

LINCOLN MEMORIAL UNIVERSITY LAW REVIEW

VOLUME 3 FALL 2015

THE NSA'S EAVESDROPPING OPERATIONS AFTER THE SNOWDEN REVELATIONS: HOW MUCH IS TOO MUCH?

JANUARY 2015 SYMPOSIUM TRANSCRIPT

James Bamford

MR. JACOB BAGGETT:

I have the pleasure of introducing Mr. James Bamford as our first speaker. Mr. Bamford is an award-winning journalist in the field of national security. The New York Times calls him the nation's premier journalist on the subject of the NSA. And his most recent book, "The Shadow Factory", which is on sale outside by Union Avenue Books, was named by the Washington Post as one of the best books of the year. And he's here to discuss the transformation of the NSA since September 11th. Please welcome Mr. Bamford. (Applause)

MR. JAMES BAMFORD:

Thanks very much. It's really great being here. I want to thank Matt Lyon and Melanie Reid, Jacob Baggett, and Lauren Mullins for taking really great care of me. It's really great being here. The fact that this university is named after

President Lincoln is really quite an honor for me because I've always admired one of the things he's said. And that is the quote he has up here. I think if he had been President about a dozen years ago, we might not have gotten into the war in Iraq. If you read his quote there, "[k]ings had always been involving and impoverishing their people in wars, pretending generally, if not always, that the good of the people was the object."¹ He was very much against attacking countries without getting congressional approval. That was before he even became President. So, being at Lincoln Memorial University is a really big honor.

Also, there was a person that said these things here², which I thought were really important. I don't know if you might be able to guess who that person was. But the person was very much against the kind of surveillance that NSA has been involved in. It's actually the namesake of the law school here. I really admire Congressman [John J.] Duncan [Jr.]. I've followed his career largely because he was one of the few Republicans who decided to vote against the war in Iraq. That was a very courageous act at the time. There were only a few Republicans who did that. So, it's another reason to be honored to be here at this law school. It's a really great honor to be in a place where if somebody like John F. Kennedy were still alive, he would have probably written a "Profile in Courage" on.

* * * *

The reason I'm here is to talk about Edward Snowden. I spent three days with Edward Snowden last summer in Moscow. It's the most time, I think, that anybody has spent with him up until this time. I hung out with him for three days, tried to get to know him a little bit, and I did a cover

¹ Letter from Abraham Lincoln, Illinois Congressman 7th District, to William H. Herndon, Lawyer (Feb. 15, 1948) (published in *Collected Works of Abraham Lincoln* Vol. 1).

² Video: *The Snowden Effect: The Impact of Spilling National Secrets*, held by the Lincoln Memorial University: Duncan School of Law (Jan. 23, 2015, 00:04:28) [hereinafter *Symposium Video Archive*] (on file with author and editors) (Mr. Bamford displays a quote from Congressman Duncan).

story for "WIRED."³ He is also a person I really admire because he had a tremendous amount of courage to do what he did.

I have been following the NSA for many, many years, since basically 1982, when my first book came out. In that book, I warned what would happen if the NSA is let out of the cage . . . if it's allowed to do pretty much whatever it wants to do without very much control. That's what happened here in the post-9/11 period when NSA really began turning its ears on the American citizens without any real legal authority. Snowden was one of the very few people who decided to stand up and tell the public what's going on.

One of the things that I thought was really interesting when I was talking to Snowden was finding out that we had a few things in common. I was actually in the Navy for three years during Vietnam. One of the places I got assigned was an NSA facility in Hawaii,⁴ which is the same kind of place that Ed Snowden was at. And then when I was in the Navy --Well, basically, when I was in law school after the Navy, I got sent to the Navy Reserves. In the Navy Reserves, I got put into another listening post for two weeks.

It was in Puerto Rico. What they were doing was eavesdropping on South America, which was fine. But then all the sudden, when I was putting the earphones on, they were listening to Americans also, which I thought was very odd since I was in law school and we were learning that you need warrants to eavesdrop on Americans.

The project was called "Project Minaret".⁵ It was designed to eavesdrop on people like Jane Fonda, these real dangerous characters back in the 1960's, '70's, and so forth. Another real danger was Dr. Benjamin Spock--you can see he's got his deadly weapon there--the baby doctor, Muhammed Ali, and Martin Luther King.⁶ So, these were the targets during in the 1960's. The NSA was eavesdropping on these people. I was in law school and I thought that was very odd that the

³ James Bamford, *Edward Snowden: The Untold Story*, WIRED, Jun. 13, 2013, <http://www.wired.com/2014/08/edward-snowden/>.

⁴ Mr. Bamford displays a photo of the facility in Hawaii. *Symposium Video Archive*, *supra* note 2 at 00:06:46.

⁵ Mr. Bamford displays a slide featuring Jane Fonda. *Id.* at 00:07:54.

⁶ Mr. Bamford features a slide with pictures Fonda, Speck, Ali and King, Jr. *Id.* at 00:08:09.

government should do this without any kind of warrant.

NSA had a program in the 1960's called "Operation Minaret". The whole idea of it was not targeting foreign enemies, it was targeting domestic war protestors. These are some of the war protestors who were targeted.⁷ I found out about it when I was in Puerto Rico because they were actually eavesdropping on Americans down there, which was surprising to me because I was in law school at the time, like the law school here, and I had criminal law. I was actually working as a student prosecutor and we talked about getting warrants, eavesdropping warrants, search warrants, those kinds of things and all the procedures you had to go through to do that. It was very odd being down there having earphones on listening to Americans talk.

So, at the same time that was going on, there was a committee in Congress that was holding hearings on the NSA and the intelligence community. It was called the Church Committee. Senator Frank Church was the head of the Committee. He was investigating abuses by the intelligence community.

It was a very highly publicized investigation back in those days.⁸ I decided that it might be very appropriate if I give them a call and let them know what was going on in Puerto Rico. I thought it might be a little dangerous for my legal career if I started off being a whistleblower. But, still, I thought that the fact that they were doing that eavesdropping was something that at least the Committee should know about.

It turns out when I told Frank Church the fact that the operation was still going on, he got very upset because the NSA had told them that they had stopped that about a year and a half earlier and, lo and behold, it's still going on. So, he sent numerous staffers down to Puerto Rico and found out, yeah, they're still doing it.

