale programs inside NSA, which are done to look at human trafficking for non-intelligence reasons, which actually end up being NSA tools rolling up sex workers, domestically.

William Binney: I can't talk to that. I just don't know anything about it. I know we have a morale problem in the NSA.

(Laughing.)

William Binney: In fact, they've started-- they've instituted a Stasi type system. Where workers in NSA are to look at and watch, "See something, say something" on other employees. So this is Stasi. Well, I refer to N-S-A as the 'New Stasi Agency'. Actually, I also reference Wolfgang Schmidt, who used to be a lieutenant colonel in the East German Stasi, he commented on the NSA's surveillance program. He said, "For us, this would have been a dream come true." And the reason they're saying it-- I mean, this is straight out of the KGB, like Gestapo, SS, Stasi playbook.

Question: So the Russians have the same program?

William Binney: No, we do much better than they did.

Question: I am sure the Chinese have the backdoors in the technology that they provide. I mean, they've built all our phones. They've built all our hardware.

William Binney: Yeah, we have the hometown advantage, too, because, 80 percent of the fiber optic capacity runs through or in the United States.

Question: Sure, but I mean we buy laptops with batteries and the hardware and the batteries can subvert the laptops?

William Binney: Yeah. I'm sure they're all trying to do the best they can. It's within their resources. NSA has like $10B a year.

Question: On the plus side, it's AT&T that has raised their capacity, too.

William Binney: Yeah. I mean, if they adopt the same philosophy. Right, exactly. At any rate, I think that's it. I don't think there's another slide.

Corrections: *An earlier version incorrectly referred to TRAILBLAZER as the program, which used the back-end of THINTHREAD to spy on American citizens (and the world). The program is STELLARWIND. TRAILBLAZER, which cost $1.2 billion dollar and never launched, was abandoned in 2006.*

Alexa O'Brien researches and writes about national security. Her work has been published in VICE News, The Cairo Review of Global Affairs, Guardian UK, Salon, The Daily Beast, and featured on the BBC, PBS Frontline, On The Media, Democracy Now!, and Public Radio International. In 2013, she was shortlisted for the Martha Gellhorn Prize for Journalism in the UK and listed in The Verge 50..

Search

About

Alexa O'Brien researches and writes about national security and law enforcement. Her work has been published in The New York Times, VICE News, The Cairo Review of Global Affairs, Guardian (UK), The Daily Beast, NY Daily News, and featured on the BBC, PBS Frontline, NPR On The Media, NPR On Point, Democracy Now!, and Public Radio International. She was shortlisted for the 2013 Martha Gellhorn Prize for Journalism in the United Kingdom and listed in The Verge 50. In 2016, she worked at The Constitution Project in Washington, D.C. on a death penalty related project that is due for publication in Spring 2017.

Contact: email at alexaobrien dot com

Find me elsewhere

About

Alexa O'Brien researches and writes about national security and law enforcement. Her work has been published in The New York Times, VICE News, The Cairo Review of Global Affairs, Guardian (UK), The Daily Beast, NY Daily News, and featured on the BBC, PBS Frontline, NPR On The Media, NPR On Point, Democracy Now!, and Public Radio International. She was shortlisted for the 2013 Martha Gellhorn Prize for Journalism in the United Kingdom and listed in The Verge 50. In 2016, she worked at The Constitution Project in Washington, D.C. on a death penalty related project that is due for publication in Spring 2017.

Contact: email at alexaobrien dot com

Recent Tweets

RT @FT: Former Trump aide advises Chinese tycoon on building contracts https://t.co/dbNr7kc8uF

6 hours

This song is so beautiful and moving. https://t.co/1xEjWLmbHh

6 hours

Follow us on Twitter

Recent Posts

Daily Beast: Chelsea Manning's Liberation, and Ours

The New York Times Opinion Pages: Ask Alexa? No, Hear This Alexa

A case for Executive mercy for Chelsea Manning

Chelsea Manning Charged Documents

Doctors of Doom: What a PhD Really Means in the US National Security Community: A VICE News Investigation

Search