

# Diane Roark

Diane Roark served as a top staff member on the House Intelligence Committee from 1985 to 2002. She fought to end the NSA's post-9/11 warrantless wiretapping initiative, telling FRONTLINE she considered the program "unethical, immoral, politically stupid, illegal and unconstitutional." Roark spoke to FRONTLINE's Jim Gilmore on Dec. 11, 2013.

Diane, let's start with a little bit of your bio. You worked at the House Intelligence Committee. Give me the years you were there and what were your responsibilities when you worked there.

I worked at the House Intelligence Committee for 17 years. For the last five of those years, I had the NSA account for the Republican majority.

What does that mean?

When you have an account, you follow it, both for operational effectiveness and for budget, and for those two, but also in NSA's case in particular, to make sure that everything they're doing is legal. ...

... Did they understand what the threat was before 9/11? ...

I took the NSA account in 1997. At that time, I felt that NSA was technologically adrift and that there was no sense of urgency to catch up to the digital age, which was coming on them like a freight train. ...

So it was a huge concern to me, and they did not seem to realize what a huge problem this was. In fact, right up to 9/11, they were denigrating the Internet as a source of intelligence, and even denied, right after 9/11, that the terrorists had been using the Internet, when it had already appeared in the front page of the *Washington Post* that they had.

[? Return to top](#)

Tell me a little about Gen. Hayden. ...

Not long after the House Intelligence Committee began raising an alarm about the state of NSA, Gen. Michael Hayden took over at NSA as the incoming director.

He did concede that there were some things that were wrong, although not necessarily what we were saying. And he appointed what was called an internal team at that time, made up of people inside NSA, to investigate what was going well and what was not going well at NSA.

I appealed to him at that time to also do an outside team, an external team, because I was fearful that the internal team might whitewash things. But as it turns out, both teams were quite critical, but the internal team was even more critical than the external team was and really ripped the place apart, to tell you the truth. It said things were, in essence, really bad.

And so Gen. Hayden agreed that something needed to be done, and that they needed modernization desperately. He eventually settled upon what became the Trailblazer program.

As soon as I was briefed on the Trailblazer program and then asked for a paper on it, the decision paper on it, and looked at the rationale for it, I immediately told him it wouldn't work.

... I don't know why, but they wanted to take the old analog systems and transition them to digital instead of starting over from scratch, and I told him it wouldn't work.

It sounds, number one, that you're very hands-on. You're involved, watching over programs; you're advising them; you're suggesting. Your reputation is what with the leadership of the NSA?

NSA regarded my oversight as far more intrusive than anything they were used to, and far more critical also than anything they were used to. I think they thought it was micromanagement. I did not regard it as micromanagement. I thought I was looking at the big-picture issues that were coming to hit them in the face, and at the frailties that they refused to acknowledge. ...

[? Return to top](#)

You oversaw the research of Bill Binney on ThinThread, along with [Ed] Loomis and [Kirk] Wiebe. ... What did you think of that program? Why the need for it? And how interested were you in the fact that that in fact might be an answer to some of the problems that the NSA had at that point?

I had heard about a number of sort of hidden programs at NSA that were promising, and I asked for briefings on them. ...

One of those programs was the SIGINT Automation Research Center [SARC], which is what Bill Binney and Ed Loomis headed. I got a briefing from them, and I thought it was pretty impressive and forward-looking, especially compared to the rest of what I had heard. I definitely thought that it deserved support. ...

... Explain what you saw in this program that was very positive. ...

The ThinThread program was very impressive because they managed to develop this technology and string together a lot of different systems that went all the way from after collection, immediately after collection, to the processing and all the way to the reporting. So it went through the whole chain of what was needed to take this data and analyze it and get it out of NSA.

And that was precisely what they didn't have. They were very weak in processing, very much limited the amount of data that they could

even handle.

Another big issue was the database. In effect, it was a revolutionary new database, also -- not only revolutionary processing, but revolutionary new database in which a huge amount of data could be stored and compared with each other, and it could be retrieved very rapidly. They were even planning automated reporting on some issues eventually, and even including automated FISA [Foreign Intelligence Surveillance Act] warrant requests eventually.

In addition, as part of the processing end, in that stage, it was managed so that all the potential domestic inner steps that were accidentally collected could be encrypted, triple-encrypted, so that nobody could ever see them until that warrant was acquired from the FISA Court, until there was probable cause that they were involved in a crime. It would be a foreign intelligence-related crime. So it was revolutionary from almost every point of view.

In addition to the encryption protection, there was also software for automated tracking of every access to this database, and that meant that there was a very high probability, if anybody looked at this data, they would be caught if they did something wrong. ...

