The State of Surveillance

Description: This week, after reminding our listeners that we just had another Microsoft Patch Tuesday, Steve and Leo examine the operation and technology behind the NSA's previously secret PRISM Internet surveillance program.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-408.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-408-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with probably the most important Security Now! we've ever done. He's looked at all of the testimony, all of the information, and he says he's figured out exactly what the NSA is doing to spy on us. Steve breaks it down next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 408, recorded June 12th, 2013: Surveillance State.

It's time for Security Now!, the show that covers your privacy and security online. And this is, I think, a long-awaited edition, at least a whole week long-awaited edition of Security Now! because there's been some stuff going on, and everybody I know has said get Steve Gibson to explain it all. Steve Gibson is the Explainer in Chief and the host of Security Now!, and each week he joins us to talk about security. And I would guess this week you're going to talk about the NSA spying, PRISM, things like that.

Steve Gibson: Yeah, we have to. I got, just as you did, a huge influx of people saying, Steve, what do you think about this? What does this mean? What do we know? What can we presume? And one of the most interesting things that for me occurred is that - and I've watched every show, I've watched all the talking heads, I've read everything that was there because I was interested in this. And so what I saw was a way for all of these pieces to fit together, for it to be absolutely true that Apple and Facebook and Google and Yahoo! and so forth are honest in their denial, yet the slides that the NSA showed saying they had direct access to their servers are also correct. That is, there is technology which the NSA has employed. We have evidence of it. The EFF has been involved in some prior lawsuits. We have testimony with photos.

And when all of the pieces clicked and, like, came together in my mind, I said, oh, now I know why it's called PRISM. I know where the name came from. It came directly from

the nature of what they're doing. And so while I have no - obviously I have no allegiance or connection in the past or present to any of our three-letter agencies. I have no specific knowledge of this. But looking at all of the evidence, what I can offer our listeners this week is something so compelling that they will know as well as you will know, Leo, that this is what's going on.

Leo: Good.

Steve: And it tells us about the technology. And but I want to lead off, because I know that many of our listeners have not been following this as closely as I have, so at the beginning of ABC's "This Week" show on Sunday morning with George Stephanopoulos, he had Glenn Greenwald on, who broke the story with the Guardian. And it was such a short, succinct statement from Glenn that I wanted to put that into the podcast at the beginning. And then I also want to - one of the things that I'm hoping could come out of this is that we could give Congress the right questions to ask because there was - there's a glaring testimony back on March 12th, just not even, well, exactly, actually, it's the 12th today, right, so exactly three months ago, where a Senator asked point blank, I mean, just directly to our Director of National Intelligence, if the NSA was collecting any information on millions or tens of millions or hundreds of millions of Americans. And James Clapper said no.

So anyway, I want to sort of fill in for people who haven't been following this as closely as we have, and then talk both about the first program, which is the telephone metadata collection - it's been, like, annoying me when I see people on the news saying, oh, well, you know, that's just metadata. That's not the phone conversations, blah blah blah. So we're going to talk a little bit about what that means and what the power of that is. And it's funny because I had already written down in my notes early in the weekend that one of the significant factors of this was the history that was collected. And then in his amazing video, Edward Snowden said that. So I grabbed that little 46 seconds of the video to also play. We might as well have it in his voice, the person who disclosed this and is now on the run.

And we have actually not much news except for that. Very little. But I think we've got a great podcast, and I think people are going to find it extremely interesting when they get what's going on. And I think I know what's going on.

Leo: Well, that's exciting. And it's very interesting because - and I'm very interested to hear what you have to say.

Steve: And no one has, no one, I mean, I've been watching everything, listening to everything. Nobody has figured this out, apparently. And I'm going to offer what is probably the answer.

Leo: Wow. Security Now! on the air, Steve Gibson, Leo Laporte. Let's get the news out of the way, and then we can start talking about PRISM.

Steve: It's going to be pretty quick, actually. The only thing that happened that I noticed, because I actually did have my attention rather intensely focused...

Leo: I bet.

Steve: ...on all of this, is that we just crossed the second Tuesday of the month. So all of our regular listeners know that means that Microsoft issued a batch of patches. And these were about as non-dramatic as any could be. So I'll simply remind our listeners, rather than going into any detail or depth, to update Windows. When I turned on my Windows 7 machine to fire up this Skype session with you, Leo, I saw 15 updates were offered to me. So everyone should find time to do that. We know that updating in a timely fashion is increasingly important because there's a window now between the time that patches are released and people act on those released patches. The bad guys are able to figure out from the patch what the vulnerability was, if it was not previously disclosed, and these were not, and then take action against people who have not yet patched that. So this is - it's becoming important to do it as quickly as you can.

And I was happy to see Apple, by the way, during the keynote at the Worldwide Developers Conference, say that iOS 7 will be updating its apps just in the background and more or less continuously. That's wonderful news since I had 86 that I hadn't updated.

Leo: Yeah, it's ridiculous. Even John McCain was pissed off. So at this point I think it's time to fix that. And we're glad that they did, yeah. And as for Zune, we'll see. I haven't looked at it yet, but Jeff has. There is a way to turn that auto-update off; right, Jeff? I think there is. So you get the choice. But the default should be on, I would expect.

Steve: And then the only other thing I have of news also is from Microsoft. It came in via a tweet from @FaustoCepeda, who alerted me to a Fixit which Microsoft published which allows Java to be disabled in IE. So this is new from Microsoft. They've never given us a, look, we understand Java's a problem; we're going to let you disable it in Internet Explorer. This is, I think, useful also because there are many people who are stuck in corporations where they have to be using Java, but not necessarily in their browser. And they also have to be using IE, so they can't use tools like NoScript in Firefox and tools to control Java in the browsers, other browsers that have done a better job of controlling that.

So if you Google "Java when you cannot let go" is in the tail of the URL. That will get you to Microsoft's Fixit. And I would recommend, for example, since we all have IE installed in Windows because we don't have a choice, even though we're not using it, we're typically using Firefox or Chrome or Opera or whatever, it makes total sense to disable Java in IE. So this just turns off Java, sorry, turns off IE's invocation of Java for web applications. And it only affects IE, won't mess up your other browsers nor Java on your desktop. So certainly a useful thing to do.

Now, the acronym search has already begun for PRISM. And although it is not an acronym - as you will have me explain later, I know why they called it PRISM - the first one's been submitted by Barry Spar a couple days ago who said, "PRISM stands for People Really Interested in Spying on Me." So that's pretty good, I thought. And Leo, I did want to mention, just for the people who don't watch iPad Today, I watched it with you and Sarah last week.

Leo: Thank you.

Steve: And the free application Dumb Ways to Die...

Leo: Hard not to - hard to stop playing it, isn't it.

Steve: Oh, my God. It is so...

Leo: It's a fun game.

Steve: It is. It's dumb, but it's fun. It's just a hoot. I tweeted it. And I didn't realize it also works on iPhones. I would think you'd need a little more surface area. So I like it on my iPad. But the music and the graphics and, I mean, somebody with a great sense of humor put this thing together.

Leo: And it's free, which is not even any in-app purchases or anything, it's just free free.

Steve: It's not a huge monolith like some of those astronomy apps or the elements or something where it's like, oh, my god.

Leo: It's fun to play.

Steve: So I wanted to recommend it. Dumb Ways to Die from the iTunes store, for anyone who has iOS. It's just a kick. And not hard to play. I did get a thousand points, and I unlocked the, quote, "music video," unquote. Have you seen that, Leo?

Leo: No, I haven't gotten that far.

Steve: Oh, god, it's worth getting to a thousand points.

Leo: Okay, I will.

Steve: And look at the music video because it's wonderful.

Leo: It's just the silliest game ever.

Steve: Oh, goodness.

Leo: But it's addictive. It's fun. You can't stop playing it, yeah.

Steve: Well, it's just, yeah, it's simple. There's also, shoot, something else I ran across that I - the problem is I've got so many icons now that when I buy something, I can't find it. And so, yes, you can search for it, but then you still don't know where it is in your 12 screens of scroll.

Leo: iOS is effectively a desktop where you put all your icons, and that's it. Just [noise]. Just like a Windows user who has everything on the desktop.

Steve: I was happy to see a feature that got applause during the Worldwide Developer Conference - I also watched your coverage of that on Monday morning, which I thought was great - that groups or folders or whatever you call them can now be scrolled. So it's like, oh, good. So I can have Games or Puzzles, and I can put them all in there, rather than Puzzles 1, Puzzles 2, Puzzles 3, because they used to fill up, and then you couldn't put any more in. So that's good news, too.