That's the problem. The problem is that they were doing enormous amounts of spying domestically. They gave a list of the people they were eavesdropping on, as I mentioned, Jane Fonda and so forth, these really horrible, dangerous

⁷ *Id.*

⁸ Mr. Bamford displays a slide with a picture of Senator Frank Church. *Id.* at 00:10:02.

characters. There were a couple of names that they wouldn't give out, that they refused to give out in terms of who they were eavesdropping on. They just released a couple of those names just last year after all these years. And that goes back to 1975 when this was going on. So, again, they finally released a couple of the names that they had withheld all those years ago that they were listening to. One of those people was Senator Frank Church, which, you know, was a very good reason why they didn't want to admit it at the time. So, when I was doing this research for my book, one of the things I did come across was a document. It was called the [Report on Inquiry into CIA-Related Electronic Surveillance Activities] -- you can read the title there.⁹ It was basically a report on potential criminality by both the NSA and the CIA.

What few people actually knew about back in those days was that in 1975, NSA became a target of the Justice Department, the Criminal Division of the Justice Department. They actually launched a criminal investigation of NSA. It was almost unheard of. As far as I know, it is unheard of that you have an actual entire agency looked on as a potential criminal entity as with a RICO investigation or looking at it as the mafia or whatever. But that's what they did.

They conducted a criminal investigation for more than a year of NSA. They actually read the Miranda Rights to senior officials at NSA. When they finally finished the investigation, they came up with about twenty or twenty-one different areas that they could possibly prosecute. Some of those were eliminated because of the statute of limitations, but other ones were still potentially prosecutable.

That's what this document was -- a prosecutor's summary.¹⁰ I got it from the Justice Department. The Attorney General released it to me under the Freedom of Information Act. And then NSA demanded it back after I got it from the Justice Department. And they reclassified it as top secret. When it was released to me, they had redacted information. It had been declassified under the Carter Administration.

When the Reagan Administration came in, the NSA demanded I give the document back and they said they had

⁹ Mr. Bamford refers to document entitled "Report on Inquiry Into CIA-Related Electronic Surveillance Activities". *Id.* at 00:11:35.

¹⁰ *Id.*

reclassified it as top secret. I refused to give the document back. I said, "The Carter Administration released it to me, declassified it and released it to me, legally under the Freedom of Information Act." But they still threatened me with prosecution. They threatened me twice with prosecution under the espionage statute basically for not giving back a document that the Justice Department, actually the Attorney General, had released to me.

So, it got very nasty for a while. But NSA didn't want their criminal file out. The Justice Department decided not to prosecute in the end because it would have released too many secrets in the courtroom. You can't have all these NSA people testifying about this illegal activity without revealing a lot of secrets. So, the Justice Department buried it. They just put the report in a drawer and hid it. And, so, nobody knew about it. I heard a rumor that they had that. And that's how I got it under the Freedom of Information Act.

So, there is precedent here. When there is an investigation of an agency like NSA, there is the potential for a criminal prosecution. Well, that was very interesting to me, the fact that NSA, an agency like that, could lie, which is one of the things I discovered as I mentioned in Puerto Rico. And another thing -- that they could be involved in criminal activity, and be investigated by the Justice Department.

So, I decided to write a book about NSA. When I graduated from law school, I didn't have my heart in practicing law. I decided to be a writer. And one of the things that I thought really needed to be written about was NSA. Nobody had ever written a book about NSA before. Hardly anybody even knew what NSA was. There were a lot of unhappy faces at the NSA. I took some pictures of a few people at NSA.¹¹ A lot of people were a little angry about the book. I went ahead and used the material.

The Justice Department didn't prosecute me since I didn't violate the law. There is an Executive Order on secrecy that says once a document has been declassified, it can't be reclassified. It then went up to the White House and President Reagan. But, President Reagan changed the Executive Order to say once a document has been declassified, it can be

¹¹ Mr. Bamford displays a humorous slide containing multiple faces with demonstrative characteristics. *Id.* at 00:15:13.

reclassified as top secret. I love this little Latin phrase that you probably all know – “*ex post facto*.” In other words, they can't prosecute you for something that was done before the law was changed. So, I'm very happy about that.

Now, to get back into NSA a bit, this is where it started basically.¹² And again, it's very appropriate being here. It started under Lincoln, except Lincoln only did it during wartime, which is the appropriate time to do it. There's no evidence that he ever did any kind of eavesdropping during the non-war period during his administration.

We go to this little townhouse in New York.¹³ I just went by it a few months ago. It's still there. This is actually the beginning of the NSA. The NSA began in 1920 basically under a different name. It was called “The Black Chamber” back then. It was the first civilian code breaking agency in the United States Government and it occupied that little townhouse in New York. The first floor was a phony company in case anybody walked in the door. It was a phony code breaking company. They did the code-breaking work on the next two floors. On the top floor was Herbert Yardley. He was the chief of the Black Chamber. He ran it all during the 1920's. Yardley had no idea what the end result of his little Black Chamber was going to turn out to be.

This is the NSA today.¹⁴ It's virtually an entire city. You've got thirty-two miles of roads in there. It's continuing to expand now that they have Cyber Command and so forth. So, unfortunately for the people on Fort Meade where this is located, they just did away with the Fort Meade Golf Course because NSA is expanding even greater now. It's becoming the Cyber Command, jointly with the Cyber Command. Here is its headquarters.¹⁵ You can put the U.S. Capitol building in there four times over. So, it's an enormous agency.

I managed to get a camera in there to take some

¹² Mr. Bamford displays a photo of Union Army telegraphers at Gettysburg. *Id.* at 00:16:06.

¹³ Mr. Bamford displays a photo of the New York townhouse and Herbert Yardley. *Id.* at 00:16:34.

¹⁴ Mr. Bamford displays a photo of NSA's facility in operation at the time of his presentation. *Id.* at 00:11:35.

¹⁵ Mr. Bamford displays a closer view of NSA's primary complex. *Id.* at 00:18:11.

pictures of some of the people at work so you can see what it looks like in there.¹⁶ You can see that Barack and George got their start there.¹⁷ I actually did get tours of the agency. They wouldn't let me take my camera in there. But for my books, they did give me a tour. Actually having a legal background was fairly useful because I did have a number of legal battles with NSA. Part of the settlement for one of my legal battles was that I got tours of the agency, interviews with officials, and the entire internal structure of the agency. That goes back to my first book, "The Puzzle Palace." It's an enormous agency.