But after 9/11, what happened was that NSA deliberately deactivated that software. So one of the things that I did immediately after I heard that they had turned the system on against domestic, the domestic people, U.S. citizens and U.S. persons, I found out that they had also deactivated those two protections, the automated tracking and the encryption.

So I focused all my efforts on, at minimum, getting the members, the Gang of Four members, so-called, the chairman and ranking member of both the House and Senate Intelligence Committees, to tell the administration in the White House at that time that they would not approve it, that they would kill it if they didn't restore those protections. That could have been done in a few minutes; all you do is reactivate the code.

That was my argument: I don't believe this should be happening, but if it is happening, you need to insist that the protections be put back on, or else you'll kill it.

[? Return to top](#)

---

... Overall, in the very simplistic terms, the idea on these programs was to do what, to analyze what kind of data for what kind of threats?

The ThinThread program was meant to analyze digital communications, and it was meant to analyze foreign threats, but also, if a foreign target, known dirty number or email address was in contact with a U.S. person, that that would be collected, but it would be encrypted until there was enough evidence that there was probable cause that the U.S. person was involved in illegitimate activity.

And the reason for that is going back to the Church Committee and everything else, in the DNA of folks at NSA was "We don't spy on Americans; we spy on foreign targets to protect America." Is that why? ...

It's correct that NSA always targeted foreign, but they also often picked up U.S. persons accidentally in doing so. And there was a procedure that was known as minimization. In other words, you protect their identity, again, until there was evidence that there was some kind of crime going on involving foreign intelligence, terrorism or whatever. So that was always the case, and there were always laws that allowed you to do that. ...

Only part of ThinThread was used. The part that was used was greatly changed. In fact, it was not changed for the better; it was changed for the worse. It was made into a sort of a database structurally that NSA felt more comfortable with. The operational rules were changed in a way that clogged up the data systems with irrelevant data. This is part of the debate about the so-called three hops that they could go domestically, which just resulted in terrible -- it just wasn't efficient.

And terrible invasions of privacy.

Terrible invasions of privacy, but also a vast reduction in efficiency. NSA has argued that what they are doing is they have to find a needle in a haystack. Well, in effect that analogy has to be turned against them. What they were doing was making the haystack so darn big that they couldn't possibly find a needle.

The other thing that happened, that needs to be borne in mind, was there was a plan for the gradual automation of ThinThread in a way in which the system itself would be automated and bring up targets to the attention of the analysts. The analysts wouldn't have to know ahead of time what the most likely targets were so that they wouldn't be concentrating on just the old targets they knew. In other words, they were going to automate it in steps progressively after it was fielded to do that.

But after Bill and Ed left NSA, NSA was not able to automate it. They eventually went to Bill and asked for his help, and he refused to help them, knowing very well that it was being used for illegal and unconstitutional purposes. ...

[? Return to top](#)

---

What was the attitude of Bill Binney and others that worked on it when they saw what was going on? What were they hearing? What did they see? ...

... Bill Binney and Ed Loomis and Kirk Wiebe had all retired on Oct. 31 or a few days thereafter in 2002. 9/11 had occurred in September, and in the meantime, between 9/11 and their retirement, it became clear to them that there was a major operation going on.

There was a lot of equipment being delivered; it was in the halls. There was a lot of secretive meetings that they were clearly not invited to. So it was obvious to them that something was going on. But later they heard that there was a domestic dragnet, domestic surveillance in a dragnet way, collecting on everybody, and Bill came and told me.

Why did he come to tell you?

Well, he knew me because he had briefed me many times and because it was my job. I was responsible for oversight. ...

You were hearing from other people as well, I'm assuming.

After I talked to him, I heard from other people, too.

So start then with Bill. He comes to you, and he tells you what, and how surprised are you? And how does that motivate you to move forward?

Bill came to me at my house and told me that part of their system, their ThinThread system, was being used for collection of domestic communications in a dragnet fashion, collection on everybody. He had also spoken with somebody who had looked up his own name, his own information, telephone number, email, whatever, and had verified that they had all the information on him.

So we knew it was happening. I was aghast. I was absolutely aghast, because this constituted a complete reversal of NSA policy. In effect, before 9/11, NSA had argued -- well, there were two arguments at NSA. The first argument from the technical people was specious, and the Trailblazer people who were in competition with ThinThread, basically, said that yes, the technology was good as it was, in a small system, but it would not scale up to a worldwide system. They claimed that couldn't happen.