Leo: Yes.

Steve: So I did have a little comment about near field communications. I got a tweet from someone in Cranbourne East, Australia, who said: "Listening to Episode 407 and NFC. Often get 'multiple cards present' when I use NFC, even if my wallet is over four feet away from the reader."

Leo: I don't know how that's possible.

Steve: It's radio, Leo. It's like, you've been a ham, and so you're aware of, like, when atmospheric conditions are just right, suddenly you can receive Russia from your porch, whereas normally you wouldn't be able to? I mean, the ionosphere and so forth.

Leo: "I can see Russia from my porch."

Steve: So the idea is that radio is flaky this way. I mean, it doesn't actually ever die. It's not like there's a cliff or anything, or an optical beam where, I mean, it's radiated. And we know from all the experiments that have been done, for example, with Pringles cans and WiFi antennas, that you can make an amazingly strong directional WiFi antenna out of a Pringles can. So my point is that it is really - it's fundamentally a bad idea to use near field communications for something as important as payment where someone can, as we talked about last week, walk past you and pull money from cards that you have in your wallet. It is just - it's broken at birth. Bad idea.

Leo: Bad idea.

Steve: Bad idea. But I have a good idea. I got a nice note, actually the subject was "Unbelievable," from a listener of ours, Eliot Fleming, who's in Providence, Rhode Island. He said, "I've listened to Security Now! for a long time, but I've not had occasion to use SpinRite before." Then he says in parens, "(Please make a Mac version someday, somehow.)" And he said - and that's going to happen. And he said, "My daughter's Windows XP Dell laptop" - so I guess daughter's using Windows and he's on a Mac - "was being sluggish, so I did a system restore. This had the unexpected result that the laptop would now not start, even in safe mode. Whoops. It would start to load Windows, go to a blue fail screen, which we all of course know as the Blue Screen of Death, and restart.

"Dell's diagnostic suite said everything was fine. Chkdsk from the XP install disk found a single error on a hard disk. I knew I could reload Windows, but thought it might be worthwhile to preserve the files and applications on the computer." And I'm sure his daughter would agree. So he says, "I bought SpinRite, burned it to a CD to boot the laptop, and ran SpinRite at Level 2. It found errors in two sectors and recovered as much data as possible, taking about two hours. When I restarted the laptop normally" - well, we know how this turns out - "Windows told me that the system restore was successful. Insert bitter laugh here," he says.

"It is unbelievable to me that you could have programmed this much functionality in such a tiny program. Could you use a Linux loader to access the hard drive level on a Mac somehow?" And of course now he's trying to solve how to get SpinRite running on his Mac. "(Consider plea for Mac version repeated here)," he says in parens. "In any case, thank you for your dedication to providing an amazing utility. My daughter thanks you for saving her schoolwork and years of photos." And for anyone new listening, I wrote quite a while ago SpinRite, which is saving hard drives, recovering the data on hard drives to this day. And you can get it at GRC.com, my website.

Leo: And I think it's probably safe to say there'll never be a Mac version of it.

Steve: It's running on my Mac right now, Leo.

Leo: Is it?

Steve: I'm secretly working on it. That's why I haven't said anything.

Leo: That's good news for us Macintosh users. You can take a Mac drive out, if you can, and put it on a PC and have it run because it doesn't care about file systems. Right? I mean, it can run against the HFS. It's not the file system that's the problem. It's the lack of BIOS.

Steve: Yeah, the problem with the Mac, well, actually, no because the Boot Camp provides a compatible BIOS. The problem was that SpinRite was using the physical hardware of the keyboard in the PC.

Leo: I didn't know that. Were you storing data there? What were you doing?

Steve: Well, there's two bytes. There are two I/O words, 60 and 61. And I'm actually, when SpinRite is multitasking, which is like you're able to jump around between screens, and it's doing all these things at once, there's actually a multitasking OS, essentially, that I wrote for it. I can't use the BIOS because the BIOS is not reentrant. And so if I'm using the BIOS to read and write the disk, I can't also be checking the keyboard to see if the user wants to switch around. So I had to go directly to the keyboard hardware.

Leo: Ah. You read the chip.

Steve: Problem is the Mac - yes. I'm actually physically reading the bits out of the physical hardware, which I can do no matter what the BIOS is up to. So all I had to do was I just reengineered the technology. The Mac uses a USB-based keyboard. So although it simulates the keyboard through the BIOS, it doesn't simulate the hardware because that would be, like, overkill. Anyway, so I did that, and I've got it running on my MacBook Air just...

Leo: Awesome.

Steve: ...very nicely. So anyway, it's what I've been working on. I didn't want to make a big announcement because I didn't want to kill sales. It really shouldn't because everyone, all the way back nine years, to SpinRite 6, is going to get a brand new SpinRite for free.

Leo: Woohoo!

Steve: I'm not going to charge you anything for it. So...

Leo: That's nice. Even if you're on a Mac?

Steve: Even if you're on a Mac. We have had listeners who bought SpinRite to support the show but have not been able to use it because they have a Mac. So how can I ask them for more money?

Leo: You can't.

Steve: I'm not going to. I'm not going to.

Leo: Couldn't possibly.

Steve: No.

Leo: Very kind of you. That's great.

Steve: Okay.

Leo: Moving on.

Steve: So I have two favorite tweets that relate to today's podcast topic. The first one, I actually picked it up somewhere else, from @StephenAtHome. And he tweeted something that I thought was quite clever. "If you're doing nothing wrong, you have nothing to hide from the giant surveillance apparatus the government's been hiding."

Leo: That's Stephen Colbert, you know.

Steve: Oh, it is?

Leo: Yeah.

Steve: Oh, I didn't...

Leo: Soon as I heard the tweet.

Steve: I did not know.

Leo: John came running and said, oh, yeah, that's Colbert.

Steve: Oh, cool.

Leo: That's funny, yeah.

Steve: Well, great. Anyway, I love that. The little double whammy there.

Leo: Nothing to fear.

Steve: And then days ago Robert Yount tweeted from Palm Harbor, Florida, noting, he said, "The NSA just needs better PR. The FREE PRISM cloud-based backup system..."

Leo: Backup, yeah, yeah.

Steve: "...would sound so much better."

Leo: Yeah, yeah.

Steve: So, okay. So where are we? We've had these revelations in the last couple days, I guess starting last Friday, couple days before the last podcast, where of course the Guardian broke the news of now we know Edward Snowden, who did not graduate from high school, got his GED, went into the military briefly, broke both of his legs during training so decided the military wasn't for him, and then got a job as a guard in an NSA facility. But apparently, from watching the video, the guy seems to have himself together. He's sharp. Apparently he's got computer skills. And so he moved up through the ranks pretty quickly.

And one of the major issues of controversy, which now is being discussed in the press, is how somebody who is seemingly not highly qualified, not the kind of person you would want to entrust all of your state secrets to, had access to all of this, part of which he's disclosed, part of which Glenn Greenwald of the Guardian, who was the reporter that interviewed him and broke the story, says they've been selectively releasing, and there's more to come. How did he have all that? One guy said, well, he was stationed recently in Hawaii, and in IT there, and the IT folks have to have access to more technology. And when you're sort of off in the boonies, the boondocks, then we're not watching you so closely. So that's one theory of that. Anyway, who knows? During the video...

Leo: I think we should also say it's possible he's completely lying.

Steve: Yes. Absolutely. All we know is what he's saying. And, okay. So a bunch of people have asked me what I feel about this. And there's been a lot of question about what label do we put on him? Do we call him a traitor? Do we call him a criminal? Some people are calling him a hero. And this is not a policy and politics podcast, so it really doesn't matter. What I know is that I am, frankly, glad that this has happened because, more than anything else, what we're going to see is that we're relying on congressional oversight, yet the people who are running the program are lying to Congress. That can't happen. I mean, that's the problem.

So this has come to light, I mean, this has brought this behavior to light. And we're a democracy. I understand the need that the NSA and the CIA and the FBI have for collecting data. And I know, Leo, I watched your coverage of this on TWiT on Sunday. And you guys were joking about googling IED. And it's like, oh, no, no, I don't want to Google that. I mean, and it is sad that I'm finding myself being self-conscious when I search things that I realize are keywords. I'm thinking, oh, I wonder if this has, you know, tripped some alarm somewhere. And or when I'm sending email, and I realize, oh, I mean, there's a creepy feeling now that we have.