* * * *

This is a document that came from Edward Snowden.¹⁸ It was one of the top secret NSA documents. It shows the budget. The budget had been classified for years. It's an enormous budget. The intelligence budget at the time this thing was -- I think it was 2002 or whatever when this document came out -- \$52 billion. NSA had \$10.8 billion.

The CIA budget used to be smaller than the NSA budget. But with all the drones it keeps buying, it's gotten up to \$14 billion now. And then this happened. This is a house in Yemen.¹⁹ It's outside of Sana'a, the capitol of Yemen. I was there. I'm one of the very few people I think that's in this country that's ever been there. I was doing a documentary for PBS on Osama bin Laden, NSA, the 9/11 attacks and so forth. One of the jobs was to actually find bin Laden's operational center in Yemen.

* * * *

¹⁶ Mr. Bamford displays multiple humorous pictures not actually of NSA employees. *Id.* at 00:18:25.

¹⁷ Mr. Bamford refers to specific pictures of Presidents Barack Obama and George W. Bush. *Id.*

¹⁸ Mr. Bamford refers to a document entitled "Consolidated Cryptologic Program," displaying a pie graph of the total intelligence budget. *Id.* at 00:19:11.

¹⁹ Mr. Bamford refers to a slide photo of three-story dilapidated home. *Id.* at 00:19:52.

This is where it all happened.²⁰ This was [bin Laden's] major communications hub in Yemen. We managed to find a driver who would take us there because we had to do some shooting of the place. And then the driver got sort of freaked out and he never wanted to come back there again. So, it was a very dangerous place to go.

This is how bin Laden communicated. He had this kind of a satellite phone up in Afghanistan.²¹ He would communicate to that house. The house functioned as an operational center. So, this is where the plans were made for the attacks on the U.S.S. Cole, the attacks on the U.S. Embassies in East Africa, and 9/11. So, that's his phone number if anybody wants to call him.²² He's probably tied up right now, but that was the number that NSA eavesdropped on. That was bin Laden's satellite phone.

NSA listened to it for a number of years. They had listened to it basically since the time he got his satellite phone. And in December of 1999, that's when the NSA picked up the first indication that 9/11 was coming. I mean, obviously, they didn't know 9/11 was coming, but they picked up an indication that this guy here, Khalid al-Mihdhar²³ and another person called Nawaf al-Hazmi, were being sent to Kuala Lumpur. That was the first step of this whole operation.

So, this is where it all began. This is the house that functioned as his communications command post. NSA had been listening to it for a long time. So, they picked up these phone calls.

One of the interesting things is the CIA wanted a lot of that information. The CIA wanted to get the information that the NSA was picking up. Obviously it would be useful. The NSA would give summaries. But the CIA was asking for the key information and the actual transcripts.²⁴ I interviewed Mike Scheuer for the PBS documentary. He was adamant that three times, he went to NSA trying to get that information that

²⁰ *Id.*

²¹ Mr. Bamford refers to a photo of a satellite phone appearing in addition to the home on the previous slide. *Id.* at 00:20:50.

²² *Id.*

²³ Mr. Bamford refers to a photo of al-Midhar. *Id.* at 00:21:49.

²⁴ Mr. Bamford displays a slide quoting Mike Sheuer's desire for information. *Id.* at 00:22:39.

was coming into that house. The NSA refused to give it to them. They refused to give that information to the CIA.

The CIA actually had to build their own listening post. They built a satellite dish basically to capture the downlink from the satellite. The problem is you're only getting half that conversation when you just have the downlink. You're not getting the uplink. So, they went back to NSA and they said, "can you give us the other half? You know, we're only getting half the conversation." And again NSA refused.

These are some of the problems that led to 9/11. One of the things that fascinated me when I did this documentary for PBS --and I also wrote about it in my book, "The Shadow Factory" - was a document I got from the FBI. They had declassified it and gave it to me. It gave almost a minute-by-minute account of where the hijackers were going and what they were doing and where they stopped.

So, I was able to actually follow them all the way from Yemen to Kuala Lumpur and then Kuala Lumpur to California. Then they went to San Diego. Then they crossed the country. When they crossed the country, they were --This is the crew --the crew that was in California were the ones that were going to blow up the Pentagon.

So, what was interesting, when they were in San Diego, they were communicating back and forth to the house in Yemen. Now, this is a house that NSA is listening to. And they're using these phones in San Diego and they're calling the house in Yemen. So, the question is --and it's a question that's never really been answered adequately --is because there are such things as caller I.D.s and NSA was actually eavesdropping on those calls --that's what the 9/11 Commission said --why didn't NSA notify anybody that there were these guys who were sent by bin Laden, they're in San Diego right now because that's the area code, and they're calling bin Laden's house in Yemen, his operational center in Yemen? So, that's another really interesting question that's never really been answered adequately--why didn't NSA pick up on that?

These guys started heading across the country. They drove this car.²⁵ Believe it or not, they stopped at the Grand

²⁵ Mr. Bamford displays a photo the 9/11 hijackers car. *Id.* at 00:24:39.

Canyon and took a tour and so forth. Then they got to the East Coast. And, again, they were focused on blowing up the Pentagon. They didn't want to get a place right near the Pentagon because that would be too obvious. So, they tried to find a place that was a little ways away from the Pentagon. They decided to go to this motel, the Valencia Motel.²⁶ It was in a place called Laurel, Maryland. So, that was basically their headquarters for six weeks or so before the attack.

You know, it's an interesting place, Laurel, Maryland, because one of the other things in Laurel, Maryland is the National Security Agency.²⁷ Actually, it's only two miles away. So, for about six weeks, that's where the hijackers were living. I've been up in the director's office at NSA . . . believe it or not. I have had a love/hate relationship with NSA. They love me sometimes; they hate me sometimes. They hated me in the first book. They tried to put me in the jail under the espionage statute. But on the second book, they actually held a book signing for me at NSA. I was invited to the director's house for dinner and so forth. That's when I was up in the director's office. You can look out his window and almost see that motel. It's not really very far away. So, that's the irony here. You have the world's biggest intelligence agency, most expensive intelligence agency, the most intrusive intelligence agency that was just two miles away from where the hijackers were planning their attack.