The lawyers were claiming something completely opposite. They were saying the system was so capable and could process so much more than NSA had ever been able to process that even though it was far more effective at screening out U.S. persons -- in fact, about three times, at least three times as effective, and near perfect -- they claimed that still too many U.S. persons would squeak through, and therefore they couldn't do it. And the NSA lawyers actually blocked its implementation. ...

[? Return to top](#)

---

This was before 9/11, of course.

This was before 9/11.

After 9/11, when they need the same system, they still deny it.

After 9/11, the legal theory reversed completely. Gen. Hayden told me that his three lawyers were on board, his three top lawyers. I questioned one of the attorneys who had carried the request down finally to the Department of Justice when Gen. Hayden made them to do so, to ask whether the system could be implemented. This was before 9/11.

At that point, even though the system was near perfect in screening out U.S. persons, the two lawyers recommended orally to the Department of Justice that they not approve the application.

This was part of the basis, then, after 9/11, when the White House asked Gen. Hayden what he could do, he said there were some things he could do, but he would need more legal authority. And the White House said, "Don't worry; you have it," because they were planning to draw on the commander-in-chief-during-wartime powers. ...

[? Return to top](#)

---

What's your view of Tom Drake?

... 9/11 was his first working day, and he was assigned, very soon, the duty of putting together testimony before Congress. In putting together this testimony, of course, he found a lot of the dirty linen. He found out they already had some communications that they didn't know about. He found out about the programs that were instituted, that were of questionable legality after 9/11. And he objected to them. Eventually also he confirmed what Bill had told me.

By communications, you mean Al Qaeda communications; he found Al Qaeda communications as he was going through these communiqués.

He found that, yes, that they had had communications between known Al Qaeda persons abroad, both, I think, in Malaysia and in Yemen, and that those had connected to the two hijackers in San Diego.

Gen. Hayden had several times stated that if we had only had this system before 9/11, we could have prevented 9/11. He said flatly, "We could have prevented 9/11." And Bill and Ed have said the same thing.

But what Gen. Hayden doesn't say is that his own lawyers blocked it and that they did have this system ready to go. And it would have found them. ...

Post-9/11, Tom becomes a supporter and someone who's pushing on the possible use of ThinThread. He's one of the big defenders of ThinThread?

Post-9/11, ThinThread had already been canceled. ... The team was broken apart, and the system was mostly canceled. The only one part of it was saved to be part of the post-9/11 system that also did dragnet surveillance on the U.S.

Tom was not supportive of that. He was not supportive of that at all, and he went internally and objected to a lot of people. When it was clear that nothing was going to happen to stop it, he then went to various persons in Congress. I did not find out about the congressional and other efforts until years later. But he did everything he could within the chain of command, and the chain of command outside, to try to stop it. ...

He came to you. Did he talk to you about things?

By that time -- well, Tom didn't say too much to me about exactly what was going on. But by this time he and Bill and Kirk [Wiebe] had connected with each other, so one time when I went to meet Bill and Kirk and Ed, Tom was there also.

I would never have done that; you protect your sources by not mixing them, you know? So for their own protection, I'd never talked about my sources with each other. So I was surprised when he came, and then it turned out they had exchanged information, and Tom didn't tell me much in addition to what Bill had told me, but he affirmed that this was going on.

... What were they feeling at that point?

They were appalled. They were appalled that this had been turned against the United States. In the immediate aftermath, of course, everybody was afraid that another attack was coming, and intelligence, having missed the first attack, was publishing anything that might have any possible relevance to another attack. Everybody was scared to death by all these warnings.

The members of Congress in particular were afraid that if they tried to exert any discipline on NSA, they would be held liable for another attack and that the intelligence agencies in general, if they didn't get everything they wanted, would say it was Congress' fault if there was another attack. So basically the committees, at least the House Intelligence Committee, decided for political reasons that it would give them anything they wanted.

[? Return to top](#)

---

When you were going to members and saying, "There's a problem here; let's talk about this," were you being rebuffed? What was the response to your problems with what was going on over at NSA?

When I heard from Bill about what was going on and I got more information over time, I wrote memos to Porter Goss (R-Fla.) and Nancy Pelosi (D-Calif.), who were the chairman and ranking Democrat on the House Intelligence Committee at the time. I wrote to them through their staff directors. To my horror, I soon found out that it appeared that probably they had already approved the system. And that was confirmed pretty soon afterward.

So, in a series of memos, I updated them on what was going on, explained to them all the technology in as simple a way as I could, and I argued very strongly that they needed to have the protections restored, that they had to insist that the encryption of domestic identities be restored and that the automated tracking system for access to the database had to be restored. I told them that if they did not, if the administration refused to do this, they should insist that the system be killed, be stopped.