Leo: It's called a chilling effect. And that's often the case when stuff like this happens.

Steve: Yeah. And of course so we often talk about tension on this show because we talk about security and privacy and ease of use. And I've often talked about how there's an inherent tension that exists between the fact that you would like things to be easy to

use; you'd also like to have lots of security. Thus, for example, the famous problem of choosing a good password or password system or whatever. I mean, the fact is you'd like to have one password that's easy to remember. We know that that's - so there's, you know, that's really bad for security, really good for ease of use. So you have to compromise.

And there's similarly, in a society and in a government like ours, a tension is going to exist where we have inherently asymmetric terrorism and crime, where law enforcement has, I mean, a clear need to be able to collect intelligence, and the intelligence is going to come from our environment, from where we are. Well, now of course we're in the world of the Internet where, as it's often observed, everyone virtually is leaving footprints behind them. And that information, you can imagine on the NSA side the overwhelming desire, I mean, just salivating to have access to everything. They're convinced they will act responsibly. And their argument is we need it. I'm sure in the intelligence meetings behind closed doors they're explaining to the people on the committees that we have to have this data. We have to have it. And we're going to do the right thing with it. Trust us.

And for me, the saddest thing was this testimony on March 12th, where I think it was Senator Wyden of Oregon, who is on the Intelligence Committee and has been concerned about these issues for quite a while, informed ahead of time the Director of National Intelligence, James Clapper, that he was going to ask him whether the NSA was collecting data on millions of Americans, gave him fair warning, and James Clapper said no. And then afterwards Wyden's office contacted the NSA and gave Clapper the opportunity to revise his testimony, and they declined to do that. This was three months ago today.

Leo: You kind of expect spooks to lie. At least in public. I'm hoping they're telling more, being more forthcoming in the closed sessions of the House Intelligence Committee and places like that. We don't know.

Steve: It's been noted, though, that it is absolutely possible to obfuscate and to say, "I'm afraid I cannot answer that on the grounds that it would be divulging..."

Leo: That would be preferable, wouldn't it.

Steve: Yeah.

Leo: But that would be an admission. I mean, if he said that, that would be an admission. Wouldn't it?

Steve: Well, okay.

Leo: So I think spooks lie. I don't think that's a surprise.

Steve: Well, I'm not a constitutional attorney, obviously.

Leo: Oh, it's illegal.

Steve: But Wyden had to - and he was sworn testimony, I mean, this is like, you know...

Leo: Yeah, it's perjury in front of Congress, yeah.

Steve: ...hand on the Bible and so forth. So Wyden would not have asked in an open session that question if he didn't expect to get a truthful answer, meaning that - and he knows way more about what's going on than I do. If that was a question he had to have asked and answered behind closed doors, then fine. But this was not. This was on the record, in public. And I have a clip of it that we'll play here in a minute just because our listeners need to hear this. And it's part of this, what is I think an important story. But I need to lay a little bit of this groundwork because what I'm going to explain is really going to upset a lot of people.

And so what I will say is, while I'm glad that this came out, I, in Edward Snowden's position, could never do it because he swore an oath, and that's the end of it, as far as I'm concerned. He no longer - the only reason he had access to this information is that he promised he would never, ever divulge it. And so his only recourse, if he found what he was learning to be distasteful, was to resign and remain silent for the rest of his life. I mean...

Leo: Well, okay. But it's more complicated than that because, if you were a Nazi soldier, you could say, well, I signed an oath that I'd be loyal.

Steve: Well, and there's - people have been calling him a whistleblower. But as I understand it, a whistleblower is when you are describing something which is illegal. And so one of the interesting points, Mika Brzezinski kept making it on "Morning Joe" early this week, was that she said, well, this is legal; right? This is legal; right? And of course the point is that, if we don't know what's happening, we can't ask the questions, and we can't fix the law which is broken. Some people are arguing that it's time to revisit this now, that maybe this has gone a little further than we intended. And if we don't have the truth being told to our lawmakers by the people who are doing the watching, that is, if there's no one watching the watchers, which is what happens if you prevaricate like this, then we don't have feedback in the system.

Leo: Right.

Steve: So let's play George Stephanopoulos's brief - the beginning of his interview because Glenn Greenwald - George asks a bunch of quick questions that are great, and Glenn answers them very nicely, I think.

[Begin clip]

GEORGE STEPHANOPOULOS: Hello again. The secret struggle to balance national security and individual liberty broke out into the open this week after a series of blockbuster revelations starting in the Guardian newspaper. We learned that the government has the

capacity to track virtually every American phone call and to scoop up impossibly vast quantities of data across the Internet. And our first guest is the Guardian columnist getting these scoops, Glenn Greenwald. Thank you for joining us today, Mr. Greenwald. You are really on a roll. You broke another story yesterday showing the scale of the data collection programs. In March 2013 you report the government collected 97 billion pieces of data, almost all of it from outside the U.S. What's the key finding here?

GLENN GREENWALD: There are two key findings. One is that there are members of the Congress who have responsibility for oversight, for checking the people who run this vast, secret apparatus of spying to make sure they're not abusing their power. These people in Congress have continuously asked for the NSA to provide basic information about how many Americans they're spying on, how many conversations in telephone and chats of Americans they're intercepting. And the NSA continuously tells them, we don't have the capability to tell you that, to even give you rough estimates.

And what these documents that we published show, that were marked "Top Secret" to prevent the American people from learning about them, was that the NSA keeps extremely precise statistics, all the data that the senators have asked for that the NSA has falsely claimed doesn't exist. And the other thing that it does, as you said is it indicates just how vast and massive the NSA is in terms of sweeping up all forms of communication around the globe, including domestically.

GS: You also drew new criticism yesterday from the Director of National Intelligence, James Clapper. He called the disclosures "reckless," said the rush to publish this creates significant misimpressions, and added that the articles are filled with inaccuracies. Your response to that?

GG: Every single time any major media outlet reports on something that the government is hiding, that political officials don't want people to know, such as the fact that they're collecting the phone records of all Americans, regardless of any suspicion of wrongdoing, the people in power do exactly the same thing. They attack the media as the messenger, and they try and discredit the story. This has been going back decades, ever since the Pentagon Papers were released by The New York Times and political officials said you're endangering national security.

The only thing we've endangered is the reputation of the people in power who are building this massive spying apparatus without any accountability, who are trying to hide from the American people what it is that they're doing. There's no national security harm from letting people know that they're collecting all phone records, that they're tapping into the Internet, that they're planning massive cyberattacks, both foreign and even domestic. These are things that the American people have a right to know. The only thing being damaged is the credibility of political officials and the way that they exercise power in the dark.

GS: Well, one of the things you reported is that the government has, quote, "direct access" to the servers of massive Internet firms like Google and Microsoft and Facebook, and all the companies have come out and denied it. You see Google saying, "The U.S. government does not have direct access or a backdoor to the information stored in our data centers," similar statements from Facebook and Apple. And Mr. Clapper also said the U.S. government does not unilaterally obtain information. Now, I take it there could be some semantic word games being played here. What's your understanding about what is actually happening? Because it does appear that they don't have direct access to the servers.

GG: Well, our story was very clear. What we said was that, and we presented it as the

story from the start, was that we have top secret NSA documents that claim that there is a new program called the PRISM program in place since 2007 that provides, in the words of the NSA's own documents, collection directly from the servers of these companies. We then went to all of those companies named, and they said, no, we don't provide direct access to our servers. So there was a conflict, which was what we reported, that the NSA claims that they have direct access; the companies deny it.

Clearly there are all kinds of negotiations taking place and all kinds of agreements that have been reached between these Internet companies that store massive amounts of communication data about people around the world and the government. We should have this debate out in the open. Let these companies that collect massive amounts of information about people and the government resolve this discrepancy in public. Tell us what it is exactly that these companies are turning over to the government, and what kinds of capabilities the government is wanting to access. So we reported these discrepancies precisely because we want them, those parties, to resolve it in public, in sunlight, and let people decide whether or not that's the kind of country they want to live in when the government can get this massive amount of information.

GS: The DNI spokesman also said that a crimes report has been filed by the National Security Agency. Have you been contacted by the FBI or any federal law enforcement official yet?

GG: No. And any time they would like to speak to me, I'll be more than happy to speak to them, and I will tell them that there's this thing called the Constitution, in the very first amendment of which guarantees a free press. As an American citizen I have every right, and even the obligation as a journalist, to tell my fellow citizens and our readers what it is that the government is doing that they don't want people in the United States to know about. And I'm happy to talk to them at any time. And the attempt to intimidate journalists and sources with these constant threats of investigation aren't going to work.