* * * *

After 9/11, President Bush decided that he couldn't trust what's known as the Foreign Intelligence Surveillance Court, even though they've never had a leak. And, so, he decided to violate the law and go around it. Anybody here who knows how to read laws can go back and read the Foreign Intelligence Surveillance Act. It's a criminal statute. This isn't something you get sued over. This isn't some regulatory body. This is a criminal statute. It's five years imprisonment if you violate it.

²⁶ Mr. Bamford displays a photo of the Valencia Motel alongside photos of the 9/11 hijackers. *Id.* at 00:25:31.

²⁷ Mr. Bamford adds to the previous slide a photo of NSA headquarters. *Id.* at 00:25:55.

The statute says if you want to eavesdrop on somebody in the United States, you go through this court. That's what it was, that's what it was set up for, the Foreign Intelligence Surveillance Court. The Bush Administration decided not to do that. They bypassed it and they began eavesdropping on U.S. citizens. The problem with that is once you start doing that and there's no regulatory body, there's no oversight between the time you're deciding to go around the oversight, then there's nobody watching you. You're basically watching yourself. And that's never good in a democracy. So, after that happened, the New York Times discovered it. And then they had a front page headline on the fact that NSA is doing warrantless eavesdropping.²⁸ And the ACLU decided to sue NSA.²⁹ I became a plaintiff in the suit. They asked me to be a plaintiff and I agreed to. Christopher Hitchens and I and two other people became plaintiffs in the suit.³⁰

It went to court in Detroit. That's where they brought the suit. And this is really the only decision that's ever come out on the warrantless eavesdropping . . . the only decision that's ever looked at the substance of the acts that took place as opposed to looking at whether somebody had standing for example. Those are the other issues that have really been the focus of most of these hearings. But this is really the only hearing where a judge actually decided on the legality of the warrantless eavesdropping.

Judge Anna Diggs Taylor was extremely articulate in her decision by stating how much of a violation of U.S. law that was. It's slowly been working its way up through the courts. It'll get up to a certain court and then it'll be thrown out for lack of standing. Standing means that we can't show exactly that we were being eavesdropped on because NSA doesn't tell you who they're eavesdropping on. It's sort of a

²⁸ James Risen & Eric Lightblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0

²⁹ See *ACLU v. NSA*, 438 F.Supp.2d 754 (E.D. Mich. 2006), *vacated*, 493 F.3d 644 (6th Cir. 2007).

³⁰ Mr. Bamford displays a slide including a photo of Judge Ann Diggs Taylor and a quote from her opinion; See *supra* note 27. *Symposium Video Archive supra* note 2 at 00:28:27.

catch-22. But it's slowly working its way up in the court system. So, that meant that NSA now all the sudden had this new mandate to go out and do eavesdropping all over, all over the country and enormous parts of the world.³¹

So, the whole idea was to collect it all. That was the idea of General Alexander to collect it all, to take that whole haystack and bring it into NSA and then look through it. And that's never been done before.

When NSA was set up, it was set up for a specific reason, to protect the United States from an attack by the Soviet Union because of the nuclear weapons and all that. So, they surrounded the Soviet Union with listening posts and they focused on military communications and diplomatic communications. It was very easy because they all had certain frequencies. The military communicated only on certain frequencies. So, you could target those frequencies. And that's what they NSA did.

After the Cold War, NSA didn't really have a mission. You know, the Cold War is over. Russia is no longer our arch enemy and all that. So, they were looking for a mission. And all the sudden, they latched on to counterterrorism. So, that's a much different target because the terrorists do not use specific channels, specific frequencies like the Russians or the Soviet Union did. They use everybody's communications. They use the internet, they use phone calls, cell phones, and all that. That's the problem. You have this whole haystack of all that communications and you've got to bring it in.

That was the name of the program, Stellar Wind.³² That was the name of the very secret program that was the principal eavesdropping program that NSA had. That's the program largely that Snowden released when he was releasing documents. One of the first documents he released had to do with the Stellar Wind program.

Now, the NSA --just to give you a little background here, NSA is not just the NSA. NSA is the largest intelligence agency on earth. But it's not just itself. It's what's known as the

³¹ Mr. Bamford displays a photo and quote from General Keith Alexander showing his approach to mass data collection. *Id.* at 00:29:52.

³² Mr. Bamford adds to the previous slide a haystack with the caption "Stellar Wind". *Id.* at 00:31:29.

“Five Eyes.” After World War II, the NSA got together with other intelligence agencies in the U.K. and Australia, New Zealand, and Canada, and they all decided to divide up the world in terms of spheres of influence or spheres of eavesdropping, actually.

The U.S. could eavesdrop on South America and Central America fairly well because of our geography. The British can eavesdrop on Europe very easily because of their geography. So, they formed this organization called the Five Eyes.³³ For example, when the U.S. wants to eavesdrop on Angela Merkel in Germany, they would give it to the GCHQ. That's the British equivalent of NSA. So, they divide up parts of the world on who's going to eavesdrop where and then they share all the information. So, it really multiplies the amount of eavesdropping that NSA can do.

This is how they do it. This is how they're building that haystack. These are communication satellites that are up in space twenty-two thousand three hundred miles.³⁴ They're in geo-stationary orbit and that's where the signals go up and they come down. So, these are phone calls, they're emails, or whatever. And what NSA does is they build these big listening posts around the world. So, in those domes are satellite antennas targeting a lot of the communication satellites in space.³⁵ And that's how they're picking up a lot of the communications. They have these facilities around the world. This one here on the bottom is Menwith Hill Station.³⁶ It's in a place called Harrogate, which is in England. So, that's one of the ways they did it.

They use these satellites like this in space. They are big antennas basically that pick up the signals. And they've got them around the world in a lot of different places. This is another top secret slide from Ed Snowden.³⁷ And it shows

³³ Mr. Bamford presents a chart showing the different organizations and countries involved in the mass data collection. *Id.* at 00:31:56.

³⁴ Mr. Bamford's slide contains photos of three communications satellites. *Id.* at 00:33:11.

³⁵ Mr. Bamford adds a picture of the system of satellites on the ground in Harrogate, England. *Id.* at 00:33:36.

