How Much Tinfoil?

Description: Though regularly scheduled to be a Q&A episode, Steve and Leo had SO MUCH to cover in the week's news that there was no time left for questions. We'll save those for episode #415 and this week enjoy a great discussion of the week's many events. We'll wrap up with a discussion of the wide range of "tinfoil" solutions available and their convenience versus security tradeoffs.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-413.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-413-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got some tech news, security news. But we'll also take a look at how much tinfoil you need to wear to protect yourself in light of the revelations about the government's spying. "How Much Tinfoil?" next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 413, recorded July 17th, 2013: How Much Tinfoil?

It's time for Security Now!. Help me. The show that helps you stay safe online. There's never been more need for Security Now! than right now. Here he is, the Explainer in Chief himself, from the Gibson Research Corporation, creator of SpinRite, coiner of the term "spyware." And, boy, I hope your ears are burning on TWiT. Steve Gibson, Ed Bott was singing your praises on TWiT this week. I don't know if you heard it yet.

Steve Gibson: Really. No.

Leo: Yeah, you've got to go back and listen.

Steve: Wow.

Leo: So I - we both know Ed for many years, Ed being chief of PC Computing and just a great guy.

Steve: Yeah.

Leo: And he has been looking into, of late, a pernicious practice that we've talked a little bit about, but that really came up on Sunday's radio show. A fellow called up, said I have this - my browser's been hijacked. My home page is hijacked, my search engine hijacked by this tool. And I got it from CNET's Download.com. And I said, well, that can't be. And then we looked into it, and the chatroom said, oh, yes, it can. And Download.com, like a lot of other free download services, has been wrapping some of their downloads with their own software that asks you, although you may not pay much attention to the ask, is it all right if we change your home page, change your search engine, blah blah blah. And if you say okay, it will.

Steve: Yeah.

Leo: Same things...

Steve: Well, I mean, if you don't say no.

Leo: Well, that's right, because it's opt-out, not opt-in.

Steve: Right, right.

Leo: So you have to uncheck those boxes, which most people don't do. And Ed said, yeah, I've been studying this, and it's gotten to be a real problem. In fact, Oracle with Java has gotten even worse now. You know they install the Ask Toolbar. And they ask you - and I'm very curious about this checkbox on here. When you're installing it, they say it will now and forever change your search engine [laughing]. And Rafe Needleman on his Google+ said, what is this change in verbiage, and what are they trying to say here? Let me show you, I'll show you the...

Steve: Wow.

Leo: Yeah. So Ed said - well, and here's where you come in. Ed said, "And Steve Gibson warned us. He has been a voice crying in the wilderness about all of this stuff for a long time. And, you know, people should give him credit because this guy has been talking about this forever." So here's the - Rafe Needleman put a screenshot of this. It says install - the two checkboxes, and of course they're checked by default. Install the Ask Toolbar in Google Chrome, and then set and keep Ask as my default search engine, which implies that it will then take steps to make sure you don't change it back, or nothing else changes it back. Can you believe that?

Steve: Yeah. The problem is, Leo, there is so much money now behind these things.

Leo: Exactly.

Steve: Mark Thompson was telling me he was experimenting with wrapping some of his freeware in one of these things, where it's opt-out, but still it's being promoted. And I get email solicitations all the time from these people. And sometimes they start phoning. And I go, look, get this through your head. I am never doing this.

Leo: Good for you.

Steve: Never. Remove me from whatever - I don't...

Leo: How much money? What are we talking about, though? I mean, it must be a lot.

Steve: It's serious money. It is serious. It's like shocking how much money, if you have something that's being popularly downloaded, because all they need is some percentage of people to get this thing in their machine, and then they've achieved their mission. And it's like, oh, it's just bad. And the Ask Toolbar, they just want it on people's browsers. And they will pay the people who convey it into the browser. You get a piece of the results. And it is - you have to have no commercial orientation in order to resist it, to say no, I'm not doing that.

Leo: Right. And he was saying, unfortunately, shareware authors aren't making what they used to.

Steve: No. And one of the things that I've noticed is - I'm sure you have, too, Leo - is every so often I go looking around for something, like I'll need to convert a whole bunch of AVIs to MP4s or, you know, something, some random sort of thing. All of what used to be even the reputable download sites, they are now impossible to navigate. They're like, unless you are very careful, you end up going off on some sideline and downloading something you didn't want. And, I mean, it's all now about upselling us and actually making money rather than offering a service of making files available. It's sad.

Leo: He recommended a couple of tools, one called PrivacyFix. I don't know if you're aware of this one. It's kind of interesting. And one of the things PrivacyFix tells you is what you're worth to various companies. According to PrivacyFix...

Steve: [Laughing] I've seen that.

Leo: ...I'm worth 123 bucks a year to Google.

Steve: That's real money.

Leo: So you're right, it is real money. If these companies can get you to use their stuff, they're making a lot of money. And even if they pass 10% along to the authors, I can see why they - they do it.

Steve: Yeah. Times however many of your users are involved in downloading their thing. I mean, it ends up being serious. It's significant. Ugh.

Leo: Ed talked about Abine Online Privacy and PrivacyFix.

Steve: Yup.

Leo: Abine's been bought by a massive, I think it was a web advertising company. So...

Steve: Oh, boy.

Leo: But PrivacyFix is still kind of an independent - and I have to say it's pretty impressive, at least just to install it - it's a Chrome plugin - and see, and just see. It shows you who's tracking...

Steve: How you're being monetized.

Leo: It's kind of like Ghostery. He recommended Ghostery, which I know you've recommended before, that I already knew about. Anyway, he gave you serious props for being a voice in the wilderness for many years. And he said that's the problem is this stuff starts innocuous, but it gets worse and worse and worse.

Steve: Yup.

Leo: And it's now in the getting worse stage.

Steve: Yeah. If it's wrong, it's wrong.

Leo: Wrong is wrong.

Steve: And it's not about scale, it's about some things are absolute. And if it's wrong, it's wrong.

Leo: Yeah.

Steve: It's like third-party tracking. It's wrong. And now we're going to start seeing it getting worse.

Leo: Yeah. I have to - I may correct myself on the Abine thing. I'm not sure. I'm trying to remind what he said about it.

Steve: Well, I did get a nice note from an Adblock Plus developer who said, Steve, we need to correct the record. So that's one of the many things we're going to talk about this week. Are we recording, by the way? Did we start?

Leo: Oh, yes. Welcome to Security Now!. Yeah, we started.

Steve: Oh, good.

Leo: I just thought I'd throw in a unit of my own. But mostly just to...

Steve: No, I'm glad.

Leo: Sincere props from Ed Bott, who is one of the great guys in the business and, like you, wears a little tinfoil from time to time. And I guess that applies to the topic of the day: How Much Tinfoil?

Steve: Well, this was nominally scheduled to be a Q&A. But the big news that dropped the day after last week's podcast - it always seems to be now timed to be the day after the podcast something huge happens. But that's good because it allows dust to settle. It allows people to weigh in. And this was important in this case because Microsoft has just gone ballistic over the Guardian's most recent news, which was a point-by-point enumeration of Microsoft's complicity - complicity? Complicit. Complicity. They're complicit, I know that.

Leo: [Laughing] Complicitousness. I don't know.

Steve: Complicitousness. See? It's a problem.

Leo: Yeah, it's not a good word.

Steve: No, I should have come up with an adjective form, then I got stuck. With the, of course, with our good friends at the NSA.

Leo: Compliant.

Steve: Compliance, okay. Anyway, so we have to talk about that. And then there was all kinds of other news. And I just realized as I was beginning to put this together, I mean, the PDF of my notes is more than twice as big as our normal PDFs. When it took a while to upload it to you on Google, I thought, what - how big is this? And I checked, and it's 213K. Normally they're about 100K. So anyway, because there's so much to talk about, I thought, well, there's no way we're going to get to any questions. So I downloaded 327 of them, but then I thought, okay, we'll just cover those in two weeks.

But after all the week's news, I thought, let's talk about how much tinfoil we really need. Because what we're seeing is, we're seeing sort of - there's a spectrum of things people can do to protect themselves. And if you just don't care, use SkyDrive and Google Drive and let your files be there. Or, you know, Gmail with no other protection. But then there are - I really believe there is a midpoint between the absolutism of you must read the open source and compile it yourself - there's a midpoint. There are people who are explicitly on our side. Microsoft is not. I mean, that much is clear.

But there are people, and we've been talking about this, like the Hemlis folks and Threema and, you know. Anyway, so we're going to talk about sort of where I think it makes sense to be, for people who care about privacy and security, short of the - I mean, like, working with people who have what I would call an open agenda, where it's clear why they're doing what they're doing. BitTorrent Sync is another example. So there are many good things people can do that back away from not caring at all. But, yeah, they don't really meet your criteria, Leo, of being open source, but I would feel comfortable using them. So the question is, how much tinfoil do we need?

Leo: Excellent. And some recommendations, it sounds like, for things we can do.

Steve: Yeah, yeah, yeah.