GS: You've described your source as a reader of yours who trusted how you would handle the material. The source has also been described as a career government official who is concerned about these programs. A former prosecutor called the source a "double agent."

[Pause clip]

Leo: This is before the Snowden revelation came out, I take it.

Steve: Yes, yes.

Leo: So they're talking about Snowden at that point.

Steve: Yes.

Leo: Okay.

[Resume clip]

GS: I know you're not going to reveal the source, obviously. But what more can you tell us about the individual [indiscernible].

[Pause clip]

Leo: Not so obviously. He did.

[Resume clip]

GG: Well, first of all, I'm not going to confirm that there's only one individual. There could be one or more than one. But let me just make this point because I think this is so critical, because every time there's a whistleblower, somebody who exposes government wrongdoing, the tactic of the government is to try and demonize them as a traitor. They risk their careers and their lives and their liberty because what they were seeing being done in secret, inside the United States government, is so alarming and so pernicious that they simply want one thing, and that is for the American people at least to learn about what this massive spying apparatus is and what the capabilities are so that we could have an open, honest debate about whether that's the kind of country that we want to live in. And if people decide that, yes, they do want the government knowing everything about them, intervening in all of their communications, monitoring them, keeping dossiers on them, then so be it. But at least we should have that debate openly and democratically.

Unfortunately, since the government hides virtually everything that they do with the threat of criminal prosecution, the only way for us to learn about them is through these courageous whistleblowers who deserve our praise and gratitude and not imprisonment and prosecution.

GS: Finally, should we be expecting more revelations from you?

GG: You should.

GS: Okay. Glenn Greenwald, thanks very much.

[End clip]

Leo: I'm not thrilled with the way that he and the Guardian are parsing this out. It feels to me like that's a little bit of a play for more views.

Steve: Yeah, I think so. And, I mean, I understand their commercial interest in getting as much bang for the buck as they can. They have a reputation that they've established, which is what caused Edward to choose them. He knew that Glenn was sympathetic to his position and civil liberties and so forth.

Leo: And Greenwald is, I think, well regarded. He's smart. He's an attorney. He is a privacy and security expert and, I think, probably the right person. And the Guardian...

Steve: Right, and...

Leo: ...is a good journal. Washington Post we should say simultaneously broke the story, so...

Steve: That's what I was trying to say, yes.

Leo: It's likely that Snowden or whoever, if there were other informants, also gave this to The Washington Post.

Steve: Well, and it occurred to me that one of the reasons that he gave them to both outlets is because there was a prior instance where this kind of information was sat on for a year. And so that didn't - that wouldn't allow Edward to get the goal of getting this stuff disclosed. He says in the complete video, which I would commend people to watch, it's very interesting, that he does not want the story to be about him, to whatever degree possible. To some degree it is. He wants it to be about what's going on.

Okay, so with that little bit of sort of backgrounding, let's look at the James Clapper video. It's only 48 seconds. This is taken from the video record of congressional testimony that was open, obviously, to cameras exactly three months ago, on March 12th, where with prior notice of the question, the Director of National Intelligence was asked what the NSA is doing.

[Begin clip]

GEORGE STEPHANOPOULOS: ...is the desire for more public information. Now, he believes that the administration has not been misleading generally the committee and the public. But I want to play an exchange that was in the Intelligence Committee in March when James Clapper was questioned by your colleague, Senator Wyden.

[Begin embedded clip]

SEN. RON WYDEN: Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?

JAMES CLAPPER: No, sir.

SEN. WYDEN: It does not.

JAMES CLAPPER: Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly.

[End clip]

Leo: All right.

Steve: So there it is. That's our...

Leo: That's not even a non-denial denial. That's a denial.

Steve: [Laughing] There's no way.

Leo: There's no way.

Steve: There's no way to walk yourself out of that one.

Leo: Yeah.

Steve: And, I mean, and then Andrea Mitchell interviewed him for "Meet the Press" on Sunday. And I'm looking for where it was he - he actually said to her, "I thought, though in retrospect, I was asked a 'when are you going to ... stop beating your wife' kind of question, which is ... not answerable necessarily by a simple yes or no." So this is - he said to Andrea, "So I responded in what I thought was the most truthful, or least untruthful, manner by saying, 'No.'"

Leo: Okay.

Steve: Oh, I know. It's just painful.

Leo: Okay.

Steve: I know. There's a great - if anyone's curious, there's a great take on this. Fred Kaplan wrote an article in Slate.com, and it says, "Fire DNI James Clapper. He lied to Congress about NSA surveillance." And I don't know whether the guy has to go, but he certainly did lie because we now know much more than we did three months ago when this was said to - when he was asked this openly. And the EFF, of course, the Electronic Frontier Foundation, is all over this, happily, or I'm happy to say. I really thought that their summation of this was perfect.

They said, quoting from a longer article, they said: "All of this would be amusing if the administration's main argument to defend the NSA's massive spying program" - and "spying" is their word, not mine. Certainly it is surveillance. Spying requires a judgment. "All of this would be amusing if the administration's main argument to defend the NSA's massive spying program is that Congress has been informed of all their activities. Democracy can't function when Congress is 'informed' by the 'least untruthful' statements of the administration, using unusual definitions that are designed to given an impression that is the polar opposite of the truth."

I skipped part of this that explains, when he responded this way, Andrea said, well, but how can you answer no, that you're not collecting information? And then he said, "Clapper's deceptions don't" - I'm quoting from the Slate article. "Rambling on in his rationalization to Andrea Mitchell, he focused on Wyden's use of the word 'collect,' as in, 'Did the NSA collect any type of data ... on millions of Americans?' Clapper told Mitchell

that he envisioned a vast library of books containing vast amounts..."

Leo: Oh, please.

Steve: "...of data on every American. 'To me,' he said, 'collection of U.S. persons' data would mean taking the book off the shelf and opening it up and reading it.'"

Leo: But this is interesting because all of these things he's saying really are an acknowledgment that "no" was a lie.

Steve: Yes.

Leo: It's only not a lie if you have these bizarre interpretations of what the question meant.

Steve: Well, yeah, I mean, what can he say now with this recording of him three months ago flatly denying what we now know has been true for years?

Leo: Right.

Steve: Okay. So, first, what was authorized under the FISA Article 215, that's the telephony metadata collection. What I found interesting about it was essentially what's going in is that all the telephone companies naturally keep the records that they need for billing. So they're recording so-called "metadata." We've talked about metadata. Metadata is essentially sort of the, not the main content, it's the embellishment. For example, when we talk about a browser query, there's the query, and then there's the headers, and the headers are metadata. They're additional information. Date and time stamp and cookies and so forth are browser metadata. Or in a file system, you know, you're storing files, but it's also keeping track of when you last accessed the file and when it was modified and when it was created and file privileges for example, who's able to access it. That's metadata.

So similarly, telephony metadata is - it's like where you are by, like, which cell tower your call is coming in on; your originating phone number, or actually it's the serial number of your phone; the number you dialed; probably where it is maybe, though if it went off out into a different phone system, they may not have that. But basically it's your call records. It's not your conversation, it's the event features of the call.

Well, what's interesting is that phone companies have no need to retain that in perpetuity. They typically only keep it for 60 to 90 days. So what's happened is, as authorized under this Article 215, the NSA has set up arrangements with all of the domestic phone companies to acquire this data before they delete it. So, and it turns out that it's not against the law to do this. The so-called "business records" have been ruled by the Supreme Court not to be subject to privacy protection. So if AT&T or Verizon's business records, this is just their records for their own purposes, and...

Leo: This is like the billing, the billing information that they would have.

Steve: Yes, exactly. And it's about to be deleted, and the NSA says, oh, oh, oh, hold on a second, let us make a copy of that. Or just send it to us before you hit delete. So in listening to all of the buzz about this, there's this downplaying of, well, but it's not your conversations. It's just the metadata. And I'm sitting here thinking, oh, my god, I mean, do you realize what it means? If there is a facility huge enough to capture and contain all of that, and the computing resources necessary to link it together, what this builds is an incredible graph of all of the connectivity that exists between everybody with a phone in the United States.