³⁶ *Id.*

³⁷ Mr. Bamford displays a chart entitled “Primary Fornosat Collection Operations”. *Id.* at 00:34:19.

where around the world that NSA has all these, these listening posts, these satellite facilities. These facilities can pull in about two million pieces of communications an hour, an enormous amount of communications. You're talking about tremendous amounts of email and phone calls and so forth.

In addition to the satellite, they're picking up microwaves.³⁸ I looked out the window today [in Knoxville] and I could see all these microwave antennas on top of buildings. So, you see them all over the place. And those are telephone calls going in and out. They're city to city, inner city telephone calls, email. That's communications going in and out.

Well, NSA needed to get ahold of all that communication. So, this is how they did it.³⁹ Those are microwaves. Microwaves travel in a straight line like a pencil. And the earth is curved. So, because the earth is curved and those signals travel in a straight line, they eventually go off into deep space. So, if you want to eavesdrop on those signals, what you do is you put a satellite out there in geo-stationary orbit and that picks up those communications. They eavesdrop on the signals and they can relay them back to NSA. So, instead of just focusing on the communications going through the air, NSA began focusing also on the signals going through the undersea cables, fiber optic cables.⁴⁰

In the 1990's, with the internet -- everybody's communicating on the internet nowadays. So, they needed to build far more communications capabilities. And it was far more efficient to do it by building undersea cables. The signals didn't have to go so far, it was more reliable, and so forth. So, they began looking for ways to tap into all these cables. And this is another top secret slide from Snowden.⁴¹ It shows you how much information you get from these cables. One cable

³⁸ Mr. Bamford displays three photos of satellite towers. *Id.* at 00:34:31.

³⁹ Mr. Bamford displays an infographic demonstrating how microwaves travel. *Id.* at 00:35:12.

⁴⁰ Mr. Bamford posts a depiction of the current and future fiber optic network. *Id.* at 00:35:43.

⁴¹ Mr. Bamford displays a partially redacted slide providing the specifications of fiber optic cable and the various types of information that the agency can gather through using this method. *Id.* at 00:38:15.

can have a hundred million simultaneous telephone or internet communications. One hundred million. So, you tap into this and you really get a lot of information.

The nice thing for the United States is that if you look at a map of these undersea cables, so much of that goes through the United States. I was in Brazil. And the people down there were kind of curious as to how much privacy they had. If you look at an undersea map of the undersea cables, all but one cable --I think there are maybe a dozen undersea cables that link Brazil and much of South America to the world --all but one go up through Miami. So, the NSA has great access to all that information from countries around the world.

When the signals come in to the United States, they come in under the sea and then under the ground, and then they go up to a building like this. This is in San Francisco.⁴² It's called a switch, AT&T's switch, a ten-story virtually windowless building where all the communications are switched from all over the world and all the communications coming in to the United States. There are a number of these around the country in different corners of the country that take these communications.

Well, NSA needed access to that. So, they built a secret room. This is the secret room in this facility here.⁴³ It was an AT&T whistleblower who took a picture of that and leaked the information that NSA was tapping into all its communications. They were getting all these communications that would come in. It would be filtered through this room. And the room would be filled with NSA equipment that would look for particular names, James Bamford or whatever --I'm probably still on the watch list --anybody's name, anybody's email address, a particular word or a phrase that they're looking for.

Some cables the NSA still couldn't get by tapping either through the United States or through a friendly country. They may go from one part of a foreign country to another. So, the only way to tap into some of these cables was by building a submarine, sending a submarine down. So, they took the

⁴² Mr. Bamford refers to a photo of an office building. *Id.* at 00:37:37.

⁴³ Mr. Bamford adds a photo to the previous slide showing a door going into the secret room. *Id.* at 00:37:51.

U.S.S. Jimmy Carter, they cut it in half, and they put a big NSA facility in the middle of it.⁴⁴ I'm not sure Jimmy Carter would have approved, but they decided to use his submarine for the NSA's eavesdropping.

They also have undersea bugs. This is a picture of an undersea bug.⁴⁵ The NSA put this cable actually in the Sea of Okhotsk under Russia Sea. Unfortunately at NSA, there was a guy that sold secrets to the Russians. One of the secrets he sold was the fact that this bug was on their cables. So, the Russians went down and picked it up and now it's sitting in a museum in Moscow.

Now, internet communications. Everybody's on the internet. Everybody's on the internet all day practically. So, NSA had to start focusing on that. You've got to start pulling in all that. You've got all the phone calls. You get the emails. You've got to get internet; anybody connecting to Google, or doing a Google search. So, they have this program called PRISM.⁴⁶ That is what's known as the front door approach.

So, they go up to AT&T --or they go up to Microsoft or Yahoo or whoever. This is another top secret slide from Ed Snowden.⁴⁷ What it shows is all the companies that NSA had access to and the dates at which NSA got access to them. And, again, this is a front door approach. They go up there, knock on the door, and say, "give me everything you have on James Bamford," or, "give me everything you have in Germany," or, "give me everything," you know, wherever it is they want, "give it to me and don't say anything about it. Don't say a word about it." So, that was PRISM. And that was the front door approach.

You know, sometimes they didn't want to go in the front door. They wanted to go in the back door so they didn't have to tell these companies what they were looking for. So

⁴⁴ Mr. Bamford displays a photo of the U.S.S. Jimmy Carter. *Id.* at 00:38:43.

⁴⁵ Mr. Bamford displays a photo of an undersea bug designed to tap into fiber optic systems. *Id.* at 00:39:14.

⁴⁶ Mr. Bamford display a chart showing the date when NSA began collecting information from commonly used websites. *Id.* at 00:40:06.

⁴⁷ *Id.*

another top secret slide from Snowden.⁴⁸ This is a handwritten note from somebody from NSA.

The whole idea is when you send a little Google search request from your computer to that --to Google, it's encrypted basically. It makes life a little difficult for NSA. That's why they have the PRISM program, so they can just ask the companies and they give it. Companies didn't encrypt the communications when they went between data centers where they were storing all this information. So, somebody at NSA had a really good idea of tapping into those cables or tapping into those systems. And, so, that was what was known as "Operation MUSCULAR." They got a back door. So, they had both a front door and a back door into these companies.