Leo: Yeah. And I want to ask you, well, we talked before the show, but I want to ask you about - I read that Edward Snowden used a particular email service, and I wanted to ask you about that. But...

Steve: Actually, that's already in our topics for the week.

Leo: I know, I know, I know. So we'll hold onto that. That's coming up in a second. All right. Let's get going, Stevie G.

Steve: Yeah. Just a real quick note, following up on last Tuesday's Patch Tuesday. Microsoft had some problems with their patches. Apparently there were three different patches that had problems, but two of those three were very obscure. One, though, is causing lots of problems. So I just wanted to mention it briefly in case any of our users, our listeners had encountered it and were puzzled. And the symptom - it was a patch in Media Player codec DLLs which caused, for whatever reason, the upper half of the video image to stay black. So this is...

Leo: That's a problem.

Steve: Yeah. This is MS - unless everybody's down in the second half of the frame waving to you. Then you're okay. But this is MS13-057. That's the bad one. And Microsoft has not yet acknowledged that this is a problem, but everyone understands it is. It's been spawning all kinds of complaints all over the Internet, that the top half of videos are displaying in black. So if that's a problem for you, wait for them to fix it, I would say, is probably best. If you can't, then you may be able to uninstall that one. It's based on the Knowledge Base 2803821, which covers that. And so they were trying to fix a malicious video problem where someone could deliberately malform a video and install malware through your Media Player. They apparently did fix that, but at the cost of your Media Player working correctly. So, oops. Anyway.

The big news dropped the day after last week's podcast, which was Glenn Greenwald at the Guardian has kept saying that there is more coming. We've got a lot more documents that Edward had already turned over to us that we just haven't released yet. Well, they did another drop. And it's significant enough, and Microsoft's reaction to it is significant enough, and it's interesting to see how this plays into the theory that we've developed on the podcast of what's going on. And so I wanted to cover that. I've got a ton of people saying, oh, my god. I mean, of course all of the Linux people were saying, ha ha, you know, we haven't been supporting Microsoft for a long time.

Anyway, so what the Guardian said was Microsoft has collaborated closely - oh, and by the way, they're the first people on the timeline. If you look at that weird timeline with that strange green arrow covered up by yellow ovals, the very, very far left beginning, Microsoft is No. 1. So whatever it means that they were "participating" in the PRISM program, they were first.

So the Guardian says: "Microsoft has collaborated closely with U.S. intelligence services to allow users' communications to be intercepted." Now, so that's - that says - and in fact what I think we're going to come away with here is it's sounding like Microsoft knows they're being tapped, that is, it's still - nothing that I've seen so far violates the theory that this is an upstream tap. And what I think we're going to see is evidence of the NSA coming to Microsoft, saying, okay, we need help with what we got because we don't know how to decrypt it. So this all fits still, [Microsoft] collaborating "closely with U.S. intelligence services to allow users' communications to be intercepted, including helping the National Security Agency to circumvent the company's own encryption, according to top-secret documents obtained by the Guardian.

"The files provided by Edward Snowden illustrate the scale of cooperation between Silicon Valley" - and specifically Microsoft - "and the intelligence agencies over the past three years." And a lot of this does revolve around specifically Outlook.com, that we'll talk about here in detail in a second, and of course Skype. "They also shed new light on the workings of the top-secret PRISM program, which was disclosed by the Guardian and the Washington Post last month. The documents show that Microsoft helped the NSA to circumvent its encryption to address concerns that the agency would be unable to intercept web chats on the new Outlook.com portal. Also, the agency already had pre-encryption-stage access to email on Outlook.com, including Hotmail."

Well, that's exactly our hypothesis of what's been going on in all these programs. The company worked with - "Microsoft worked with the FBI this year," and that's in February, "to allow the NSA easier access via PRISM to its cloud storage service SkyDrive, which now has more than 250 million users worldwide. Microsoft also worked with the FBI's Data Intercept Unit" - there's an acronym for that somewhere - 'to understand,'" they said in quotes, "'understand' potential issues with a feature in Outlook.com that allows users to create email aliases." So that sounds like they were noticing people could have multiple identities, and so they said, oh, help us disambiguate these multiple identities in

Outlook.com through aliases.

"In July last year," that would be 2012, "nine months after Microsoft bought Skype, the NSA boasted that a new capability had tripled the amount of Skype video calls being collected through PRISM. Material collected through PRISM is routinely shared with the FBI and CIA, with one NSA document describing the program as a 'team sport.'" And they actually used that term, "team sport."

"The latest NSA revelations further expose the tensions between Silicon Valley and the Obama administration. All the major tech firms are lobbying the government to allow them to disclose more fully the extent and nature of their cooperation with the NSA to meet their customers' privacy concerns." And, boy, we'll get to that in a second because Microsoft has just gone ballistic over this.

"Privately, tech executives are at pains to distance themselves from claims of collaboration and teamwork given by the NSA documents, and insist the process is driven by legal compulsion. In a statement, Microsoft said, quote" - oh, and this is - we're going to get this in two different places. I love this. It says: "When we upgrade or update products, we aren't absolved from the need to comply with existing or future lawful demands." Which is legal speak for "We had to put in backdoors." They said, "When we upgrade or update products, we aren't absolved from the need to comply with existing or future lawful demands." It's like, okay.

Leo: But that's a given. I mean, let's face it. They work in the United States. You have to obey the laws of the United States. That's just the way it is.

Steve: Well, right. But so they're saying...

Leo: I mean, asking them to break the law is asking too much.

Steve: No, this is new, Leo. This is saying we are modifying our products to be able to comply with requests, rather than saying we're unable to comply.

Leo: Can you say you are unable to comply?

Steve: Yes. You could say, I'm sorry, we don't - we're happy to give you this bunch of pseudorandom noise. This is all we have. So at this point there is no law that says that encryption is outlawed, or encryption must be defeatable. All they're saying...

Leo: There was talk about that. But they never passed that.

Steve: Yes. And, I mean, that's the other shoe. I mean, that's why I aborted CryptoLink was, like, this is coming. It's clearly coming. And so I was unwilling to invest a huge amount of effort to create a commercial product that I would then have to put a backdoor into.

Leo: So put yourself in Microsoft's shoes. They might have decided preemptively, well, we might as well just do it because we're going to have to. Right?

Steve: Yeah.

Leo: They're, I mean, they're a business. And they probably wanted to avoid this issue. So they said, well, what the hell, it's for a good cause. It's to prevent terrorism. We'll do it.

Steve: So I have here this discussion...

Leo: I wish they were more forthright about it.

Steve: Yes. Well, and they're saying, I mean, they're really...

Leo: Kind of saying it.

Steve: They're really upset. I mean, they really - we'll get to that in a second because I've got a quote from Brad Smith, who's their executive VP and head of legal, who is like, I mean, they're livid over the fact that their hands are tied.

Leo: Crocodile tears.

Steve: I know. Well, you know. But consider that this is, I mean, this is clearly costing them from a business standpoint. Microsoft users are not just our listeners.

Leo: Well, and the European Union, yeah.

Steve: Oh, yeah, yeah. I mean, this is really - this is really a disaster. I mean, what we're going to see, and I'm getting ahead of myself a bit here, is that it seems very clear that the NSA came to them and said, let's work together, and don't worry, it's all going to be secret. And it's not now.

Leo: Well, but they may have also come to them and said, we're going to work with you, and don't worry, it's going to be secret. I mean, they may have said you want this Skype thing to go through? How do you feel about - we don't - I think the government has far-reaching powers that may not be fully acknowledged. And I don't think they'd be hesitating to strong-arm them and say, look, you're not going to get approval on this Skype acquisition unless you cooperate.

Steve: Oh, oh, you mean the acquisition.

Leo: Yeah.

Steve: Wow.

Leo: That's about when this happened.

Steve: Yeah. Actually, well, the work on reengineering did predate the actual purchase. But you're right, these things don't happen overnight. I mean, surely there was six months of discussion going on.

Leo: Right. Well, and Skype was not a United States company until acquisition.

Steve: Correct.

Leo: It was, I believe, was in Holland. So I don't know. I'm just saying we don't know how much pressure Microsoft was under to comply.

Steve: So the Guardian says the files that they have "show that the NSA became concerned about the interception of encrypted chats on Microsoft's Outlook.com portal from the moment the company began testing the service" last summer, July of last year. "Within five months, the documents explain, Microsoft and the FBI had come up with a solution that allowed the NSA to circumvent encryption on Outlook.com chats." So again, this is saying that the NSA is intercepting and tapping outside of Microsoft, but they're concerned that chats are going to be encrypted, and so they work out a way to solve that problem.

Leo: Gee, Skype was owned by eBay, wasn't it, before it was sold. So it was a U.S....

Steve: And wasn't it originally Israeli?

Leo: No, it was the guys who did, of all things, Kazaa.

Steve: Yeah, that's right. That's right. Yes, yes, yes.

Leo: It was peer-to-peer. And they were from Luxembourg or somewhere. I can't - anyway, non-U.S. But it was eBay owned when Microsoft bought them. You know, I could totally see the Justice Department, concerned about Skype being used and them not being able to tap it, and going to eBay and saying, look. You want to get rid of this, don't you? We can help. We're going to go to Microsoft. Let's work something out.