And it's funny because in my notes I was already making a note that, well, the history is also really important, and crucially important to the NSA because, for example, if they got, identified a person who was a suspect of something, a terrorist presumably, or a bad guy qualifying for further surveillance, they can query this network. And what the continual collection of the data means is that they can go back in time, they have a time machine that allows them to walk back and look at the history of all past connections over time. That's unbelievably rich. And it happened that Edward, during his interview, said exactly that. So I thought, it's a very short piece, we'd just hear it in his own words.

[Begin clip]

EDWARD SNOWDEN: ...care about surveillance. Because even if you're not doing anything wrong, you're being watched and recorded. And the storage capability of these systems increases every year consistently by orders of magnitude to where it's getting to the point you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody, even by a wrong call. And then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer.

[End clip]

Steve: So...

Leo: And by the way, I want to point out that, if anybody would say, well, the government would never do that, just there are some pretty good examples with Nixon's enemy list and J. Edgar Hoover's persecution of Martin Luther King.

Steve: Yes.

Leo: That it is not unusual for our government, our republic to do this kind of thing.

Steve: And it doesn't, I mean, these are people who at the time righteously believed that they were doing the right thing. I mean, they were doing it in secret, and that's a problem. And, I mean, secrecy is what we have to worry about because, exactly as you say, Leo, there is ample history of abuses of this kind of data collection. And so I just wanted to shine a little light on this notion that, oh, well, telephony metadata is not useful. Remember we talked about some time ago this new facility that the NSA is

building. We were scratching our heads at the time, wondering what is a zettabyte, because this place can store five of them. Five zettabytes worth of...

Leo: Million square feet. Million and a half square feet.

Steve: Yes. It's a million and a half square feet costing $1.2 billion dollars, 26 miles south of Salt Lake City, in a town called Bluffdale, Utah. It uses 65 megawatts of power. It has its own power substation and, like, cooling ponds; and, I mean, it's just phenomenal. And at the time we were thinking, well, what are they going to put in that? What are they going to fill that with? Well, you know, we have an answer to that question now.

Leo: We continue on. Steve Gibson, we're talking about, of course, PRISM and the revelations which continue from the Guardian and The Washington Post and others, about some sort of federal spying. We've heard the word "Echelon" for more than a decade. We knew that after 9/11 President Bush authorized warrantless wiretaps. I remember, don't you remember, the whistleblower that in 2000, I think '6 or '7, told us that the NSA had a secret room at AT&T headquarters in San Francisco so that they could collect this kind of data. So this is not - we're not talking about anything new here.

Steve: No. And I think that, well, there is something new. And that's PRISM. And I'm going to explain what's been done differently than as far as we know anything we had before.

Leo: Excellent.

Steve: Because this may be, this podcast may be viewed by people who are not regular listeners, if people want to send this link to others and so forth, I'm going to give a little bit more background to the way the Internet works than our regular listeners would need. We've had a series of podcasts in the past famously on how the Internet works. And of course I'll keep it brief and aim it at the point that I'm bringing.

So what we have with the Internet, the word "Internet" is interconnected networks. The Internet itself is a global interconnection of privately owned networks. And in some cases they may be government-owned networks. Or, in the U.S., generally we have AT&T and Verizon and Level 3 and large carriers who then supply connectivity to Cox Cable and Cablevision and smaller carriers, and ultimately down connected to our own little network in our homes. And this is all glued together with routers. We've got consumer routers made of plastic in our homes; but there are, as they're called, Big Iron routers, which route vast quantities of data across the Internet.

And I'll just take Google as an example because it's so well known. All over the world, people are sending data to Google. They're putting Google in their browser. They're asking Google to find them things. They're doing searches. Maybe they're using Gmail and establishing a secure connection to a Google server that exists in a Google datacenter somewhere on the planet. So the way that happens is that, with all the people scattered around, they put packets of data onto their own network, the network that they're on, and the router on that network by definition is connected to at least two

places. Consumer routers are connected to their home network and to their ISP's network. So there's only two connections.

But the router's job is to forward that data towards its destination. So when someone at home puts a packet of data bound for Google, it goes to their router, and the router sends it to the ISP. The ISP's network looks at the packet's addressing and says, oh, okay, it goes to an ISP router. Now, a big ISP router will have an octopus of connections. It'll be connected to many other routers, not just one other network, many other networks. And so it uses its routing tables to send the packet towards Google.

And this is where the robustness and the strength of the Internet comes from is it's inherently redundant. There are many routes to get to Google from any given place. But there's typically a best one, and so the router will try to use that. If that link happened to be down at the moment, the router would go, oh, and use a next-best route, maybe off in another direction that would then loop back around and eventually get there. So that's how this works. It's an interconnected set of networks that are connected to each other. That is, the interconnection points, you think of sort of like a spider web where the points that the web comes together there's a router there. And the router isn't very smart. It knows just enough to route that data in the proper direction.

Now, there's an interesting phenomenon that occurs, which is, as you get closer to Google, more of the traffic which is being carried by routers will be Google's, as a percentage. If you think about it. Because the Yahoo! traffic, that went off in a different direction. And the Microsoft traffic was headed to Redmond, and the Apple traffic was to Apple's farm, their datacenter in Cupertino or wherever. So the idea is that, with each of these hops, as they're called, across the Internet, the packet is getting closer to its destination. And if you think about it, the percentage of traffic that that router is carrying or forwarding will tend to be concentrated toward, for example, its destination, Google. There will be no Yahoo! traffic if Yahoo!'s routers and their datacenter is off in a different direction. That will have been sent out other links. So there's a concentrating phenomenon.

And the other thing that's interesting is then to ask yourself about the question of ownership. Who owns this data? And again, I don't know, from a legal standpoint. I'm coming from a technology standpoint. But this is still the public Internet. It was the public Internet when it was on your ISP, I mean, it was their network. But the way this all works globally is everybody with connected networks has agreed to provide transit for, to carry everybody else's traffic. So they just said, okay, I'll carry yours, if you'll carry mine. And that's the way the Internet works.

But the packet that a user generated is just this little blob of bits that has an address, a source and a destination IP, the Internet protocol address that is used to send it towards its destination. And so the wires that the packets are moving over belong to the public or private carriers of the data. But the data is sort of - it's public. I mean, you've lost control of it. You've put it on the Internet, and it's gone. So, well, we'll come back to this because it's an interesting question about what this means that what I think it's very clear the NSA has done.

Now, as Leo mentioned a minute ago, back in '07 there was a lawsuit, and I have not had any chance to do any deep research on the lawsuit because it really wasn't relevant to this. But it was about, I think, some privacy complaint that someone had. Testimony was given in deposition of a technician who worked in a facility at 611 Folsom in San Francisco. And Leo, I provided a link to a PDF to you. If you put up the image there, that's useful. I'm just going to read what the EFF's page has. They summarized this, and it is - it's another piece of this puzzle [www.eff.org/NSA-spying].

Leo: This was, by the way, another whistleblower.

Steve: Yes.

Leo: So unfortunately, this is what often has to happen is somebody has to step forward, say I have knowledge of this. This is an employee, I think, of AT&T.

Steve: Yes. And in fact, a few seconds ago, while you were telling people about proXPN, I tweeted five bit.ly links to a set of documents, including the redacted testimony for national security reasons that this comes from [bit.ly/sn408a, bit.ly/sn408b, bit.ly/sn408c, bit.ly/sn408x, bit.ly/sn408y]. So the full testimony is available with photos of the door of the room I'm going to be talking about in a second.

Leo: Amazing.

Steve: "AT&T's Internet traffic" - I'm reading now from the EFF's summary of this. And this is titled "AT&T's Role in Dragnet Surveillance of Millions of Its Customers: AT&T's Internet traffic in San Francisco runs through fiber-optic cables at an AT&T facility located at 611 Folsom Street in San Francisco. Using a device called a 'splitter,' a complete copy of the Internet traffic that AT&T receives - email, web browsing requests, and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service from people who use another Internet service provider - is diverted onto a separate fiber-optic cable which is connected to a room, known as the SG-3 room, which is controlled by the NSA."

Leo: By the way, this is not cellular data. This is not phone calls. This is ATT as an ISP.

Steve: They - yes.

Leo: It's important because the ISP is the - you mentioned collection point. The ISP is the collection point for everybody. Everything you do goes through that ISP.