Then the metadata. You know, a couple of years ago, nobody had ever heard the word metadata. Now everybody knows what metadata is. Metadata is when you pick up your telephone. Anybody here, pick up a phone right now and press the button, NSA is going to get a record of that. They've been getting a record of it ever since 9/11. I don't know if anybody ever gave them permission for that. I never did. But they've been doing that. Everybody, whether you're five years old and happen to press it by accident or whether you're ninety-nine years old and you're calling your great, great, great grandson, all that is being recorded by NSA.

So, where are you going to store it all? I mean, you're talking about huge amounts of information that's being picked up. The NSA just built this new facility in Utah; Bluffdale, Utah.⁴⁹ And it's an enormous facility --I think it's the largest data center in the world, a million square feet --to store it all. And part of it is going to be like a hard drive. NSA will access it from wherever --from headquarters or from listening posts or from various places around the world. So, that's where it's all going. If you want to know where all those records are of who you called yesterday, that's where it is. It's in Bluffdale, Utah.

Now, this is actually hitting close to home here; Oak Ridge, Tennessee, at the National Lab. That's where they

⁴⁸ Mr. Bamford refers to a slide showing a hand-written note depicting NSA's data gathering. *Id.* at 00:40:52.

⁴⁹ Mr. Bamford displays a photo of the Bluffdale, Utah NSA facility. *Id.* at 00:42:39.

developed a lot of the nuclear weapons, the Manhattan Project during World War II. Now they've got a new Manhattan Project. It's developing the world's largest computer, the fastest computer.⁵⁰ It's an enormously fast computer. That's to search through all this. You get all this information, you have to store it someplace, and then you've got to go through it somehow. So, this is how you go through it --with a massive computer that can do one quintillion operations a second. I mean, in the time it takes to blink your eye, it can go through a quintillion emails, a billion, billion operations a second. They expect that, I think, in the next year it'll be finished.

* * * *

Now, just to give you an idea that we're really covering all bases here --the NSA doesn't want to let anything get away --they have this new thing where they're trying to figure out how they can get every single phone call in every single country.

They started out with this real hardcore terrorist threat. I guess it was the Bahamas. Yeah, the Bahamas there.⁵¹ So, they managed to record every single phone call in the Bahamas. So, I'm sure you feel very safe now. And they've done it with three other countries now. I think they're moving in that direction.

So, the question is, how much information do you need, how much is useful and how much is not useful? And that's really the issue here because when you do an analysis of what all this has gotten you, doing all this eavesdropping on everybody's communications, here's the misses⁵²: They missed the first World Trade Center attack. They missed the attack on the U.S.S. Cole. They missed the attacks on the embassies in East Africa. They missed 9/11. The Director was having a meeting in his office and he happened to look over at his TV

⁵⁰ Mr. Bamford alludes to a slide entitled "Analyzing the Haystack," which depicts two buildings representing the exaflop computer. *Id.* at 00:43:53.

⁵¹ Mr. Bamford refers to an aerial photo of the Bahamas. *Id.* at 00:43:53.

⁵² Mr. Bamford's slide list various notable terrorist attacks against the United States. *Id.* at 00:44:42.

set and saw the plane go into the World Trade Center. So, he found out about it not by his worldwide listening posts, the listening posts and the billions of dollars we're spending on equipment, he found out about it on a three hundred dollar TV set in his office. Missed the Underwear Bomber or the Christmas Day bomber flying into Detroit, missed the Boston Marathon bombing, and so forth --so on and so forth.

What are the successes?⁵³ After the Snowden leaks, the NSA came out very defensively and said, "oh, we have fifty-four times this has, you know, saved everybody." And it turns out, by the time they actually got in front of the Committee with sworn testimony and so forth, it turned out it was one instance when they were using all the metadata collection that it actually turned out being useful. I mean, if you want to call it useful. They found a taxi driver in San Diego that had sent \$8000 to some group in Somalia. That was it. For what? Since 2001 until now, that was the one success they could point to. So, you've got to wonder, why are we spending all this money doing all this, collecting all this information if we're missing everything, but we're collecting everything? And that's really one of the questions that has come out from the Snowden leaks. Why are we collecting all this? If we are collecting it all, why aren't we getting better results from it?

Well, now NSA is moving into a new phase here.⁵⁴ That's cyber warfare. There's this new organization that's coming now under the Director of NSA. The Director of NSA is the most powerful intelligence official in the history of the world. I mean, he runs the largest intelligence agency that's ever existed, the NSA, and the most intrusive one. Now he's got another hat on his head at the same time. He is running Cyber Command.

Very few people realize that we now have a Cyber Army, we have a Cyber Navy, and we have a Cyber Air Force. Now, all that is not really to defend the United States or defend Sony or defend your little laptop there. It's all offense.

⁵³ Mr. Bamford displays a quote from Representative Mike Rogers which touted the success of NSA, along with a quote from Senator Patrick Leahy refuting Representative Rogers' claim of success. *Id.* at 00:44:51.

⁵⁴ Mr. Bamford's slide displays four separate photos of NSA and the caption "NSA's Future". *Id.* at 00:47:00.

Well, it does have a defensive capability. It defends the government's own classified network. So, we've built up this enormously offensive capability, Cyber Command. And the key word in that is dominance.⁵⁵ The whole idea is to dominate the internet, dominate cyberspace in the same way that the Navy dominates the sea. This is their own advertisement here. We're going to dominate cyberspace like we dominate the sea or the Air Force is going to dominate cyberspace like we dominate air and space and so forth.

So, with all this dominance, you wonder why is Sony getting attacked? Why are we losing all this money that they're getting? But, again, the whole idea here is offensive, not defensive. And that's one of the things that Snowden made clear.

When I was in Moscow, I also interviewed Snowden for PBS. I'm doing a documentary on cyber warfare for PBS. I spent an hour with him and he went into a great amount of detail. That's actually on the web.⁵⁶ You can look it up if you just do PBS, Snowden, Bamford, cyber, or whatever and you'll get it. It's very interesting, a twenty-five page transcript of the interview with him where people realize that was his last job working as a contractor for NSA as a cyber warrior. So, he's able to actually talk about it from a first person perspective. It was very interesting. And we're going to have that on PBS. We'll have that documentary on later this year.