Steve: Oh, Leo. Oh.

Leo: Why not? I mean, you have to understand, the guys who are doing this are not doing this out of evil intention. They're doing it to stop terrorism.

Steve: Correct.

Leo: And they feel, perhaps even legitimately, that this is something they need to do.

Steve: Well, I'll bet you that they are tapping communications of known bad people who are using Skype. And they're frustrated. They're frustrated to death that they...

Leo: Well, they've talked about this a lot.

Steve: Yeah.

Leo: This is their inability to tap these new electronic communications are very concerning to all law enforcement.

Steve: The "going dark" problem.

Leo: But I think the big issue is federal law enforcement charged with fighting terrorism. And it's hard, if a guy from the FBI comes in and says - the director of the FBI comes in, says you've got to help us fight terrorism. It's hard to say no.

Steve: I, yes, I completely agree with you.

Leo: Do you want to be the company that then the director of the FBI says, oh, by the way, we got no cooperation from these U.S. companies. And as a result, this terrorist act was planned using Skype. You don't want that.

Steve: No.

Leo: So I don't - I wouldn't cast aspersions or blame on Microsoft. I think it's important we understand what they're doing.

Steve: Yes. They said also, "Another newsletter entry stated that NSA already had pre-encryption access to Outlook mail. 'For PRISM collection against Hotmail, Live, and Outlook.com emails will be unaffected because PRISM collects this data prior to encryption." So there we are. They're upstream, outside of - basically this is the problem

we've discussed now several times about email, that the underlying protocol, SMTP, by which it moves across the Internet from server to server, is almost never encrypted. Not absolutely never. It can be. But that requires an agreement at each end.

And, for example, remember, of four major email providers, only Google offers SMTP encryption. Specifically, Outlook and Hotmail don't. And Yahoo! doesn't. And there's a fourth one, too, I can't remember. But so only Google does, meaning that there isn't going to be encryption on SMTP going in or out of Outlook.com or IE Hotmail because it's not available at the server. Which means they've got access to it.

Then it says: "Microsoft's cooperation was not limited to Outlook.com. An entry dated 8 April" - this year - "2013 describes how the company worked 'for many months' with the FBI, which acts as the liaison between the intelligence agencies and Silicon Valley on PRISM, to allow PRISM access without separate authorization to its cloud storage service SkyDrive." Now, that's also new. I mean, if true.

"The document describes how this access 'means that analysts will no longer have to make a special request ... for this, a process step that many analysts may not have known about.'" So, "The NSA explained that 'this new capability will result in a much more complete and timely collection response.' It continued, 'This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established.'"

Now, I can't read - we can't technically parse that to understand what it means. Unfortunately, the documents are NSA sort of capabilities overview summaries. So they don't explain how this happens. But, I mean, what we have in quoted terminology says that the FBI is the interface arm of PRISM, and they were working to establish access to SkyDrive of some sort. Despite the fact that Microsoft furiously denies exactly that.

And then it says: "A separate entry identified another key area of collaboration. 'The FBI Data Intercept Technology Unit" - that's the acronym I was mentioning, DITU - "team is working with Microsoft to understand an additional feature in Outlook.com which allows users to create email aliases, which may affect our tasking process." So that was where they were talking about working on arranging to disambiguate aliased identities in Microsoft. And then I have some stuff here about Skype, but we've already covered that.

Microsoft immediately, the same day these documents came out, briefly responded. And so the first response was, in response to an article - this is Microsoft speaking. In response to an article in the Guardian on July 11th, and this response is dated July 11th, Microsoft issued the following statement. And this is - I'm reading from the press release on Microsoft.com: "We have clear principles which guide the response across our entire company to government demands for customer information for both law enforcement and national security issues.

"First, we take our commitments to our customers and to compliance with applicable law very seriously, so we provide customer data only in response to legal processes. Second, our compliance team examines all demands very closely, and we reject them if we believe they aren't valid. Third, we only ever comply with orders about" - so far this pretty much says nothing - "comply with orders about specific accounts or identifiers, and we would not respond to the kind of blanket orders discussed in the press over the past few weeks, as the volumes documented in our most recent disclosure clearly illustrate. To be clear, Microsoft does not provide any government with blanket or direct access to SkyDrive, Outlook.com, Skype, or any Microsoft product.

"Finally, when we" - oh, and here's this line - "when we upgrade or update products,

legal obligations may in some circumstances require that we maintain the ability to provide information in response to a law enforcement or national security request." I wonder if that includes upgrading SSL keys. Anyway...

Leo: Uh-huh. Uh-huh. Well, it certainly, well, here's the point: It lets them off the hook.

Steve: Yeah.

Leo: Right? So if they wanted to, they could.

Steve: Yeah. "There are aspects of this debate that we wish we were able to discuss more freely."

Leo: But they can't.

Steve: "That's why we've argued for additional transparency that would help everyone understand and debate these important issues." Okay. And then, finally, yesterday came - this is from Brad Smith, general counsel and executive vice president, legal and corporate affairs, Microsoft. He says: "Today we have asked" - so this is dated - this is yesterday, July 16th. "Today we have asked the Attorney General" - and I guess that's Eric Holder - "of the United States to personally take action to permit Microsoft and other companies to share publicly more complete information about how we handle national security requests for customer information. We believe the U.S. Constitution guarantees our freedom to share more information with the public, yet the government is stopping us. For example, government lawyers have yet to respond to the petition we filed in court on June 19 [so nearly four weeks before] seeking permission to publish the volume of national security requests [just how many] we have received. We hope the Attorney General can step in to change this situation."

Leo: Same thing as Facebook and Google are trying to get them to do.

Steve: Yes. Yes. "Until that happens, we want to share as much information as we currently can. There are significant inaccuracies in the interpretations of leaked government documents reported in the media last week," referring to the Guardian drop of news. "We have asked the Government again for permission to discuss the issues raised by these new documents..."

Leo: Okay. That does have to be frustrating.

Steve: Oh, my goodness.

Leo: Because the documents are out there, and they can't legally respond.

Steve: Right.

Leo: Yeah.

Steve: And they said "...and our request was denied by government lawyers. In the meantime, we have summarized below the information that we are in a position to share, in response to the allegations in the reporting." So he says: "Outlook.com (formerly Hotmail): We do not provide any government with direct access to emails or instant messages. Full stop," he wrote in a separate sentence. So he says, "We do not provide any government with direct access to emails or instant messages, full stop." Now, we can parse that. What does "direct access" mean? Because if any of what the Guardian said was accurate, and if there is filtering and capture technology standing outside of Microsoft, and it really looks like there is, then it could be that encrypted traffic is captured, and then letters are sent compelling Microsoft to provide the ability to decrypt it.

And so again, so if we parse this that way, then it's not blanket. It's not everything. And there's no direct access to Microsoft's backend, yet the same is achieved, essentially, but not on a wholesale basis, but rather on a NSA is grabbing it, can't decrypt it until they ask, until they send Microsoft a letter saying we wanted to decrypt this which we grabbed going off in this direction to somebody who we believe is a foreign person and is an entity of interest.

Then Microsoft continues: "Like all providers of communications services, we are sometimes obligated to comply with lawful demands from governments to turn over content for specific accounts, pursuant to a search warrant or court order. This is true in the United States and other countries where we store data. When we receive such a demand, we review it; and, if obligated to, we comply. We do not provide any government with the technical capability to access user content directly or by itself." And we know they don't have to. It doesn't have to be provided because all the NSA has to do is tap it upstream.

"Instead, governments must continue to rely on legal process to seek from us specified information about identified accounts." And he goes on. I'm going to skip the rest of it. But so this is the position they're in. And so you can - that does sound like they're - some of this is very carefully worded to be technically accurate, but also misleading, and that they really do want to talk more, and the government is saying no, you cannot.

So, I mean, I really do feel like this is really damaging the companies that are alleged to be complying to the degree that we were told they were four weeks ago; that they want to clarify it. And this podcast probably is clarifying it, but of course it's not official, it's just conjecture based on the technologies that we understand. And here's Microsoft's counsel saying we're directly asking the government, please let us respond to these damaging news reports. They are truly damaging us. And the government says, no, you can't. And you'll remember, Leo...

Leo: It's so hard to know who to believe because of course...

Steve: Yeah, it is.

Leo: ...the slides imply very directly, clearly, that there is in fact full government access to - directly to the servers.

Steve: They say that, yes. They say that.

Leo: And it's probably the case that, if that were true, those companies couldn't say it was true. On the other hand, their blanket denials imply - I don't think there's anything requiring them to blanket deny it. Who knows.

Steve: Correct. And remember, last time, last week I took the position that, I mean, the technology required to allow a third party's systems to go in and interpret encrypted databases is significant. So...

Leo: Somebody in the chatroom brought up the concept of a panopticon. This was a prison designed in the 18th Century, never built, but designed in the 18th Century by a guy named Jeremy Bentham, the idea of which was that every prisoner could be observed by the guards, but without the prisoners' knowledge of whether they were being observed, the point being to create this impression that you could be observed at any time, anywhere, and you never knew whether you were or weren't, and that that would ensure good behavior. And the philosophical - it's the philosophical basis for the notion that the government wants us to know this stuff because what they'd like to do is create this impression that in fact everything is being observed, collected.