Steve: Yes. And the way the Internet is organized in a hierarchy is we have so-called Tier 1 providers like Level 3, like Deutsche Telekom, like AT&T, the really big carriers like Sprint. These are - and there's, like, I think there's a small number, 20, maybe it's 12 or 25. I can't remember the number exactly. But there's a relatively few. And they're sort of the - they're the networks that straddle the globe; or, for example, maybe an entire country. And then they resell connections to their network. They resell bandwidth to Tier 2 providers, then to Tier 3 providers in a hierarchy. So what this is, this is a fiber-optic tap using a splitter in the Folsom building in San Francisco that makes a copy of, essentially receives a copy of all the data passing along this major trunk of AT&T. And it goes into this SG-3 room which, as EFF writes, "is controlled by the NSA. The other copy of the traffic continues onto the Internet to its destination."

Continuing to read from the EFF document: "The SG-3 room was created under the supervision of the NSA and contains powerful computer equipment connecting to separate networks. This equipment is designed to analyze communications at high speed and can be programmed to review and select out the contents and traffic patterns of communications according to user-defined rules. Only personnel with NSA clearances - people assisting or acting on behalf of the NSA - have access to this room.

"AT&T's deployment of NSA-controlled surveillance capability apparently involves considerably more locations than would be required to catch only international traffic. The evidence of the San Francisco room is consistent with an overall national AT&T deployment to from 15 to 20 similar sites, possibly more. This implies that a substantial fraction, probably well over half, of AT&T's purely domestic traffic was diverted to the NSA. At the same time, the equipment in this room is well suited to the capture and analysis of large volumes of data for purposes of surveillance."

Now, this came from sworn testimony by Mark Klein, which he gave under oath on the 26th of May, 2006, so a few years back. And this is lengthy, I'm not going to go over it, but there are a few points I want - I'll just give you a sense for it. He says, "I, Mark Klein, declare under penalty of perjury that the following is true and correct: I am submitting this declaration in support of Plaintiff's Motion for a Preliminary Injunction. I have personal knowledge of the facts stated herein, unless stated on information and belief, and if called upon to testify to those facts I could and would competently do so. For over 22 years I worked as a technician for AT&T Corporation, first in New York and then in California. I started working for AT&T in November 1981 as a Communications Technician." Okay, and blah, blah, blah.

So he's been put in - he became involved in the installation of this room that we were just reading about. It says: "AT&T Corp., now a subsidiary of AT&T Inc., maintains domestic telecommunications facilities over which millions of Americans' telephone and Internet communications pass every day. These facilities allow for the transmission of interstate or foreign electronic voice and data communications with the aid of wire, fiber-optic cable, or other like connections between the point of origin and the point of reception."

He says: "Between 1998 and 2003 I worked in an AT&T office located on [and then it's been redacted] in [redacted] as one of [redacted] computer network associates in the office. The site manager was a management level technician with a title of [that's redacted], hereinafter referred to as FSS #1. Two other FSS people [blah blah blah]." He says: "During my service at the [redacted] facility, the office provided WorldNet Internet service, international and domestic Voice over IP," so forth and so forth.

I'm going to skip down, and he says: "In January 2003, I, along with others, toured the AT&T central office on Folsom Street in San Francisco, actually three floors of an SBC building. There I saw a new room being built adjacent to the 4ESS switch room where the public's phone calls are routed. I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room. The regular technician workforce was not allowed in the room.

"In San Francisco the 'secret room' is Room 641A at 611 Folsom Street, the site of a large SBC phone building, three floors of which are occupied by AT&T. High-speed fiber-optic circuits come in on the eighth floor and run down to the seventh floor, where they connect to routers for AT&T's WorldNet service, part of the latter's vital 'Common Backbone.' In order to snoop on these circuits, a special cabinet was installed and cabled to the secret room on the sixth floor to monitor the information going through the circuits. The location code of the cabinet is [and he gives a number] which denotes the

seventh floor, aisle 177, and bay 04.

"The secret room itself is roughly 24x48 feet, containing perhaps a dozen cabinets including such equipment as Sun servers and two Juniper routers, plus an industrial-size air conditioner. Plans for the secret room were fully drawn up by December 2002, curiously only four months after DARPA started awarding contracts for TIA," whatever that is [Total Information Awareness]. And then we have two photos in this deposition, photos showing the room.

And then he says: "While doing my job, I learned fiber optic cables from the secret room were tapping into the WorldNet circuits by splitting off a portion of the light signal." And that's why the program is called PRISM, Leo. What does a prism do?

Leo: Oh, it splits a light signal.

Steve: It splits light. "I saw this in a design document available to me entitled 'Study Group 3, LGX/Splitter Wiring, San Francisco,' dated December 10th, 2002. I also saw design documents dated January 13th, 2004 and [blah blah blah] which instructed technicians on connecting some of the already in-service circuits to the 'splitter' cabinet, which diverts some of the light signal to the secret room. The circuits listed were the Peering Links, which connect WorldNet with other networks and hence the entire country, as well as the rest of the world."

So here is what NSA has done. This is installed in San Francisco. The NSA has installed this technology, this PRISM fiber-optic tapping/splitting technology, just upstream of all of those companies named. It is absolutely true that they probably never knew about it. They may be finding out about it for the first time, listening to this podcast. And I imagine it will suddenly all make sense to them. The NSA has said they had direct access to these companies' servers. Well, and that's the funny thing, the thing I noticed when I realized what was going on is that "server" is the only word anyone knows. My mom knows the word "server." Mika Brzezinski on "Morning Joe" knows about the AOL server or Google's servers. That's in the common parlance.

The word that we should have been using is "router." And that's not a word that people understand. But that's the key to this technology. As I was saying, routers concentrate data. Somewhere, and the NSA knows exactly where it is, Google is buying their bandwidth. And there are routers upstream of Google whose purpose it is to take the disparate packets all coming into Google and route them down fiber-optic lines which finally make the transit into Google's data center. It is unnecessary to have access to the datacenter if you are tapping the fiber-optic line going into and out of the datacenter.

Leo: Okay, but isn't this encrypted traffic?

Steve: Ah. Well, yes and no. So some of it is encrypted. But, for example, how is this useful? We all know that email has never been an encrypted technology. Email SMTP does not involve encryption when we send email from place to place unless an individual deliberately encrypts their email. And even if you were using Google, you may have a secured SSL connection to Google's web server when you're using Gmail. But the moment that email leaves to go to your mom on AOL, or it goes anywhere else outside of Google, it is being sent over SMTP connections which are not, that is, SMTP protocol, which is not encrypted. So even whereas our interchange with Google on their website is

encrypted, email transiting the Internet isn't.

So all email outbound from Google is fully readable, and all email incoming to Google is fully readable. It's certainly true, and our surveillance state is unhappy with the growing use of encryption. But a huge, a vast, still the majority, arguably, of data is not encrypted. And then there is other sorts of metadata. We've talked about this on this podcast, for example, DNS queries. When you go to a website, your system has to query a DNS server in order to get the IP address. Well, that's typically not encrypted unless you use the service that OpenVPN offers.

So what we have is we have this system called PRISM. We have this bunch of companies that are absolutely sure that they have never agreed to blanket eavesdropping/wiretapping with the NSA. And I believe them. If the NSA had reason to specifically require data that is specific to a given case, we already know they go to a court, they get a warrant, and under a bond of secrecy they're able to get the data that the company has, if any, and the company is bound not to say it.

I don't believe that's what's going on. The fact that this is called PRISM, the fact that a prism splits light, the fact that we know from this prior testimony that there is a facility on Folsom that the NSA has been doing this - in fact, further on his testimony he quotes the specific routing technology, the gear that's being used. There is a semantic analysis technology. I don't know if I can find it here on the fly. But I just tweeted all the documents that contain this information for anybody who's wondering.

Anyway, I am convinced, from everything that I've seen, that - oh, also the timeline. This is not something you can do instantly. This is going to take time. So what it looks like from the timeline that we saw in one of those slides, where individual corporate entities were added to the PRISM project one at a time, that fits the facts, too. The idea that the NSA would say, okay, now we want to get everything, all of Apple's traffic we want to tap. Essentially what we have is wiretapping of these companies.

Now, remember that I don't know legally where this stands because this is the Internet. You could argue that, if somebody was installing, surreptitiously installing equipment inside Google's facility, well, then it's under Google's control, and it's Google's. All the NSA is doing is tapping the communications, which is still the Internet, it's just been filtered down so that it's nothing but Google's traffic.

Leo: So all they really need to do is find the backbones, the big Tier 1 providers. And you say there are about eight or nine of them? Or how many are there?

Steve: Well, no. What you need is, where you need to place the tap is as close to Google as you can get, or as close to Microsoft, or as close to Yahoo!, because you don't want a lot of other extraneous traffic. You want to get all of that.