In terms of attack, that's what NSA did in Iran. It was actually the world's first cyber-kinetic attack.⁵⁷ The first time any country anywhere has ever used cyber to actually destroy physical objects. And that's the future. Using cyber not just to wipe out a hard drive or to steal some money, but to actually destroy them. I mean, in our program, we'll be able to show how that's possible, take out an entire power plant or whatever.

⁵⁵ Mr. Bamford displays six separate government official publications including the word "dominance". *Id.* at 00:48:06.

⁵⁶ See James Bamford & Tim De Chant, *Exclusive: Edward Snowden on Cyber Warfare*, PBS (Jan. 8, 2015), <http://www.pbs.org/wgbh/nova/next/military/snowden-transcript/>.

⁵⁷ Mr. Bamford's slide contained global map and the term "Stuxnet". *Symposium Video Archive*, *supra* note 2 at 00:49:52.

The U.S. launched the very first attack. It was called "Stuxnet." That was an attack against the Iranian centrifuges that were used in their nuclear research program to separate isotopes and so forth. What's interesting was that the intelligence community told the President --both President Bush and President Obama, look, you don't have to worry about that, we'll be able to do this attack, nobody will know about it. Nobody will know. First of all, it will just go into this one plant in Natanz in Iran. It will wipe out these centrifuges. And it's not going to go anywhere else. So if it does happen to escape, nobody will ever notice it. And if somebody does notice it, they'll never be able to tell where it came from. It won't have a return address.

Well, guess what? None of those things were true. They launched the Stuxnet attack. And it did escape. It also affected about a hundred thousand other computers around the world. We actually interviewed them on PBS on the documentary. These people who are like digital anthropologists or they do these like dissecting a frog or whatever. They dissect an actual piece of code, an actual piece of cyber. And they can actually tell where it came from, who created it, and why they created it.

So, before long, everybody in the world knew that the United States launched this attack against Iran, the Stuxnet attack. It didn't do any good, really. I mean, it knocked out about eight hundred centrifuges. Iran just put eight hundred more centrifuges in there. But, what we did was launch the very first cyber kinetic attack, which opens it up for the world so everybody can say, well, the United States is doing it, we can do it, too. The problem was, Iran never had a cyber command before that. They had never even thought about attacking the United States through cyber.

After we attacked them and after it came out that we attacked them, then they launched an attack against one of our allies, an oil company in Saudi Arabia called Saudi Aramco. They wiped out thirty thousand computers. They wiped out completely the hard drives on thirty thousand computers. Then they turned their attention to New York and the banks in New York and they began denial of service attacks on the banks in New York. Again, none of this happened until we attacked them. So, this whole idea of being this aggressive nature where we're going out and doing these things, it comes

back and it's got this boomerang effect.

So, what is "Treasure Map."⁵⁸ Treasure Map is another top secret slide from Snowden. This is very interesting if you read this. The whole idea here is to map the entire internet, every device anywhere all the time, which means the little things sitting in your pockets right now. Your pockets. Not terrorists' pockets; everybody's pockets. Everybody connected to the internet, we've got to map them out because at some point, who knows, we might have to put malware in your little device. The whole idea is to map everything, get everything mapped that's going to the internet. And, again, these are all top secret things. Nobody even knew this. Nobody gave them permission. Maybe some little Senate Intelligence Committee that was half asleep when they asked permission or something. Most Americans I don't think had any idea that the NSA was involved in these things.

So, the next thing was to plant malware around the world. This is again another top secret slide.⁵⁹ The little yellow dot is what is known as CNE, Computer Network Exploitation. And Computer Network Exploitation is sending malware to systems around the world. Now, you think, okay, North Korea, why not? Of course. It would be irresponsible not to do it there. But the problem is, when you look at those dots, they're not just in North Korea or Russia or China; they're in Brazil, they're in a lot of Europe and friendly countries. That got those countries rather upset. I was in Brazil a number of times last year. And, you know, the President of Brazil, Dilma Rousseff, decided to cancel this formal dinner with the President over it. A lot of bad things happened because of this.

The NSA has been working on this for quite a while. What they're working on right now is another program called "Turbine."⁶⁰ The previous slide showed it was fifty thousand locations around the world that they were planning it. Turbine will move it up to about a million, covertly inject millions of


⁵⁸ Mr. Bamford displays a slide outlining "Treasure Map". *Id.* at 00:53:21.


⁵⁹ Mr. Bamford refers to a slide entitled "Driver 1: Worldwide SIGINT/Defense Cryptologic Platform." *Id.* at 00:54:21.

⁶⁰ Mr. Bamford's slide depicts the Turbine program on a global map. *Id.* at 00:55:28.

malware implants around the world.

So, this is the future. And, again, Snowden felt that it was important that the public should at least have an idea that this is being done at least in their name. There are dangers to all this when you're doing it. So, how are we being protected here, the American public from NSA?⁶¹ One of the ways is this very secret court. I mean, before Snowden -really before the '90's, for example, I would give talks. I would give talks to legal groups. I'd say, you know, there's a Federal system out there that none of you even know about. It's top secret. Even its location is secret. We didn't even know where it was. They just thought I was making it all up.

Well, it's true. It's called the FISA Court, Foreign Intelligence Surveillance Court. You're not allowed to know where it is, but I'll tell you. 

 Nobody that I know has ever been in there. It's a very restricted place. I was able to get a picture out of their session one time.⁶² There's the Judges and here is the session right there.⁶³ It's, it's the kind of court that if you're a prosecutor, you really love. They brought in thirty-three thousand nine hundred requests and they've only turned down eleven. The odds of being turned down are very slim. Then if you are turned down, though, there's another court that's even more secret.

It's called the Foreign Intelligence Court of Review, which is the appeals court. And it's sort of the Maytag repairman of the Federal judiciary. I think in thirty years, they've only had maybe one or two cases. And in both those cases, they did side with the government. But, again, if you lose in that court, you have a third bite of the apple if you're a prosecutor. You can go to the United States Supreme Court for an immediate *in camera* session, a secret session with the Supreme Court.

So, the odds of not getting a warrant are almost zilch. You also have the Senate and House Intelligence

⁶¹ Mr. Bamford displays the seal of the Foreign Intelligence Surveillance Court. *Id.* at 00:55:57

⁶² Mr. Bamford adds a picture of cartoon characters with hammers to the previous slide. *Id.* at 00:58:52.