Steve: We are in a surveillance state.

Leo: Yeah. Whether we are or not, they want to create the impression. It is in their interest to create that impression.

Steve: Boy, it's really upsetting people, Leo.

Leo: It's very upsetting. It's very upsetting. And it's not - it's not upsetting if you assume that the government is benign and the information they're gathering is for purposes of fighting terrorism. It's only upsetting if you think that perhaps it might always not be that way.

Steve: My favorite quote came from someone who tweeted this, and I shared it before. But it's even still being echoed by people who are catching up with my feed on Twitter. "I have nothing to hide from people I trust."

Leo: Right.

Steve: That just says it. It's like, "Well, if you have nothing to hide, why are you

encrypting?" I have nothing to hide from people I trust. So speaking of people we trust, you'll remember that in the first PRISM podcast I really - I was so upset with the testimony that James Clapper gave that we played it into the podcast, where he responded to Ron Wyden, "No, we're not collecting any data on American citizens, not deliberately." Or "not wittingly," was his word.

Anyway, so the Guardian posted something, and then I found some further, I think it was in the Huffington Post. Now Clapper, James Clapper, the Director of National Intelligence, yeah, DNI, Director of National Intelligence, he is the DNI, he said: "I gave 'erroneous'" - he's now calling his answer "erroneous" - "because I forgot about the Patriot Act." And so...

Leo: Seems an odd thing to forget about.

Steve: Yeah, this is the headline: "I gave 'erroneous' answer because I forgot about the Patriot Act." And then the subheading of the Guardian story was "Intelligence chief tries to explain false Senate testimony by saying he 'simply didn't think' of NSA efforts to collect..."

Leo: That's stupid.

Steve: Yeah, we're going to believe this.

Leo: It's so stupid.

Steve: Oh. And then the story reads: "The most senior U.S. intelligence official told a Senate oversight panel" - this was a month, so this is recently, after the first Snowden revelations - "that he 'simply didn't think' of the National Security Agency's efforts to collect the phone records of millions of Americans when he testified in March that it did 'not wittingly' snoop on their communications."

Continuing: "James Clapper, the director of national intelligence, made the comments in a letter to the Senate Intelligence Committee, released in full for the first time [yesterday] on Tuesday. Portions of the letter, in which Clapper apologized for giving 'clearly erroneous' testimony at a March hearing of the committee," which was the snippet that we played, "were first reported by the Washington Post on Monday. Clapper had previously said that his answer to the committee was the 'least untruthful' one" - and of course our boys on Comedy Central had a ball with that - "that he could publicly provide.

"In the full letter, Clapper attempted to explain the false testimony by saying that his recollection failed him. 'I simply didn't think of Section 215 of the Patriot Act,' he wrote to Committee Chairwoman Dianne Feinstein on June 21st, referring to the legal provision cited to justify the mass collection of Americans' phone data, first disclosed by the Guardian."

And the thing that makes this so ridiculous is that he was notified ahead of time that this question was going to be posed. And then afterwards, after lying, clearly lying, he was - Wyden's office contacted him again and said, you know, do you want to correct the

record? And they said no. So I just wanted to wrap up that little tidbit. Meanwhile, the federal government has been disinvited to DefCon. At the end of this month...

Leo: They can still go, they just can't go officially.

Steve: At the end of this month, beginning of next month - yes. They can sneak in. But so Infosecurity magazine covered the story, said: "As the annual DEF CON event prepares to launch in Las Vegas on August 1, 15,000 hackers are planning to descend upon the hot desert landscape. Organizers have however warned federal agents, government security staffers, and law enforcement agents that their particular presence is not required.

"In a post titled 'Feds, We Need Some Time Apart,' conference founder Jeff Moss noted on the event website that a 'time out' is in order in the wake of the uncovering of PRISM, the widespread computer surveillance program that has been operated by the U.S. National Security Agency since 2007." And that was when Microsoft first got involved, according to the documents.

And so remember that we have DEF CON and Black Hat, and those are adjoining conferences. And General Keith Alexander has not been disinvited and is in fact a keynote speaker at Black Hat. And Keith Alexander is famously the director of the NSA, in addition to being - and this was probably his main focus for Black Hat, was he's the commander of the U.S. Cyber Command, USCYBERCOM. And so he's still on the agenda. And so he will be speaking. I imagine it'll be a rather boilerplate presentation, slide presentation about cyberwarfare and cyber contingencies and so forth, as befitting Black Hat.

But as for DEF CON, I mean, traditionally it's been a, yay, come on in, we're all in this thing together. And the federal government's various agencies presented their credentials without any concern. And not so much this year. Okay, now...

Leo: Which, by the way, is meaningless because they just go. There's plenty of contractors. You think Edward Snowden, an Edward Snowden from Booz Allen wouldn't go, or wouldn't be able to - of course.

Steve: Exactly, yeah.

Leo: Yeah. So, nice idea.

Steve: Now, this story - this story, Leo, is so bizarre that I thought it had to be a hoax. And I pursued it back to its source, and apparently it's true. Some offices in Russia are switching to typewriters because they've just given up.

Leo: You know, I know ABC or NBC or somebody repeated this. I just don't buy it. But anyway.

Steve: I know. I know. But we have a photo of it now. We know the model number of

the typewriter. I mean, yes, you can embellish the hoax...

Leo: I trust no news coming out of Russia. Come on.

Steve: Yeah. So what we're led to believe, because this is just too funny, whether it's true or not, the "Kremlin returns to typewriters to avoid computer leaks." Subhead, "The Kremlin is returning to typewriters in an attempt to avoid damaging links from computer hardware, it has been claimed." So even the news guys are saying, okay. So it says: "A source at Russia's Federal Guard Service (FSO), which is in charge of safeguarding Kremlin communications and protecting President Vladimir Putin, claimed that the return to typewriters has been prompted by the publication of secret documents by WikiLeaks, the whistleblowing website, as well as Edward Snowden, the fugitive U.S. intelligence contractor.

"The FSO is looking to spend 486,000 roubles" - which actually doesn't buy you very much, around $15,000 - "on a number of electric typewriters, according to the state procurement agency. The notice included ribbons for German-made Triumph Adlew TWEN 180 typewriters, although it was not clear if the typewriters themselves were of this kind." So maybe they should just switch to Linux, rather than that.

Leo: Yeah. I don't think typewriters are more secure. Not at all.

Steve: No. No, in fact we know that, not only - well, and there was some actual - the story goes on to talk about how there's an advantage, which actually sounds a little more, makes it even sound a little more ridiculous, that you can always identify the source, the particular typewriter that types a document. And of course we know you can also identify the particular printer that printed the document because of the little yellow dots that are scattered around in a given pattern. So...

Leo: It's just, you know.

Steve: I wanted to correct the record. Thanks to...

Leo: Yeah, Pilot Sum Ting Wong was flying the Asiana Air...

Steve: Oh, my god, did you see that, Leo?

Leo: Unbelievable.

Steve: Oh, goodness. Along with Wi Tu Lo, who was the copilot.

Leo: Yeah, it's "Anchorman" in real world. The moron newscaster just read what she saw on the prompter.

Steve: And being sued for it now.

Leo: And rightly so because that's absurd. Although apparently a summer intern at the NTSB did in fact confirm it. We're talking about Channel 2, local news operation, which is normally a pretty good news operation, although all local television news is ghastly. But their noon news - and I even know this anchor. The anchor read clearly prank names for the four pilots of the plane that crashed in San Francisco. You know, Sum Ting Wong, Wi Tu Lo. They were offensive. And if she was not a complete idiot, she would have noticed the minute she started saying them, and if she had had any brains would have said, no, no, no, this is wrong. I'm not going to read this. We're moving on.

Steve: And they were up on the...

Leo: They were on the screen.

Steve: They were up on the screen.

Leo: I thought it was an Onion thing until I saw that it was true.

Steve: I know. I didn't believe it. A buddy of mine sent me the link. I said, no, come on.

Leo: Ron Burgundy lives. Unbelievable [laughing]. Anyway, I believe that story as much as I believe typewriters in Russia.

Steve: Yeah, good.

Leo: I don't - you know, the mainstream news is so godawful nowadays, I don't trust them. Just use your brain. It doesn't make any sense. Go ahead.

Steve: No, no. Okay, here's what does.

Leo: Yes. I listen to Steve. I trust Steve.

Steve: I got a tweet from one of the developers of Adblock Plus, who wanted to explain. He sent me a link to an image which, Leo, you can bring up: eyeo.com/images/acceptable-ads-facts.png.

Leo: Okay.

Steve: Because last week we reported on a story in TechCrunch. TechCrunch was saying

Google and others reportedly pay Adblock Plus to show you ads anyway. And that's where I had said, you know, that annoys me. And right in the options there you can turn that off. So here's the story: Five Facts About Acceptable, what they call "Acceptable" Ads, which is a term of art for them.