What was their response? I got no feedback from -- most of the time, I got very little feedback. But it became apparent that nothing had happened. I was about to retire, so this was over about a three-month period.

How unusual is it that you're not getting a response?

It was unusual not to get a response. I went and talked to other people in the administration and tried to talk to people in the judicial branch, too, and it soon became apparent that they had basically signed away their life, that before they were briefed on this, that they would never breathe a word to anybody about it or confirm anything about it to anybody. It became very obvious after I had talked to a number of people. Mostly they would listen and not respond.

But these are the folks with the oversight.

Despite the fact that the House Intelligence Committee and the Senate Intelligence Committee had the oversight, the members -- and the members were not well versed in the technology, nor were any of them attorneys either. But despite that, they kept their promise not to talk to anybody about it.

This became, I think, a critical problem, because intelligence, especially with NSA, is a very technical, very difficult subject, and the Intelligence Committee members rely more than other committees in Congress do on their staff. So in this case, they were unable to get any advice or feedback from their staff, either legal or technical. ...

What else were you hearing? Other people came to you. ...

Over a period of a couple of months, it became quite evident that the program was expanding greatly. My initial hope was that at least this might be temporary in the fear of a new attack that they could find if there was another attack coming.

But the seductive part of the system is that it was designed to get better and better over time. It was designed to take massive amounts of information, and the more information it got, it was supposed to winnow it down to fewer and fewer targets. I became very concerned that if it went on for a long time, nobody would ever want to cancel it in the hope that it would, that they could become more and more reliant upon it.

[? Return to top](#)

---

When I found out that, for instance, by July, the number of servers holding the data had doubled, and it was a massive increase, and it was apparent -- then I also talked in July to Gen. Hayden. That was the second time I talked to him about it, and it was clear that he did not intend to stop it. In fact, he basically sought to prevent me from lobbying against it. ...

Where?

At NSA headquarters.

... You sit down. What happens?

I had a half-hour appointment with him, and he was a little late, so first we talked about ThinThread, and he promised me that the system was to be deployed, which as it turned out, it never was.

Then we got into the post-9/11 surveillance program. My whole point in going there was to ask him why he had taken off the protections, the encryption and the automated tracking. I asked this any number of times, and he always evaded answering. I finally just decided I was not going to leave the room until I got an answer, so I kept asking.

About the fifth time, he looked down, and I remember he could not look me in the eye, and he said, "We have the power; we don't need them." In other words, they didn't need the protections. Then he made clear that the power he was referring to was the commander in chief's wartime authority.

He admits no warrants are necessary as well.

At the time also, I asked Gen. Hayden if they had a warrant, and he said they didn't.

So what are you thinking?

I was stunned. I didn't see how they could have gotten a warrant, but I was even more worried. ... He said that attorneys from all three branches had agreed that the program was legal. ...

This made me even more worried, because I was not sure that even the White House knew that it was possible to do this with protections that would make it far more palatable to be pursuing these activities. It was not clear to me that the vice president knew or the president knew or the FISA judge knew or the Supreme Court knew.

And so instead of allaying my concerns, this actually made me far more worried. So I decided that I would branch out, and I would try to go to the FISA Court judge and to Judge Rehnquist.

Before we do that, how did the meeting end with Hayden?

Toward the end of the meeting, Gen. Hayden made it pretty clear that he wanted me to stop lobbying against the program. I thought when he alluded to it that he was implying that I would leak it. And I told him, I said, "I will not be going to the press, if that's what you mean." And he said, "That's not what I meant."

It was clear to me that he didn't like my talking to other people in the executive branch and on the House Intelligence Committee and trying to convince them to put controls on the program.

His opinion was that checks and balances were not necessary.

Apparently so. Gen. Hayden told me that his three attorneys at NSA had agreed that this was a legal program, constitutional program. It was obvious to me, even as a layman, that that was highly arguable. That was an opinion of some attorneys, but you could not possibly be confident of that until it actually went to the Supreme Court. ...

I knew somebody who knew Justice Rehnquist's daughter, and I sent a note with my credentials and a way he could verify them to Justice Rehnquist and said that I needed to talk to him about a post-9/11 program that appeared to be unconstitutional and that he might know about, but might not know all the pertinent facts.

I also called [Vice President Cheney's Chief of Staff] David Addington, who did not return my call. I also contacted the judge of the FISA Court, the primary judge of the FISA Court, Colleen Kollar-Kotelly, and I asked her for a meeting, because it was not -- if she was aware of the program, I was not sure that she would have been told about the possible protections. And all three of those attempts basically did not come to fruition.