Leo: I want it all.

Steve: Yes.

Leo: Okay. So would it have to be in Google's facility?

Steve: No. It would be - so, no. Google's going to have fiber that is going to be fed from their provider. Google is buying bandwidth from somebody.

Leo: Let's say it's Level 1. We don't know.

Steve: Level 3.

Leo: Or Level 3, I mean.

Steve: Yes.

Leo: Actually, let's say it's Level 1.

Steve: Okay, good.

Leo: Somebody called Level 1.

Steve: Somebody innocent.

Leo: So you would then go, as the NSA, to Level 1, issue them an NSL, a National Security Letter, which means they can't speak.

Steve: Yup.

Leo: And say we want to - we're just going to plug this little thing into your router. Can you give us a room?

Steve: Yes. We need, yes, we need a secret room, and we're going to staff it with our own people. Oh, at one point the air conditioning, the air conditioner's condensation tray overflowed and was spilling water in the secret room, and it was dripping down to the floor below, so that caused some problem. I guess they hadn't quite figured out how to drain the air conditioning condensate. But, yeah, so give us a secret room. So go ahead, Leo. I want you to restate it.

Leo: No, well, I think that you've answered my question. So they go to the Tier 1 provider, the Level 1 or whoever it is, and say give us...

Steve: Well, no, they go to the bandwidth provider of the company they're targeting. So it's not Tier 1. It might be Tier 3. I mean, it's like...

Leo: Aha.

Steve: Because it's going to come down the hierarchy until it gets to the entity they want to tap.

Leo: And you don't need to tell Google about this.

Steve: No. Google would have no idea.

Leo: And this gives them plausible deniability. They may know about it, but they may just - this gives them plausible deniability. No, no, they don't have access to our servers.

Steve: No, I think they'd be furious, Leo. They're being - this is a wiretap on...

Leo: Yeah, but surely they've figured this out.

Steve: Well, I haven't heard about it anywhere in the news. Nobody else seems to have figured out what PRISM is. And there is - this fits every fact. It's why it's called PRISM. They're using fiber-optic cable splitting. And it fits the whole timeline. They didn't just, bang, do it all at once because it's going to take time. They're going to have to go to the individual carriers who are providing bandwidth to these companies who are - and, I mean, the only thing Apple and Google and Yahoo! represent are major social focal points.

Leo: Right.

Steve: And actually, by tapping those major carriers, those major companies, the NSA is minimizing the work that they have to do because most people are going to use Google or Yahoo! or AOL and Apple and so forth.

Leo: There's precedent for this because remember Carnivore, which was renamed after they realized it was a terrible name, which was the FBI's attempt to get every Internet service provider in the country to put a box in their - again, another focal point. In fact, the best place to collect all this stuff is at the ISP level. And for individuals you can get it in every respect. And there's never really been any proof that this didn't happen. And then of course there's the recent law which was not passed, but might well still be, requiring ISPs to collect 18 months of data for use.

Steve: Well, so, again, I'm...

Leo: This all makes perfect sense. It's exactly how they're operating, and in fact the most efficient way to do it.

Steve: Yes. Yes. This is - if the NSA had come to me and said, Steve, what should we do?

Leo: How would I do this, yeah.

Steve: This is what I would design. I would design this system. I would say, you want to get, you know, if you need to be - you need to keep this a secret. You want to get all the traffic coming in and out of Google. You get as close to Google as you can. You get on the router that is feeding Google, and you clone all of the data. And that's exactly - and that's why it's called PRISM is that now, at this bandwidth level, they're using fiber optic cables, so it splits the light. The power drops by 50% down each of the splits because the power of the light has been split, but that's - there's still plenty. And so it's going to be received easily by the other end. And then it goes off to this secret room controlled by the NSA.

And it also fits what we heard because there was - we heard that there was this notion, I mean, we heard of PRISM, that you can - or maybe it was Edward who said that you could task this equipment to find things. So they're - so an analyst...

Leo: Wow, smarter than just a collector, it's actually sifting.

Steve: Yes, yes. And I'm looking here, if you see the link, it's klein-decl. It's cryptome.org/klein-decl.htm. So it's Klein Declaration. In there he shows the documents about installing the splitter, how to split it, all of the technical details. And he does cite the name of the company providing this - they call it "semantic analysis" equipment. So the idea is that an analyst sitting in Langley is able to task the Google tap to select, I mean, this is a torrential flood.

Leo: Remember, this was years ago, though. And I would guess now, because they have such high-end storage and processing, they probably just send it all to the center; right?

Steve: Well, they're readying five zettabytes.

Leo: Yeah, they'll end up sending it to Utah.

Steve: So why filter it? We may miss something we want.

Leo: Right. Well, precisely.

Steve: Let's just suck...

Leo: Save it all.

Steve: Yeah, suck it all in.

Leo: You never know what you might want.

Steve: Yup. And again, having the history allows them to go back and do research on the past.

Leo: So let me - let's get clear, though. What is it that they have? This is no longer metadata. This is all data that isn't encrypted.

Steve: Yes. So, yes. So, now, at this point, as far as we know, the use of SSL encryption will withstand the NSA's attack.

Leo: But they're saving it anyway, just in case.

Steve: Well, they're saving it because they know in the future your computers will get stronger. Maybe quantum computing technology will actually allow them to just collapse the 128-bit key. I'm uncomfortable with 128 bits. We really need to start thinking 256. And we'll talk about that soon on the podcast because the protocols exist on SSL; but, as we've spoken about the way SSL exists, both ends have to agree. And we've got all these banks out there who are scoring F's on their SSLLabs.com test because they're not using strong encryption. And so the cipher string has to be agreed to by each end.

But the point is certainly there's a percentage of data that the NSA - it is encrypted. They cannot read it. But any email coming into Google, any email leaving Google, which is to say any non-Gmail-to-Gmail communication, does exit - and in fact maybe it still goes, if it's going off to a different physical datacenter in Google, it's going to go out over the Internet. I don't know if Google maintains encryption of email traffic between their datacenters.

But anything, essentially everything coming and going in and out of the companies that were named, is probably now being tapped. And PRISM is the technology that does it. It is sitting just upstream of these companies, monitoring everything that they're doing, everything, I'm sorry, that every of their users are doing. Anything not encrypted is subject to surveillance.

Leo: Quite amazing. And what you say now makes perfect sense. I think you're right. We don't know because, A, anybody who knows probably is enjoined from saying anything by pretty strong federal restrictions.

Steve: Right. It's the only reason I can talk about it is that no one there told me

anything, yes.

Leo: But what does make sense and I think is interesting is this is probably too technical for most lay observers to deduce. So they say "have full access to servers." And while Google is certainly, you know, the engineers at Google are certainly smart enough to understand that this is the risk, they're not allowed to say anything anyway. So they're going to say only what's strictly, you know, that they're allowed to say that's strictly true, which is they don't have access to our servers.

Steve: Yes. And it's absolutely true. They do not. Unfortunately, they have access to the pipe connecting your servers to the rest of the world.

Leo: They don't need access to your servers.

Steve: Yes, exactly. And it's funny, too, because the press, in trying to explain this discontinuity between the formal statements that were immediately issued by these companies, they were saying, well, they're parsing their words very carefully, or they've got really good attorneys. It's like, no. They're absolutely not complicit in this. The NSA has installed a tap in their connection to the Internet. And the tap, I'll say again, it's on the Internet. I mean, I don't know about the legality of this, but I was chuckling to myself because the NSA is doing this deliberately. Google did it by mistake when they were collecting unencrypted WiFi with their mapping technology.

Leo: Right, right. Well, so if you want to explain this to your grandma or a layperson, it's really something that I think any layperson can understand. You just say it's an upstream tap.

Steve: Yes.

Leo: They're tapping the Internet, and as a result they're getting...

Steve: Where it connects to the company.

Leo: To these companies.

Steve: Yeah.

Leo: And for all we know they're also tapping it where you connect to the Internet. So they can get you coming and going if they want.

Steve: Well, yes. They would, see, again, being sympathetic to the need for intelligence, I get it that they chose these companies because they are major focal points. So a tap located there would give them the most bang for the buck.

Leo: And the reason we know these companies is this is one of the slides in that slide deck that Snowden released.

Steve: Yes.

Leo: However, I have to think that really it goes much wider than this because, if you're going to Level 1, you might as well just say who else connects through you?