They said, before we get into the five points: "Online ads are annoying. That's why millions of people love Adblock Plus. However, ads play an important role in keeping content and services free on the Internet." And there's no denying that. I will argue that tracking doesn't, but ads certainly do. Continuing with their note: "For this reason, Adblock Plus started an initiative in 2011 called 'Acceptable Ads,' which aims to create a middle ground for websites and users, while keeping control firmly in the users' hands to determine how they want to experience the web." That's all we want.

"Here are five key facts about it: First, Acceptable Ads is only about unobtrusive advertising, usually small text links, the kind preferred by most users. Banners, video ads, pop ups, et cetera, will NEVER" - all caps, their emphasis - "be allowed. There is no way to 'buy' a whitelisting." Which goes against what the headline was, the way TechCrunch reported this. "There is no way to 'buy' a whitelisting. If ads do not meet our criteria, they can never be whitelisted. Our open community of over 27,000 members has the final say in whether ads comply with the rules, and the rules are completely unambiguous. Third, whitelisting is free for small websites. Only larger corporations pay."

Leo: Well, I'm confused. You can't buy a whitelisting, but corporations can? Doesn't that contradict No. 2? There's no way to buy a whitelisting. Only corporations pay. These are contradictory items.

Steve: "Whitelisting is free for small websites. Only larger corporations pay."

Leo: There's no way to buy a whitelisting, says Item 2. No. 3, only corporations pay.

Steve: Well, somebody can figure that out.

Leo: What they're saying is you can't buy a whitelisting if ads do not meet our criteria.

Steve: Correct. There's no way to purchase around the criteria.

Leo: However, there is a way to buy a whitelisting. Pay us, and have the ads meet our criteria.

Steve: No. If you want to be - if you're a large corporation, we will ask you to fund our effort. And if your ads meet the criteria, then we will add you. So large corporations have to pay to have acceptable ads accepted. Small companies don't. Yeah, so that does fit.

Leo: Yeah. Well, okay.

Steve: Hey, I love Adblock Plus. Okay. "Four, about 80% of all Adblock Plus users like Acceptable Ads." And mine's turned again, by the way, because I have no problem with this.

Leo: So you can't pay - unless you're a big corporation you can't pay. And by the way, everybody likes it anyway.

Steve: 80% does.

Leo: 80%.

Steve: And there's a checkbox. "They view it as a fair balance" - the users, 80% - "as a fair balance between their interests and the interests of website owners and publishers." And, finally, and for those who want to block ads of all kinds, every Adblock Plus user has a choice at any time to switch off acceptable ads with just one click in the Options menu." So anyway...

Leo: And that is true. You can click that box, and you will never see any ads.

Steve: Yes. And I've never turned mine off before. I have Adblock Plus on all of my browsers, and nothing is ever jumping around and annoying me. And I have ads on my pages. They're just not crazy. Sometimes I use someone's browser without it, and it's like, oh, my lord, is this what people view? No wonder they're crazy. Anyway, so, yes. Are we done?

Leo: Moving on.

Steve: I think it's fine. Lavabit.com. So what I got was a number of people - and I never found the story or where it was claimed that Snowden was using Lavabit.

Leo: I know. I never saw it, either. I just read it. It was all secondhand; right.

Steve: Yeah. Yeah. So I saw - and I thought, huh, what's Lavabit? That's interesting. So I did a dive into it to figure out what the story is. Now - oh, and so I was - so what was tweeted was that Edward Snowden was using Lavabit, as if that was some wonderful, super-secure solution for email. So of course I went there to find out what the story is. And it's not. Because it actually can't be. And what I thought I remembered, and then I did go back and track that down, was that Greenwald was actually given, like, was given his initial communications months before this happened. Snowden was trying to get him to use encryption of sufficient strength, and it was just because Greenwald wasn't a techie that they were unable to do that.

So anyway, okay, so here's Lavabit. Lavabit, what Lavabit offers is very well-designed encryption at rest. Which is to say that your email on their servers, they're an email service company. So they offer ad-embellished email for free, or you can pay a nominal

sum, like $8 a year, it's very inexpensive, and get an account with Lavabit. And they will encrypt your email on their servers.

Now, they overstate, in my opinion, the value of that because they're saying they cannot comply with letters to compel them to turn over your email, which I believe. But they are able to decrypt it when it comes in and when it goes out because the email itself is not encrypted. Now, they do offer SSL connections between your email client, if it supports SSL, and their server. So you would have an encrypted connection to them. And when you log in with your username and password, that information they themselves receive. Then they hash it, salt it, and use that as the key for decrypting - I'm sorry, as the key, yes, for decrypting the private key, which is then used to decrypt your stored email in order to send it in the clear back to you over SSL. But at that time, they have it. It's available to them when it's sent to you for you to receive it.

Incoming email - and this is the clever part. Incoming email to you comes in, of course, unencrypted because email is, by default, a nonencrypted protocol. They use your public key, which they keep in the clear, to encrypt incoming email, to store it so that only you are able to pick it up and decrypt it. So I give them credit for doing something, for storing it in an encrypted format, which they then need you to log onto your account in order to decrypt the key that gives them access to it so they can decrypt it and send it to you. So it's like, eh, it's better than nothing. And so it's encrypted at rest and decrypted when you pick it up. And if you're sending email out through them, then it would never be encrypted because they would have to - you use SMTP to send the mail to them outgoing somewhere else. So they would not encrypt it, and it would not be encrypted when they send it.

So it would be incoming email to you, encrypted while it's stored, waiting for you to pick it up. That's what they offer. And maybe Snowden used that. I mean, it sounds like he would, except we also know, and I have since verified, he uses Leo's favorite email encryption, which is PGP.

Leo: Yeah.

Steve: And I found an article in The Huffington Post to fill in the facts, that "Edward Snowden first approached the Guardian's Glenn Greenwald in February," so many months before this was finally divulged, "and, by the journalist's account said he had information" - that is, Edward did - "'that would be of great interest.' But there was a problem. Snowden only wanted to communicate securely using PGP encryption, for which Greenwald didn't have the proper software installed at the time. In an interview with The Huffington Post, Greenwald acknowledged that he's no expert in using such technology and said that Snowden even provided a step-by-step email and video to help secure their communication. At that point, however, Greenwald didn't know what his would-be source had - or might not have - and continued to prioritize other stories" ahead of Snowden's.

So of course the benefit of PGP, I mean, that's - you need to use end-to-end encryption. It's better than nothing to have it stored encrypted, but it's going to be decrypted when it's sent to you. And of course what PGP does is it provides local pre-Internet, PIE, as we've the acronym, PIE, Pre-Internet Encryption, so that it's encrypted in your computer as it leaves your browser, and then it doesn't matter who has it along the way, or who stores it in the clear. It's just noise. It is pseudorandom noise. Then only when it goes to the recipient who has access to your public key are they then able to decrypt it, so using - in standard PGP style.

Leo: We should do a how-to on using...

Steve: Yeah, we ought to. Or maybe on one of...

Leo: Yeah, maybe one of the other shows or something. I could do a special. I recommend GNU Privacy Guard, which is an open source, open PGP...

Steve: GP - GPG.

Leo: GPG.

Steve: Reverse the letters, GPG.

Leo: Yeah, it's at GnuPG.org. And it's very easy to install. There's Mac and Windows installers. It's not hard. The only negative, as we talked about last week, is that it's not signed by any third party. It's not certificate ensured.

Steve: Right.

Leo: So you get other people to sign your key, and you sign their key.

Steve: And it's person-to-person. And so if I wanted to send email to you, I would use your public key to encrypt the email so that only you with the matching private key would be able to decrypt it.

Leo: Exactly.

Steve: And then we've got point-to-point encryption. And, I mean, bulletproof. I mean, absolutely. You need to get the key exchange made in a secure fashion. So...

Leo: Well, there are key servers, and that's one of the nice things about GNU Privacy Guard and PGP in general is MIT and others run key servers that you can go to. And if you know somebody's key thumbnail or whatever, you can download their key.

Steve: Yeah. And again...

Leo: You can also put it on your website, if you want. I mean, you know.

Steve: Right.

Leo: I think it would be better probably just to put it on the MIT server.

Steve: Yup. So a little bit of news about Google Authenticator. And I don't know if they're going to fix this. I don't know if Google - or how much they care that iOS7, the current beta, breaks Google Authenticator. There's been a lot of information and thread about this. And Google Authenticator has not been updated since 2011, for two years, which leads some people to believe that maybe it's abandonware. I hope Google fixes it, or maybe that iOS7, when it's finally done, won't break it. What happens is it just loses your settings and your sites. And apparently, even if you put them back in, it then doesn't retain them. So it's a problem.

And in the discussion thread about this over on code.google.com about Google Authenticator, two alternative authenticators have been suggested which are compatible. They still use the One-Time Password, the open technology. And it's one that - one of them referred to there is one that I have talked to our listeners about already, which is really pretty, and that's HDE OTP, available on iTunes. And then one that also looks nice that I hadn't seen before is called Authy, A-u-t-h-y. And that's at www.authy.com.