Why did you continue down this route? ...

I persisted in my attempts because I knew the program better than they knew it. A lot of these decision makers did not know the program; they did not know the technology. ... I had been briefed many times on it. I knew what it was capable of doing. And that was one of the reasons I persisted.

Another reason was I had persuaded Congress to finance it. I was culpable also that it had been turned to nefarious purposes, and I had to do everything I could to stop it. Besides that, it was simply my job. I mean, I never even considered not trying my best, because I was the primary person and apparently the only staffer who knew about it on the Intelligence Committee, and it was my duty to stop it.

That was why I was there, to make sure everything was legal and to make sure it was also optimally effective and protected the national security.

I argued with everybody that I met, and I got no refutation from them. I said it was unethical, immoral, politically stupid, illegal and unconstitutional, and stop. And when this comes out, all hell is going to break loose.

[? Return to top](#)

---

One of the next big things you did is you, Binney, Wiebe file a confidential report with the Department of Defense IG. Why was that decision made, and what were you telling them?

After I had reached a dead end with everybody in the summer of 2002, I finally agreed with Kirk Wiebe, who had been agitating with the rest of the group, to file a complaint with the Department of Defense Inspector General about the waste of money at NSA, and in particular the ThinThread and Trailblazer issues.

I finally agreed with Kirk that that was about the only thing left that we could do. So we filed a hotline complaint, the four of us -- Kirk, Ed, Bill and I -- signed the complaint. It was a hotline complaint in which we were supposed to be protected, or their sources were not supposed to be revealed. Tom had agreed to work on the inside with them if they needed help. ...

And the result of the investigation eventually was?

The investigation eventually resulted in a report. There was a preliminary report in December 2004, I believe it was, and months and months later the final report. It was distributed to very few people, and NSA attempted to limit the distribution also by classifying everything. In fact, it wasn't really technically classified. Most of the report, by far the great part of it, was unclassified, but they slapped a "For Official Use Only" label on it, which is not a classification term, and to this day, they have withheld practically all the report.

Again, what this was was about the massive waste and fraud of Trailblazer. It wasn't specifically about the domestic wiretapping, the things that you were more concerned about. Why not bring those issues up to the IG?

I had opposed an IG solution earlier on because this was a very difficult issue in that it went all the way to the White House. I had found that out immediately. And the White House can trump anybody. The DoD IG reports to the secretary of defense; he was certainly in on it. There was basically no hope that the IG would ever be able to do a thorough investigation of the program, in my view. ...

So it was a start, more or less.

Yes. And I remember, we hadn't really finally decided before the meeting with them not to raise the 9/11 surveillance issue, but I turned to them at the end of the meeting, I remember, and said, "Do you want to raise the other issue?," and Bill shook his head no. And we didn't.

Because you guys basically were between a rock and a hard place.

Yes. There was no one to go to. The judicial branch wouldn't even meet with us, with me. And people in the executive either didn't do anything or were unsuccessful. And Congress didn't do anything either. There was nowhere left to go. ...

[? Return to top](#)

---

So 2005, December, [The New York Times article](#) comes out by [James] Risen and [Eric] Lichtblau. It reveals that there is an NSA warrantless wiretapping program. When it comes out, are you surprised? How important is it that this information is finally out there?

The information didn't leak for so long that I thought maybe I was wrong and it wasn't going to leak. I had told everybody, and nobody had disputed me. I had said: "This is going to leak. It's so obviously illegal and unconstitutional. It goes against all the training in the SIGINT community that they've ever had. It's going to leak." And nobody had disagreed. ...

Finally in December 2005, it did leak. But it leaked only partially, and only the least controversial part of the program came out. And the administration effectively spun it to me to say that it was only discussions between known terrorists and their domestic contacts.

It had already been legal actually to collect on that before 9/11. So the additional War Powers and Patriot Act and all that was not necessary even to make it legal, to make that part of the program legal.

To my amazement, when Gen. Hayden was made the point man publicly on this, and he called a press conference in January 2006, and I listened and I guess I read the transcript of the entire press conference, and I was amazed at what he was saying, because it was not truthful; it was misleading. And that was the beginning of the spinning and the lies.

You knew it went a lot further.

I knew it went a lot further.

What did you know, and how far had the program gone by this point?

I knew the program had involved blanket surveillance of the U.S. persons in order to try to go after the domestic threat. But at the press conference, Gen. Hayden claimed that the program was only collected between known terrorists abroad who were in contact with U.S. persons, and that those were the only U.S. persons collected against. I knew that wasn't true.