Steve: Well, Leo, we already know because the article that I read was an AT&T facility. This was tapping the so-called backbone. This is the - remember that the way these - at the very, very top we have the so-called Tier 1 providers. And they have what's called peering relationships with, like, so, like Level 3 and AT&T and Sprint have peering relationships with each other, where they are, because they're peers, and so they agree that they will send traffic to each other. What we read in this testimony and on this EFF page is this was the peering pipe at AT&T going to its peers.

Leo: So they did it. This is how they did it.

Steve: Yes. This is the entire Internet being tapped.

Leo: Yeah. If you were a WorldNet user in 2007, they were listening.

Steve: Yeah. Or, if you happen to be at two distant locations, and your traffic goes through AT&T on its way to another network, then it's present there. And I just - there's one more comment I wanted to make that I thought was - I felt, I mean, I understood it, and that is that Europe is very unhappy over this. We're sitting here, and the NSA is saying, and I don't believe them because how can I believe them now, they're saying we're only, I mean...

Leo: No, that's obviously not...

Steve: I mean, their great caveat is that they're only looking at foreign people.

Leo: Well, that's all they're technically allowed to look at.

Steve: Well, and that's nonsense.

Leo: By their charter, yeah.

Steve: Yes, that's nonsense. But even so, that means they're looking at everything outside the U.S. Well, that's half of this podcast's listeners, Leo.

Leo: And the FBI has the charter to do inside the U.S. and is presumably doing this with the help of the NSA.

Steve: Well, and I saw a little blurb yesterday that said that the "Finnish communications minister, Pia Viitanen, has stated bluntly that the NSA may be breaking the laws of Finland. According to the Finnish Constitution, capturing and reading emails or text messages without privileges is illegal."

Leo: I think it's illegal in the U.S.

Steve: "Viitanen plans to take up the issue with the European Commission."

Leo: Wow.

Steve: "Several European countries are apparently considering unleashing Neelie Kroes..."

Leo: Oh, she's great.

Steve: "...the feared European Commissioner for Digital Agenda, in an effort to fight back against the NSA's PRISM program."

Leo: Don't mess with Kroes, that's for sure.

Steve: So hide under a desk.

Leo: Oh, wow. The mind reels.

Steve: And lastly...

Leo: Yes, go ahead.

Steve: Lastly, in reaction to this, a site has been put up that immediately, along with the EFF - stopwatching.us. Stop Watching Us. It's taking signups. There are 63 companies that have already, or organizations that are behind this. And so I suggest that anybody who's interested - they've got a really crappy security certificate. I was disappointed in the security certificate for the site because it's an HTTPS site. I would like to see something better there. But stopwatching.us is someplace that anyone can go who's interested.

And Jon Stewart is off for the summer directing a movie, so John Oliver is standing in for

"The Daily Show" on Comedy Central. His opening piece Monday night [June 10, 2013] was wonderful. Basically summed up the political side of this with the typical "Daily Show" comedy. So I wanted to recommend that to our listeners. It was really terrific. So if you can find "The Daily Show" for Monday, which would have been, what, the 10th of June, the beginning of it with John Oliver as the guest host, filling in for Jon Stewart, was great.

And, yes, Leo, you're right, the mind reels. But at least now we know what's going on.

Leo: The next step I would like, and maybe we'll do this on Know How, maybe you can do it, too, is telling people some simple steps you can take to encrypt your email, encrypt your traffic. If you really, I mean, you can't hide who you're sending it to because that has to be public, otherwise it won't get there, although I guess you could use Hushmail or something like that and have private addresses, as well. But I think this, you know, for a long time I used PGP and encouraged people to send me encrypted email. Nobody ever did it.

Steve: Here's what's interesting is the polls came out yesterday morning.

Leo: 56% of Americans don't care.

Steve: I saw 62, 62 versus 34% of Americans say they are okay with this.

Leo: Because it's protecting us against terrorism.

Steve: If it protects us against terrorism.

Leo: Right.

Steve: And then there's always the conundrum, well, if you don't have anything to hide, what do you care?

Leo: I even heard a federal official say that this week, that nobody who's a law-abiding citizen should worry about this.

Steve: So I was very annoyed that Google got in the trouble they did for inadvertently collecting unencrypted WiFi which was being broadcast to them in the air, when here we have the NSA that has used prisms to split the optical cables going to these major companies to install local taps. It's just there's something wrong there. I understand the NSA's need for the data, but - in order to find bad guys. But they have to tell the truth. I mean, they have to tell Congress the truth. They don't have to tell me or you. They have to tell Congress because that's the only way that we have checks and balances.

Leo: Well, and they may. They may have told the House Foreign Intelligence, and they may have told people this. It's my suspicion that some lawmakers, not all, know about it and have approved it. And I think this is the problem is that people want to be safe against terrorism and understand that this has to be done. And I think the fear is, if the federal government admits to this, then the bad guys go, oh, well, that's no problem, we'll just use Cryptocat.

Steve: Well, here's what's really interesting, too, is imagine that you have the dragnet over all phone communications, all telephony metadata. And three clever terrorists say, oh, well, we're going to avoid the system. We're going to get so-called "burner" phones, you know, temporary phones. And we're never going to give the phone number out. We're never going to dial any other phone except these three. And we're only going to use it to talk to each other. Well, how suspicious is that?

Leo: You immediately know.

Steve: Yes.

Leo: Big red flag.

Steve: The NSA would find three little nodes with lots of connections among themselves, but nobody ever phoned into them, and they never phoned out to anyone else. There's a little island there, and that's something to look at. So this is phenomenally powerful, this so-called metadata, powerful information. And as far as I know, Leo, this podcast is the first disclosure of what the NSA's PRISM program is, that it is a tap, an optical fiber tap on these companies. I don't know what results from this. But I imagine now Congress will know how to ask some better questions.

Leo: I hope so.

Steve: And these companies will probably want to find out if this is going on.

Leo: Yeah. Steve Gibson is at GRC.com. That's his website, if you want to spy on him. He gives away many, many wonderful security tools including ShieldsUP!. Make sure you check your Plug & Play status there with the ShieldsUP! program. Make sure your router isn't releasing information to the outside world or access to your inside network. You can also get SpinRite. That's his bread and butter, the world's finest hard drive maintenance and recovery utility. And for people with bandwidth issues, the 16Kb version of the show. And if you would like to send a transcript to your elected officials, that might not be a bad idea, and those transcripts are made by Elaine Farris and made available on Steve's site as well, GRC.com.

Steve: Elaine's a little under the weather at the moment.

Leo: I'm sorry, Elaine.

Steve: She didn't know when we were going to get the audio; but, if it came in time, then she thought she'd be able to start on it. So anyway, the point is that we will have full textual transcripts of the podcast in all of its glory a couple days from now, posted on GRC.

Leo: Good, good. You also can go there to ask questions. And we will do a Q&A episode.

Steve: Yup, I imagine we'll have lots of questions. And we'll probably still be talking about this next week.

Leo: Yeah. And that will be GRC.com/feedback, if you'd like to pose a question to Steve Gibson. We've mentioned before he's on Twitter @SGgrc. Follow him there.

Steve: I was just going to say that I just tweeted five bit.ly links to these documents, to some PDF forms and these redacted and redaction-filled-in documents that exist on the 'Net. If anyone's interested in additional information, I mean, it just - it's riveting stuff, really interesting.

Leo: Yeah, it really is. Thank you, Steve Gibson. We do this show every Wednesday. You can find us right here at 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 19:00 UTC on TWiT.tv. Do watch live. Lot of fun. And you're welcome to visit us in-studio, as well. We always have visitors. People love to see you live, Steve. But if you can't, we always have on-demand audio and video after the fact, not only on Steve's site, but high-quality audio MP3s and video, as well, available at TWiT.tv/sn, or wherever you get your podcasts, like iTunes.

Steve: I think I'm going to be up maybe in August.

Leo: Ooh.

Steve: I think Jenny's going to come up to do her regular summer visit of friends, and I thing I'm going to come up, and I'm planning to synchronize it with a Wednesday so I can do the podcast in-studio with you, Leo.

Leo: Great. That would be a lot of fun.

Steve: Yeah, it would be.

Leo: I look forward to that. And I'll buy you...

Steve: Okay, my friend.

Leo: Dinner's on me. Or lunch.

Steve: Okay.

Leo: Thanks, Steve. We'll see you next time...

Steve: Thank you.

Leo: ...on Security Now!.

Copyright (c) 2012 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/