So if you're using Google Authenticator on iOS platform, and you upgrade to iOS7 when it happens, and there isn't a fix for it before then, it may be necessary to look for an alternative. And these two work just fine under iOS7. So I don't know what's wrong with...

Leo: Oh, they'll fix that. That's...

Steve: I would think so.

Leo: Remember, iOS7 is beta. Nobody's supposed to be using iOS7. It's beta for developers only.

Steve: Right.

Leo: It'll be fixed.

Steve: Also, BitTorrent Sync. I'm still waiting for the formal documentation from them of their protocol, but we'll talk about them, come back toward the end of the show, talking about things that I think that seem to me to be - I would call them "open intent." Yesterday they just went to v1.1.42. Android support has been added. Ars Technica just reported hours ago that it had moved from alpha to beta. I was contacted by them last week by their communications guy, his name's Christian, says, "Hey, Steve, we will be at beta, out of alpha at beta on Tuesday." Looks like that was a day later than he expected back then. But apparently it has happened. So it's moving forward. Android platform now.

And then I tweeted a link, in case anyone is interested in following up on this, or people

who don't follow me on Twitter wouldn't know that someone who's in charge of their communication or their - his name is Dan Brown, BitTorrent's digital creative manager. I guess Ars Technica was where I found out about this. Then I went to his blog post.

And he said: "I've been using BitTorrent Sync for syncing several gigabytes of RAW photos" - R-A-W photos, meaning big - "and video across my various machines," wrote Dan Brown. "There is the occasional scenario, however, where I've wanted to grab a few files, but my other machine is turned off. To solve this problem, I'm using a Raspberry Pi as a low power, always-on device with Sync installed." So BitTorrent Sync installed in his Raspberry Pi. "Just for kicks, I'm also using ownCloud" - which is an open source cloud - "to provide me with a web interface for accessing my files from any computer, including my mobile phone."

And so what I have is - and I just tweeted this, so you could go to Twitter.com/SGgrc, and you'll find it. Because he's blogged the step-by-step process. And the blog is "How I Created My Own Personal Cloud Using BitTorrent Sync, ownCloud, and Raspberry Pi." So I know that there's a huge interest in Raspberry Pi because it was such an incredibly inexpensive and cool little platform. And if you've ended up not doing something with it, here's a way to use, basically to create a truly Trust No One point-to-point cloud, and give you Raspberry Pi something to do. Which I think is cool.

And I responded to Christian with this news, saying, "Christian, thank you for the update. I will share it with our listeners. But I still want the public protocol, the protocol to be released publicly." And he said yes, you know, as soon as they can do it they will.

And then totally off the path, except that this, I actually saw this happening, was Network Solutions was down, off the air under a DDoS attack for about an hour this morning. Which caused a lot of pain for people who are hosted by Network Solutions. And in Network Solutions' own Facebook posting - they needed to put something somewhere, they could tell people what was going on - they said "Network Solutions is experiencing a Distributed Denial of Service attack that is impacting our customers as well as the Network Solutions site." And that's the case. I was unable to get to their site.

"Our technology team is working to mitigate the situation. Please check back for updates." So there were many people who, as I said, are hosted, they've decided just to have their websites hosted by Network Solutions, and all of those sites were blown off the 'Net during this. Yeah, I had not seen that before.

We spoke last week of Hemlis, which "hemlis" is the word that means "secure" in Swedish. They were rapidly achieving full funding. It took them less than two days to cross the 150% point, at which they closed down. They went 50% over, and they closed down their offering for early funding. And these are the simple, beautiful, secure instant messaging people. One of them was the cofounder of the Pirate Bay. And a nice little video online. And I gave them 50 bucks last week before the podcast. And a lot of people were interested in what they had to offer. So they very quickly generated more than $150,000, and they're going to move forward and create the product, which is cool.

Update on SmushBox, which, Leo, you and I talked about.

Leo: Yeah, where is our SmushBox?

Steve: Where's our SmushBox?

Leo: I want my SmushBox.

Steve: On its way, apparently. Well, not actually shipping, but moving forward. They received their cases. And I got email from them with a photo of all of the cases, the exterior extruded aluminum cases, sitting there on a big table. So they're moving forward. There's been an ongoing interest that really pleases them because they intend to commercialize this after they fulfill all of their Kickstarter early purchaser requests. And so they're pleased that it looks like they've got a product coming.

And also, remember that we spoke quite a while ago about a movie that a local movie producer, Jonathan Schiefer, wanted to put together called "The Root Kit." And he had attempted to launch it over on Kickstarter. I think he was going for $50,000 and fell short of the goal in the period of time that he had allotted, and so it didn't happen. Well, he's back. And I looked at his video, which he has on his relaunch. He actually sent a letter which indicated he would never do another Kickstarter project because apparently it just was a huge time sink to babysit Kickstarter for whatever reason.

Leo: It's a lot of work, yeah, yeah.

Steve: Yeah, and he just said, okay, never, never, never again. But he's back. He's rewritten and has actually got his screenplay that can be downloaded by anybody who's curious. What he's doing now is he's over at Indiegogo.com with a project called "Algorithm." And the movie will be called "Algorithm." He wants to presell the Blu-ray and DVD for the movie "Algorithm," use that to generate $30,000, which will finance the production of the movie and the production of the DVDs for all the people who want to see the movie.

So he said, "What's it about? A hacker-for-hire discovers that the government monitors everything we do. He and his friends fight back. 'Algorithm' is a story with a message, and the message is that we are not powerless; that we can fight back; that more than money or guns or nuclear weapons, computers have leveled the playing field. If you want to know more, you can read the screenplay." And then he provides a link to it: spiritusvult.com/algorithm.pdf.

So anyway, I wanted to give people the heads-up. They can go to TheRootKit.com, or his new link is TheHackerMovie.com. And that is a redirect, actually, over to the Indiegogo page, where you can watch a video that Jonathan has produced explaining his plans, why he has the ability to do this, and so forth. And I want to see it. So I gave him 25 bucks to prepurchase a copy of the Blu-ray and DVD. And so any of our listeners who feel similarly are welcome to.

And I had another nice SSD success that I wanted to share with our listeners about SpinRite, from someone named Dennie Warren Jr. And he wrote to our tech support guy, Greg. He said, "I am by no means a tech geek, but I do listen to Security Now! as much as I can and learn something every time I listen. I did go ahead and purchase a Lenovo W530 laptop and replaced the C-drive with a Crucial M4 SSD as the main drive because it was too small" - oh, the original drive was too small for his liking.

He said, "On July 14, 2013 at 9:45 a.m., I noticed that three updates were waiting for me." Oh, so that was last week's Second Tuesday of the Month update. "Three updates were waiting for me to install, so I clicked to install them. When I returned to my laptop,

it said that I needed to restart it, so I did. Well, then my laptop notified me that it could not boot into Windows because the drive was inaccessible." Ooh. "Even though my machine was SSD-based, I purchased SpinRite 6 and created a USB boot drive to see if SpinRite could fix the issues. After about 45 minutes SpinRite had finished working its magic. I restarted my laptop, and it booted into Windows 7. And it worked normally, as it did before it had crashed.

"I jumped to the ceiling of my home, screaming with joy, and told my wife that we're renaming our son 'Steve.' I won't share her response [laughter]. I won't share her response to me except that she's glad for me to have my computer working again. It's working as if nothing had ever happened. I can't remember what kind of updates caused this crash." Wow, I wonder if it was a problem with the updates because...

Leo: No, no no no.

Steve: Probably not. However...

Leo: It's coincidental. Whenever you're doing a lot of disk writing...

Steve: Oh, it is coincidence because SpinRite fixed it, and it wasn't a matter of removing the update.

Leo: Right.

Steve: "However, tell Steve I said thank you. He is the best. He is the one thing" - oh, he says, "It is one thing to hear others say how much they like SpinRite. But it's a whole other feeling to have your computer rescued by it. Did I mention that Steve is the best? Jay. Kind regards."

Leo: UOSD Wiz said he should have said rename him DynaStat [laughter]. Forget Steve. Rename him DynaStat.

Steve: His wife would really have a problem.

Leo: Honey? Hey - go ahead.

Steve: One thing I wanted to add was that Elaine sent me a first. So Elaine said, "Steve, you're not the only one getting testimonials <grin>. Had to show this to you."

Leo: Oh, that's nice.

Steve: So she received a letter, said, "Elaine, I am a subscriber/listener of Steve Gibson's Security Now! podcast. I just want to personally thank you for the wonderful

transcription detail and clarity that you provide for a niche technical (and at times complex) recorded broadcast. Your thorough, accurate, and complete approach preserves the culture/humanity of the podcast, while also making archival episodes easy to search on Google, et cetera, post-broadcast for years to come. Appreciated, Ross Blaettner, Subscriber, Security Now!." And then he said, "P.S.: You are more than welcome to use my commentary in a testimonial because you are certainly deserving of all such praise."

Leo: That's nice.

Steve: So, yay to Elaine. Shout out for her. [Elaine says thanks, guys.]