Gen. Hayden's initial press conference introduced many of the tactics that the administration has used to deflect questioning and also to mislead the public. First of all, he said at the beginning of the press conference that he wanted to make clear that he would discuss the program that had leaked, but he would not discuss anything else. ... They've used that technique ever since also, answering questions with regard to only a small part of the many -- one of the many programs that were involved in the overall program.

Secondly, he also appeared to use unconventional definitions of key terms; for instance, "intercept." It appeared that he was not telling the truth, unless he had a novel definition. And that has often happened since.

For instance, the witnesses before Congress have claimed that there was, is no domestic collection. But they are now defining "collection" not as the physical act of getting communications, of capturing them, but they are now defining it as what we used to call "analysis." In other words, they have admitted that collection now means to them that until an analyst pulls a file out from the database, that is not considered collected.

So you can collect all the metadata and--

Or content, for that matter.

Or content, and not consider it collection because someone hasn't pulled it out of the pile.

Unless they have analyzed it, they will deny that they have collected it.

[? Return to top](#)

---

And from what you knew at that point, what type of information was taken, and how pervasive was the collection?

It is now quite obvious, since the Snowden revelations, that the program grew progressively over time. Initially, I knew that it involved a lot of broad domestic surveillance, bulk collection, domestically. And I knew that it involved emails, landlines, regular house phones, cell phones. I also knew that they had branched out into non-communications data.

Which is what, bank records?

I'm not really -- they have not acknowledged that. All I can tell you is that when I met the second time with Gen. Hayden in July, I said to him that it appeared the program was expanding, not only in number of servers, but also that two new data categories had recently been added, and he nodded to confirm that. I knew that one of those data programs was not communications data. ...

And other commentators have made allusions to other personal data that may be collected. Of course, we all know that transportation data, airline data is connected. We know that international banking data is collected; that has been acknowledged. But there have been allusions to other items, too, by people hypothetically, such as credit, medical, banking and so on.

All warrantless.

Well, all of those as a matter of course.

And content --

So all of that is added to your file with the communications data. So they know, they can join everything together.

All that content and metadata throughout.

It's clear that content was collected on emails. It's not clear from the public data as to whether content was collected on the phone calls. This would, frankly, be very difficult because voice obviously takes a lot more room, storage space than does text. ...

The other thing that we have to be worried about is that they wouldn't be needing all this storage space if they weren't collecting content. The metadata, according to Bill, the way he designed it, can be stored in a very small space. And that was part of the revolutionary design that he came up with. It could be stored very well and in a very small space, and could be easily retrieved.

So you don't need a new data center at NSA headquarters, a new data center in San Antonio, a new data center in Bluffdale, [Utah,] which are several million, 2.5 million square feet total, if you are only collecting metadata. There is no way that you need that. And so I think on the face of it, you have to assume that they're collecting a lot of content, and it's not just foreign content probably. ...

[? Return to top](#)

---

So an investigation is started up. They really want to find the whistleblowers involved in *The New York Times* article. How did they turn toward you guys? ...

After the programs leaked in December and January of 2005 and 2006, I assumed that they would be coming to question me because I read in the paper that a huge team had been put together to find out who leaked the information. It involved, as I recall, five U.S. attorneys and 20 FBI agents. It was a very high-priority thing, and the White House was demanding somebody's scalp.

I assumed that they would call me because I had talked to so many people, opposing the program. But I didn't hear from anybody until August 2006, so eight months later. The general counsel of the House of Representatives called me and asked me if I would voluntarily participate in the leak investigation, and I said I would. But I also said that I would never reveal my sources because -- and that this was a separation-of-powers issue that Congress' investigatory and oversight powers were involved, and I would not reveal my sources.

So that was August 2006. I did not finally meet with the FBI and the U.S. attorney until February 2007 when I was back in D.C. ... My attorney and I went into the meeting in Washington, D.C. To my amazement, it started out in a very hostile manner. It was a very aggressive interrogation, like I was a criminal. That was the first time it occurred to me that they would think that I had leaked it. I was also surprised that they were treating a former congressional staffer this way. ...

[? Return to top](#)

---

July 26, 2007, the feds raid your home. Take us to that morning. Tell us the story of what happened.

My interview with the FBI and the U.S. attorney lasted for three hours, and by the end, it was much more friendly than it had been at the beginning. So I assumed that they were satisfied. We never heard anything after that. My attorney in fact put the case in a dead file.

And then, at 6:00 a.m. on July 26, 2007, five months later, six months later almost, they raided my house and spent five hours there going through everything, and took a whole lot of papers, Rolodex, electronics, only a few of which I have gotten back.