⁶³ Mr. Bamford's slide contains a photo of a blind taste test panel with the participants wearing blindfolds. *Id.* at 00:58:54.

Committees.⁶⁴ They really are keeping track of everything. You can tell that they were very aware of the Bush Administration bypassing the Foreign Intelligence Surveillance Court, violating the FISA Act. I mean they're really on the ball there. I'm really confident that they're going to find anything that NSA does wrong.

You know, if I could resurrect Frank Church, I'd be very happy to put him back into the Senate. Unfortunately, that's not going to happen. So, what do we have to depend on then if we don't have those people to depend on? We have the intelligence community.⁶⁵ Well, there it is. James Clapper lied before Congress. General Alexander, he was asked these questions. This was all before Snowden when nobody knew anybody was going to actually rat on them. And totally lying. You know, "are you intercepting American cell phone conversations?" "No." I mean it's just breathtaking that you have this government and it actually lies to Congress. Actually, the intelligence committees knew what was going on. They were actually lying to the public because the people there with the clearances in the Congress, they knew. But the public didn't. So, these are basically lies to tell the public, not to the Congress.

So, here's the only resort, the whistleblowers.⁶⁶ Bill Binney was a whistleblower. He'd been there almost forty years. A very senior official. He was in charge of the automation of NSA around the world. He was a very brilliant mathematician. He cooperated with me on my "WIRED" articles, a cover story on Bluffdale, Utah.⁶⁷ He told me about all the domestic eavesdropping that NSA was doing. He had quit NSA after forty years of really honorable service. He found out that NSA was eavesdropping domestically and decided to leave NSA, do the honorable thing and just walk

⁶⁴ Mr. Bamford displays photos of various members of Congress appearing to be asleep. *Id.* at 00:58:04.

⁶⁵ Mr. Bamford displays photos of James Clapper and Keith Alexander taking an oath. *Id.* at 00:58:44.

⁶⁶ Mr. Bamford displays photos of five prominent whistleblowers. *Id.* at 00:59:38.

⁶⁷ See James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED, Mar. 15, 2012, http://www.wired.com/2012/03/ff_nsadatacenter/.

out. He told me about it and I put it in the magazine. That's why General Alexander was called in front of that Committee. And he denied it all. He just denied it all. And then when I was talking to Ed Snowden, he said that was one of the reasons he walked out with all of the documents because of what happened to Bill Binney and what happened when I wrote my article. He didn't want to have happen to him what happened to Bill Binney where he does the honorable thing and tells what illegal things are going on and then have the NSA just lie about it.

So, taking the documents, you couldn't do that. Then you had Kirk Wiebe. Tom Drake was charged with five counts of espionage because he leaked information to the Baltimore Sun. I was actually the legal consultant on that case. They brought me in on the defense. He had no more money left after NSA went after him for four years. So, he had a Federal Public Defender. The Public Defender's Office hired me. I was able to show the judge that all of that information they were charging him with espionage, all of it was in the public domain. It wasn't just in the public domain, but I showed that the government actually placed it in the public domain.

This has almost never happened. I don't think it has ever happened. The prosecution just dropped the case, threw it out on one condition --Drake sign an agreement saying he confessed to a misdemeanor, which was less than a parking ticket. There was no jail time and no fines. So, it went from five counts of espionage down to basically a parking ticket. The judge spent twenty minutes chewing out the NSA and the prosecutor and basically congratulating Drake for putting up with it for four years.

* * * *

Let me just wrap up here. What's the takeaway from all this? The NSA and the telecoms have been cooperating ever since Yardley, basically a hundred years. They occasionally get caught. Nobody ever gets punished. Nobody ever gets prosecuted. Then after they get caught, they just keep doing it again. So, what's the answer? The answer is to have a major Church-style investigation like they did in '75. That worked then. They found a lot of things. They did some corrective measures. They aren't doing that now. Another thing is to

have a major hearing where you're calling the telecom people and asking what is it that you're doing, tell us what NSA is forcing you to do.

That actually happened in the mid '70's. A woman --the Chair of the Congress, Bella Abzug, a Congresswoman from Brooklyn, she really was --If anybody ever looks back at Bella Abzug's career, it's really amazing. So, she called the telecom people and said, "I want you to testify." Well, President Ford for the first time in history, the first and only time, issued a Presidential Executive Order ordering the private companies not to testify. They were more afraid of Bella Abzug than they were of Jerry Ford. They actually did testify. So, there's precedent for that. As I mentioned before, they actually did have a criminal investigation of NSA. They came up with twenty, twenty-one different areas of prosecution. That's got precedent, too. Those are the answers.

The key thing here is to prosecute. You've got to prosecute people. It works sometimes. That's what the judicial system is about. They commit crimes. But they only prosecute the whistleblowers. They don't prosecute the people who are actually committing the crimes. So, you know, if they put General Alexander⁶⁸ or, this is sort of fantasy here, but put him in jail for lying to Congress or put government officials who actually commit crimes in jail, maybe that won't happen again.

There's a lot of reform that comes from going to jail. I've interviewed loads of people in prisons. Some people come out and they're really reformed. I think General Alexander would be reformed.⁶⁹ I think he would have a really change of heart when he came out. And I think that would be a good thing.

Eventually, you'll see Ed Snowden on the NSA Hall of Honor there.⁷⁰ He'd be right next to Herbert O. Yardley, who after he became the head of the first Black Chamber, he wrote a book about NSA and then they went after him. But seventy years later, he got put up on the Cryptologic Hall of Fame at

⁶⁸ *Symposium Video Archive*, *supra* note 2 at 01:04:39.

⁶⁹ Mr. Bamford's slide now shows General Alexander with an Edward Snowden t-shirt on. *Id.* at 01:04:59.

⁷⁰ Mr. Bamford displays a slide entitled "Cryptologic Hall of Fame," showing various public figures including Edward Snowden. *Id.* at 01:05:12.

NSA. So, in seventy years maybe we'll see Ed Snowden up there. Anyway, I really appreciate being here. It's a great school. And I wish you a lot of luck and thanks a lot.⁷¹

(Applause)

(End of presentation by Mr. Bamford.)

⁷¹ Mr. Bamford ends with a slide containing his contact information, including the email address WashWriter@gmail.com. *Id.* at 01:05:43.