Leo: We say that every day. Yay to Elaine.

Steve: We do.

Leo: Hey, before we get - I think we should talk - the subject matter is How Much Tinfoil?

Steve: Yeah.

Leo: And I think we're going to talk a little bit about what you can do to protect yourself. We've talked a little bit already.

Steve: What you should do, what's overkill, and so forth.

Leo: Yeah.

Steve: In other words, how much tinfoil do you need?

Leo: How thick does it have to be?

Steve: Yeah.

Leo: Now, Steverino, let's get a little tinfoil.

Steve: Yeah. I was trying to think, what would be the sequence that law enforcement would use if they wanted to access stuff that is available to them and is encrypted.

Leo: You know what hackers say is first you get the dox, d-o-x. And that's

information: date of birth, address, IP address, ISP. The more you know; right?

Steve: Well, yes. Right. So you would learn where the target's traffic was transiting, and then you would tap that. So you would collect traffic, and you would look at the IPs that the traffic was bound to. You would know that it was coming from the target. You would look at the IP addresses of where it was bound to. And that would tell you, oh, this is going to Google Drive or - SkyDrive or Google Drive or email. They're using Yahoo! as their email account.

So the idea would be you'd collect the traffic at the source to determine, like, what cloud providers they have chosen. Then you'd go to the cloud provider and say, encrypted traffic was going to you. We need you to decrypt it for us. I mean, that would be the sequence of events. So, okay. So it's very clear that, first of all, many people aren't worried about this at all. They go, well, okay. I mean, and you've expressed an opinion, Leo, sort of one of resignation. It's like, well, we're in a surveillance state. That's going to happen. There's tapping going on, and so that's - so we live with it.

It's clear that something is going on with these major terminuses - Microsoft, Google, Yahoo!, Dropbox, Facebook, and so forth. They're on the PRISM timeline. We don't know in detail, and we probably never will, exactly, I mean, precisely technically what's happening. But the damage that we referred to earlier, that seems to me is clear, to their reputation as a consequence of this is that, if people felt creepy that the NSA had chosen these major providers for PRISM, whatever that is, then why not use one that's not on the list? Which, you know, seems like that makes some sense. Use anything that isn't a major target because clearly the NSA, I mean, if they're doing, and they seem at least partially to be doing what I originally suggested that made sense, which is tapping upstream of these major guys, they chose those big guys because such a large percentage of Internet traffic has chosen them because they are Microsoft, because they are Google, because they're Yahoo! or Dropbox or whomever. So this argues for not going with one of these big guys, just to stay off the radar, stay off of, you know, so that your traffic is not participating in PRISM by default.

Now, if you're a target, then the other end of your traffic, as I initially started talking about, would be intercepted. Clearly they have the ability to do that. So that's a different scenario than the rest of us who are not targets for any particular reason, but just don't like the idea of pervasive surveillance. So they're the big guys. But then we've also talked about - and those are like, I don't want to use the word "Tier 1" because that refers specifically to Internet traffic transit providers. But these are top-tier corporate cloud products - Microsoft, Google, Yahoo!, Dropbox, and so forth, the big guys. And they're going to be targets.

Then you have your second-tier providers that are - and, for example, in our cloud storage podcasts [SN-349, SN-350, SN-351], where we went through 15 of them or so, many of them have poor security models. But they don't care. They've got beautiful-looking websites. And people go, oh, look how pretty their website is. They must be nice people. And so people use those as their cloud storage provider, although not offering a great deal of security.

And among those there were - there was clearly a few who focused on a TNO model. And so that's really where - that's where I come back to. I mean, that's where I'm - it's Pre-Internet Encryption. It's PIE, one of the early acronyms, along with Trust No One, that we coined because it's always been clear that that's the only way to be secure is this stuff is encrypted before it leaves, and it is not decrypted until it comes back. And so that

immediately rules out the generic use of SkyDrive and Google Drive and storage at Yahoo! or Dropbox, which are not pre-Internet encrypted technologies. They're very convenient. They offer lots of features. But if you're able to use some foreign browser and get access to your content through a browser interface, that's not pre-Internet encryption unless the way it works is that it downloads a decryption technology into that browser and then does local decryption. But that's not the way these things operate.

So those guys don't have end-user security as their first issue. And so for me, they're just - unless you pre-wrap everything you're storing with them with your own local pre-Internet encryption technology, don't even consider using them. But if you do pre-wrap your data, by all means. All they're storing for you is pseudorandom noise that they have absolutely no ability to decrypt. So the NSA or whomever can go to them and say we want this person's data. And they apply the encryption keys, and it changes it from one set of pseudorandom noise to another one and still tells them nothing.

So I look at the cloud providers who explicitly want to protect our data. I mean, they see that's their mission. Microsoft doesn't. Google doesn't. I mean, they're not protecting, they're providing no protection at all. And Dropbox doesn't. They're, oh, yeah, yeah, we're secure storage. Baloney. You may be secure against hackers, not secure against somebody who can send you a warrant and say we want to look inside. So if we're going to do something, then it's about pre-Internet encryption.

And so when I look at BitTorrent Sync, yes, I wish we had an open protocol. They say they're going to do that. But it is, to me, their intent is obviously to create, in the case of BitTorrent Sync, a truly secure Pre-Internet Encryption, Trust No One technology that allows us to link our machines together for large filesharing. Hemlis, same thing, all about this can be simple. It can be beautiful. We're going to create something for iOS and Android. Here's our model. We're not going to make it free. We're not going to put ads in it. So we're going to ask you for a little bit of money, and that's how we're going to fund the backend that we need for linking this stuff together. It'll be encrypted before it leaves. It'll be decrypted when it comes back. And we're going to solve all the details. To me, that's who we want to work with.

Threema, the thing that we've talked about a couple times, currently shipping. And those are the guys that have the three dots. You either get one dot, two dots, or three dots based on what level of authentication you have achieved. And you only get the green three dots when the phones are facing each other and directly exchange keys. Then you have absolute authentication, and your then-encrypted communications between iOS and Android devices always show with three green dots, and absolutely impossible for a third party monitoring your traffic to gain access.

And then Cryptocat, same thing. We talked last week about the disaster with the poor coding in JavaScript of their multiparty chat. But their point-to-point chat always was and is secure and uses an open protocol, which they have a good implementation of. They just gave it a nice web browser interface. And so to me, that's where I am is - it's like, yes, these things are not open source always. Even LastPass. LastPass did something I thought was brilliant, which was they explained to me exactly how it works, so complete open protocol. Then they went further and said we're going to demonstrate that this is the way we're encrypting. We're going to prove that what we just said was true by giving you a web page with JavaScript that does what we just said it should do, and you can see by putting your own data into this web page that it works, that you can decrypt your stuff with this web page. This is the way it was encrypted. So it was a proof of openness, essentially, that was like, okay, for me, this is exactly the right solution. I mean, Joe designed this thing so that it achieves - it was using the cloud for synchronization, but it was 100% Trust No One and Pre-Internet Encryption. I haven't audited the source. I

don't need to.

I mean, so when I talk about how much tinfoil, I guess I'm at a softer place, Leo, than the absolute "ism" of it's got to be open source. I think if it's open protocol, if it's open agenda, and if every scrutiny of the effort says these are good people, then it's like, okay, you know, I'm comfortable enough with that. I mean, first of all, I need nothing. I need to encrypt nothing except my data. For example, if I were using a cloud provider and putting - and actually, for example, GRC's corporate books are encrypted by Jungle Disk and stored at Amazon S3. Still using Jungle Disk. That's pre-Internet encryption. It's TNO. It's local symmetric key. And there's no way I would let our corporate books leave our control for cloud backup unless it was pre-Internet encryption. So there you absolutely want to use good encryption.

But I don't, you know, my text messages are just to my friends. So I don't need it. Although when point-to-point text messaging encryption becomes ubiquitous or easy to use, like Hemlis is making it and Threema have made it, then it's like why not? It's just kind of cool. Just a coolness factor.

Leo: Yeah. Well, I just exchanged - somebody who was listening, obviously, to the show got my key off the key server and sent me email using my key, which I decrypted.

Steve: Cool, yup.

Leo: I then got their key, because they had a key when they did it, and added it to my key. In fact, it's on there right now. And it's very easy. Now, whenever I email Doug, it'll automatically be encrypted. Transparently, without any effort on my part.

Steve: I'll bet you that at some point the world, I mean, I don't know, a decade...

Leo: Let's just do it. If everybody did this, yes, of course the NSA grabs your stuff. I made my key 4096 bits.

Steve: Yup, to NSA that's...

Leo: Planning for the future.

Steve: Yes. Yup.

Leo: And it's good. It's the way to do it. So make, you know, it's really easy using these GNU Privacy Guard tools. The Mac thing is - it works with Apple Mail. It's very transparent. Little harder to do if you're using a web-based mail server, unfortunately. It's really easy on a client like Mozilla Thunderbird or Apple Mail, something like that. It's very easy on Thunderbird.

Steve: Well, and I would imagine there will be plugins at some point, if there aren't already, for specific browsers.

Leo: There probably is for Gmail. But it's - that's harder to do right.