Why?

The warrant that was presented to me indicated that I was suspected of having leaked the story to *The New York Times*, and it also raised the issue of a *Baltimore Sun* article. And I had indeed talked to Siobhan Gorman of *The Baltimore Sun*, but I had not given any classified information. I had no contact or association whatsoever with *The New York Times* or James Risen, so there was no evidence whatsoever against me.

And what happened to your case for the investigation?

As bad as the raid was, and as shocking and stressful as the whole thing was, I at least took solace in the fact that I had done nothing wrong, so there was no evidence that I had done anything wrong, so I assumed that the whole thing would be cleared up quickly.

However, it dragged out for years and years and years. Finally, in about December 2009, so almost two and a half years later, my lawyer was contacted and told that they were asking me to plead guilty to a felony perjury from my interview two and a half years prior. They claimed that -- I had made the statement that I had no idea whatsoever who had leaked the information to *The New York Times*. They claimed that I had said I had no idea whatsoever who had leaked information to *The Baltimore Sun*.

So they deliberately lied in order to get me to plea bargain. And in addition to pleading guilty to a felony that they knew I hadn't committed, they wanted me to tell them that Tom had done illegal things. My response was I didn't perjure myself; it's a lie, and secondly, I don't know anything that Tom has done that was wrong.

And what happens to the case against you? And the case against Tom is what I'm asking next.

After all the charges against Tom were dropped in June 2011, the five of us went to a Maryland court and initiated a lawsuit to get our property back. It appeared that I had been monitored, both my computer and I think for much of that time my phone also, ever since before the raid in 2007. So for years and years, I basically had no privacy.

As part of that lawsuit, I kept asking the status of my case, because I was the only one of the five of us who had not heard, and they always refused to answer formally. ...

Ultimately, finally, I had to sue them in Oregon instead of in Maryland for return of my property because it was seized in Oregon, and at the same time I sued them for violation of my civil liberties. As part of that lawsuit, the government finally stated to the court that the case was dead. I think the only reason that they finally decided to do that was that the statute of limitations had run out.

What was it like to have those men marching, coming into your home at 6:00 in the morning? What was that like?

It was pretty shocking. It was quite shocking. And in fact, I was preparing at the time for a wedding reception for my older son that was to take place at my home in 10 days' time. And they went through the whole house, and went through every book, every paper, every drawer. Turned the mattress over. It was quite shocking. ...

[? Return to top](#)

---

Comes 2009, the Obama administration comes in. Was there a feeling that maybe things would change and that the aggressive actions against you guys might fall off? ...

My attorney and I were hopeful that with the Obama administration coming in, in January 2009, that the administration would back off, because he had said he opposed the program previously. But then that didn't happen, and they became very aggressive. ...

[? Return to top](#)

---

... Along with the fact that it was illegal, along with the fact that it was done in complete secrecy, that checks and balances were subverted, what was the thought among all of you and the people you were hearing from about the effectiveness of this program?

What really bothered me was that the rampant violation of civil liberties was totally unnecessary. It was unnecessary because it could have been encrypted, access could have been tracked, so to make sure that nothing was done that was blatantly illegal.

But the other problem with the program was that they changed it in critical ways, both operationally and technically, in ways that made it much less effective than it could have been if they had done it the way ThinThread had done it.

First of all, they made major technical changes to it. And secondly, they made operational changes. And the operational changes were what became known in recent congressional testimony as the "three hops."

As it happened, I was officially briefed on the program along with other congressional staffers -- on one small part of the program, I should say -- along with other congressional staffers in early March 2002, before I retired. And they told me that they were routinely going out three hops, which means if a terrorist contacted me, they would collect on me, they would collect on anyone I talked to, and they would collect on anyone that person talked to. So that's out to three hops. It massively increases the number of people domestically who are being collected on.

And that is, while they're still denying that they're doing mass upstream surveillance, which is the really important part of this, a lot of the other named programs are basically intended in large part to, quote, do a "legal" cover story for the massive upstream collection that was happening. That in no way can be considered legal.

Define what that is. What is the upstream collection you're talking about?

The upstream collection is the collection off fiber-optic lines, basically duplicating everything on the fiber optic line, making a mirror image copy of what the telephone companies were getting.

And this was finally revealed in -- actually, it was revealed in January 2006, as I recall, when right after *The New York Times* published it, [Mark Klein](#) had already gone to the Electronic [Frontier] Foundation and it had revealed what was happening at the San Francisco switch. So EFF was all prepared with a lawsuit when the item leaked.

That is what they were doing. More recently, the [Edward] Snowden documents have revealed that the U.K. is doing this on hundreds, hundreds of fiber-optics lines, which is a massive amount of data. It's just really hard to conceive of doing that.

So what do you mean, the rest is legal cover mainly?

What has happened here, it is quite obvious, what has happened here is that when they do this, they don't want to admit it to a court. From the beginning, Bill and I realized that this would render unconstitutional many of their lawsuits against terrorists who they might actually find, because if the court ever found out that they were collected against in an unconstitutional manner, with critical information, the thing would be thrown out of court and they would go free. That was another really serious aspect of this.

What has happened, I think, is -- it's pretty obvious to me -- is that the database is now being used, because it has so much domestic

information in it, is now being used for criminal purposes also. It has gone from a national security database and counterterrorism, to national security, to a criminal database.

There was an article published recently in which there were sources from the counternarcotics teams, who are sometimes international, sometimes domestic, and who often cross borders, that NSA was giving them data. And what they developed was -- they had another term for it -- but basically they developed a fake trail of evidence to explain how they got the data so that it could be presented in court. ...

The other item that people haven't focused on is that if they're collecting massive amounts of email and phone conversations and contacts and so on, obviously that could have some exculpatory information, too. But they're not handing it over. And that's illegal, not to hand it over.

So I think what has happened is this has trickled down from we initially became a national security state; we are now becoming a police state in which this huge database with everything on everybody is being used for criminal prosecutions. That's a police state. That is our liberties just simply evaporating.

And it is not only going to be used for criminal prosecutions; it's going to be used against political enemies. And we are the canaries, the five of us. We are the canaries in the coal mine. We never did anything wrong. All we did was oppose this program. And for that, they just ran over us. ...

[? Return to top](#)

And in the end, how has it affected you? ...

Obviously it was a massive stress to be under investigation for six or seven years. And to never know if you're going to end up in jail or spend your whole retirement on legal fees and then go broke, that's a massive stress.

But it will all have been worth it if the U.S. public gets away from this view, "I don't have anything to hide." I cannot understand how people can say such a thing. They don't know history. They don't know political theory. They don't realize that if you believe in anything, it can be used against you. If you have any political beliefs at all, it can be used against you by the opposition if they're in power. ...

[? Return to top](#)

 [E-MAIL THIS](#)  [239](#)  [165](#)  [2](#) [0](#)

#### RELATED

May 29, 2014 / 11:07 am

[How the NSA's Secret Elite Hacking Unit Works](#)

May 23, 2014 / 11:06 am

[How the NSA Can Get Onto Your Computer](#)

May 21, 2014 / 4:51 pm

[How the NSA Can Get Onto Your iPhone](#)

May 20, 2014 / 9:53 pm

[Live Chat: Silicon Valley, the NSA, and You](#)

Comments for this thread are now closed.



0 Comments

FRONTLINE

 [Login](#)

Sort by Best

[Share](#) [Favorite](#)

Be the first to comment

 [Subscribe](#)  [Add Disqus to your site](#)  [Privacy](#)

In order to foster a civil and literate discussion that respects all participants, FRONTLINE has the following guidelines for commentary. By submitting comments here, you are consenting to these rules:

Readers' comments that include profanity, obscenity, personal attacks, harassment, or are defamatory, sexist, racist, violate a third party's right to privacy, or are otherwise inappropriate, will be removed. Entries that are unsigned or are "signed" by someone other than the actual author will be removed. We reserve the right to not post comments that are more than 400 words. We will take steps to block users who repeatedly violate our commenting rules, terms of use, or privacy policies. You are fully responsible for your comments.

[The Trouble with Antibiotics](#)  
October 14th

October 10, 2014 / 10:19 am  
[Courts Block Texas, Wisconsin Voter ID Laws](#)

October 7, 2014 / 6:36 pm  
[Death by Fire: An Update](#)

October 3, 2014 / 7:38 pm  
[Florida Gov. Opens New Investigation into O'Connell Death](#)

JOIN OUR NEWSLETTER

e-mail address

**Like** 387,188 people like this. [Sign Up](#) to see what your friends like.

**Follow @frontlinepbs** 115K followers

FRONTLINE on



Funding for FRONTLINE is provided through the support of PBS viewers and by the Corporation for Public Broadcasting. Major funding for FRONTLINE is provided by The John D. and Catherine T. MacArthur Foundation. Additional funding is provided by the Park Foundation, The Ford Foundation, the Wyncote Foundation, and the FRONTLINE Journalism Fund with major support from Jon and Jo Ann Hagler on behalf of the Jon L. Hagler Foundation.



Supporting Investigative Reporting