Steve: Yeah.

Leo: If you think about it. So...

Steve: Yeah.

Leo: You can't - and you know, by the way, you can use PGP locally. Just take a block of text, encrypt it, and send it off. So that works fine with any mail server.

Steve: And in fact the protocol, the PGP protocol is mature enough that I'm seeing other new efforts launching that are going to be using PGP as their well-proven crypto model because the code is available, and they're just going to package it up and use it for different - to transport different sorts of information than traditional email, as it's been used for.

Leo: There was a Know How episode on this. I did not know. The last Know How episode, No. 50, shows you how to do this. I'm not sure exactly how they did it. I haven't seen it yet. But my recommendation...

Steve: In fact, I remember hearing that there was going to be some thing special...

Leo: Yeah, I'm glad they did that. My recommendation, and I suspect, I'm sure that they - this is how they did it, is GNU Privacy Guard and GPG Tools. They're really great. Really great. And it's open source, so you know it's not - there's no backdoor.

Steve: Yeah. So I think, bottom line, we're never going to know what's going on. We know now that our law enforcement agencies have taken the position that they need to capture everything and build networking models of interactions of people. I think most of us it's sad. It's a little creepy. But it's the reality of the 20th Century, 21st Century, whatever century we're in.

Leo: Yeah. By the way, this is the command line interface for GPG. It says - you just type "GPG." It says, go ahead, type your message. You type your secret message in cleartext. And then if you have the right keys, which I haven't installed yet, it'll encrypt it, and you'll be given some junk that you can then paste.

Steve: Nice.

Leo: And you just do it to annoy the NSA. Here's another story, by the way. This happened this morning. I don't know if you heard about this, the NSA testifying before the Judiciary Committee. An aide - during testimony on Capitol Hill today, a National Security Agency representative admitted that the government's perhaps looking at more data than we had thought.

Steve: [Sighing]

Leo: So this is Chris Inglis. He's the deputy director of the NSA, testifying before the House Judiciary Committee. He said that analysts look two or three hops from terror suspects when evaluating terror activity. Previously they had admitted to two hops. That means, if they're following a terrorist, and he calls somebody, they could then look at the person that that person, the person the terrorist called, called.

Steve: Three degrees of separation.

Leo: But now it's three hops, which means terrorist calls somebody. That person calls somebody. That person calls somebody. They can start collecting data from that third person. And that's pretty much everybody.

Steve: That really is, yes.

Leo: Because according to a study at the University of Milan, we're all 4.74 steps away from everybody else. So three hops, three degrees of separation is a vast universe.

Steve: Yeah.

Leo: Very quickly means that everybody is involved.

Steve: It's funny, too, because the now head of the NSA, Alexander, who I was talking about before? Apparently he was involved in Iraq and our efforts there. And when he became involved, and they were using communications signaling intelligence in order to track down terrorists within Iraq, his solution was, instead of looking for a needle in a haystack, let's collect the entire haystack.

Leo: Just the haystack.

Steve: Yes.

Leo: And then when we need to look, we'll have it.

Steve: Yes. So it was originally there, apparently a very successful approach over there was record everything, and then we'll sift through it when we know what we're looking for.

Leo: By the way, the members of Congress, not being mathematically inclined, had no idea what he had just said.

Steve: And Leo, saying "not being mathematically inclined"...

Leo: Is an understatement. But nobody said anything. But that's the first time the NSA's admitted three hops. He said, eh, two or three hops. Very casually. As if it could be four.

Steve: Oh, as if it was nothing.

Leo: And it could be five, really. I mean, it could be, I don't know...

Steve: Let's explain exponentiation to you. Please.

Leo: Yeah. They had no clue.

Steve: Wow.

Leo: And I think that that's the other thing that happens, is the people at the NSA think, and they're probably right, that they're smarter than Congress. And so they just mislead them. They say things like that in a way that just misleads them.

Steve: Yeah.

Leo: And when you mislead Congress, whatever you think of Congress, you're misleading us because they're the people who are supposed to enact this stuff.

Steve: Yeah, well, and the whole, I mean, part and parcel was oversight.

Leo: Yeah.

Steve: And oversight means telling the truth when they ask you a question. And that was my argument with Clapper and his ridiculous, oh, I forgot about the Patriot Act. Uh-huh. Yeah.

Leo: Hard to believe.

Steve: Yeah.

Leo: Hard to believe. Well, Steve, thank you. Once again, another great episode. And I think you're right, we didn't have time for questions. But we'll do it in a couple of weeks. If you have questions for Steve, go to GRC.com/feedback. While you're at GRC, get SpinRite, the world's best hard drive maintenance utility. Yes, it works on encrypted drives. Somebody asked in the chatroom. Doesn't care what's on the drive. It's right below everything else.

Steve: Yeah, actually a lot of people have used it. When TrueCrypt hits a problem, it'll say - it'll stop and back itself out, saying, oh, I'm unable to decrypt this drive. And so it's very much sort of like the way Microsoft used to have a problem when you were trying to convert from FAT16 to FAT32. If there were any bad clusters or sectors on the drive, you were unable to do a FAT16 to 32 conversion. And so people - we sold a lot of copies of SpinRite to people who needed to fix their drive in order to convert to FAT32. Similarly, people when they're trying to encrypt or decrypt using TrueCrypt, they'll often hit a problem that they didn't know they had. And SpinRite will fix it, and then TrueCrypt will go ahead and operate.

Leo: I should give a little more credit to some of the members of Congress. Here's some of the things that members of the House said in this hearing. Minority member John Conyers of Michigan: "You've already violated the law, in my opinion." Jerry Nadler of New York: "I believe it's totally unprecedented and goes way beyond the statute." Ted Poe of Texas: "Do you see a national security exemption in the Fourth Amendment? We've abused the concept of rights in the name of national security." And Jim Sensenbrenner of Wisconsin, the author of the Patriot Act, said, hey, you know what, it's up for renewal in 2015. The provisions for phone metadata collection, he warned, have got to be changed. Otherwise, in a year and a half, you're not going to have it anymore.

Steve: I would say that what we need to respect are their staffs.

Leo: Yeah, because they're intelligent. The staffs are intelligent.

Steve: The staffs do all the work, Leo.

Leo: Congress represents us. They are our representatives. You voted for them. If you don't like them, vote them out. But they're what we got right now, and it's the only line of defense. You've got to write to your member of Congress and say this will not stand. It's not - we don't believe it's constitutional. And you've got to overturn it.

Steve: What I would recommend to anybody who likes to follow this stuff, is to get

yourself on the EFF's mailing list, the Electronic Frontier Foundation. They really are leading this. They've already filed a lawsuit against the NSA over this. And they've got smart attorneys. They know the law. The EFF is a great organization. And they're one of the Twitter feeds that I follow in order to see what's going on. So I see what's going on with them. But also, so either follow them on Twitter, and/or subscribe to email from them. And then you'll know what's going on. And they often send you, here's a link to a page that will immediately, on your behalf, you fill out your name and address and where you are, and it will send email or letters to your local representatives, it figures out all of that for you, to help you express your opinion to your local people in Congress and government. So...

Leo: And don't buy the BS that, oh, well, they're all in it, and Congress sucks, and the government's - because if you don't go through Congress, your only other alternative is leave the country or revolt.

Steve: And move, yeah.

Leo: So let's try the democratic process, shall we? It'll work. But you've got to get involved. You can't say, oh, they're all losers anyway.

Steve: Yeah. I think it's true that there were some early - there were some people ahead of the curve in Congress, who under- who are on the Intelligence Committee, who realize this was not - what was happening was not what America thought. And, I mean, right off the bat I said I would not do what Edward did because my oath would prohibit me from doing that. But I'm glad he did. I mean, and now, of course, look at the result. The result is good. This is all good.

Leo: I'm glad we're having the conversation.

Steve: Yeah, although it sure has hurt those companies that we're enumerating.

Leo: Well, good. Because guess what runs this country? Those companies. And if it's bad for business, that's the best possible way to get this thrown out. Bad for personal rights, big deal. Bad for business, watch out.

Steve: Yeah.

Leo: Microsoft has lobbyists. They listen to Microsoft's lobby. They'd listen to us if we'd pay attention. But the electorate doesn't really pay attention.

Steve: No.

Leo: GRC.com - enough politicizing here. Although, hey, this is one case where the

politics has a lot to do with what we talked about.

Steve: It's tech politics, yeah.

Leo: And if people who understand technology don't get involved, well, who is?

Steve: And it's nonpartisan. I mean, everybody's upset about this equally.

Leo: Yeah. We have 16...

Steve: GRC.com.

Leo: Yup, 16Kb audio versions of the show, as well as Elaine Farris's fabulous transcriptions, available at GRC.com. Full quality audio and video available after the fact on our website, TWiT.tv/sn, for Security Now!. And of course you can always watch us do it live, 11:00 a.m. Pacific, that's 2:00 p.m. Eastern time, 19:00 UTC on Wednesdays, right here at TWiT.tv. Steve, have a great week. And I will see you next time on Security Now!.

Steve: Thanks, Leo.