Inflection Points

Description: This week we mix security news and updates with a discussion and analysis of the security industry's evolving reactions to the NSA/Snowden revelations. Steve and Leo examine several of the more significant news items and blogs relating to the issues of widespread Internet surveillance.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-414.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-414-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Lots of news. We're going to talk about PRISM yet again. Looks like Steve was right about the SSL keys, too. And the most amazing memo you've ever heard of from Homeland Security. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 414, recorded July 24th, 2013: Inflection Points.

It's time for Security Now!, the show that protects you and your loved ones online. I'm Leo Laporte. That's Steve Gibson, the Explainer in Chief. Hello, Steve.

Steve Gibson: Hi, Mom. Hello, Leo.

Leo: Does your mom watch?

Steve: No, no, no. Jenny sometimes. When she's, like, really bored.

Leo: Or she wants to be bored. She wants to sleep. She says, "I'll watch" [snoring]. Well, Steve, it's nice to be here on the second anniversary of our move into the new, I still think of it as new, studio.

Steve: Well, and I got a very nice invitation from you guys to come up for it. The problem is I'm in Orange County, and we have basically a shack for an airport, which it used to be. It used to be a shack that was paved. And then of course it grew a little bit. But it's called John Wayne, quote, "International," which is a joke because it has a 10:00

p.m. curfew because the planes fly out over Newport Beach, where all the money is...

Leo: Right, right.

Steve: ...and thus all the political power. So you can't - and so many times when I've been coming across the country, we'll be delayed at O'Hare or something or...

Leo: And now it's too late, right.

Steve: You can't land after 10:00. So then they send you off to, what was that airport you and I - Ontario.

Leo: Oh, no, that's the middle of nowhere.

Steve: I know, and then they bus you, and you end up getting here about 1:00 a.m.

Leo: So you don't want to go anywhere, in other words.

Steve: Well, the point is that the only way to avoid that is to do about an hour and a half drive up to LAX, which is an actual airport. And anyway, so with the logistics of the party you guys are having tonight, and I would have had to spend another night, and basically it would have taken two days out of my life to come up and say hi to everybody. So I thought, well, I'll just wave. See? There, you see, here I am waving.

Leo: We're glad you were here.

Steve: I'm virtually there. And I'll be up later this year to actually be there in person, so.

Leo: Oh, you will.

Steve: Oh, yeah.

Leo: Oh, good.

Steve: Yeah, I'm going to come up. I haven't seen my family for a couple years. And so, yeah, I'm going to definitely come up.

Leo: Well, it's appropriate. That's good.

Steve: Yeah. Yeah.

Leo: So we are having a lovely Italian dinner for 30 after the shows tonight.

Steve: An intimate little thing. That sounds great, actually. Yay.

Leo: An intimate gathering for staff and loved ones.

Steve: You guys have a neat Italian restaurant nearby?

Leo: We have several. It's kind of hard to choose. But we're going tonight to Cucina Paradiso, which is about two blocks from here, and it's fun. Or are we going to - no, we're going to Cucina Paradiso, yeah. So it's fun. I mean, two years. It's kind of hard to believe we've been in here two years. And now we finally have a sign. I don't know if you saw, we put a sign up on the front so people can find us now. For a long time it felt like we were renting.

Steve: Well, believe me, if those are tenant improvements that you've put in, then...

Leo: Well, they are, and we paid for them. We actually are renting.

Steve: Wow.

Leo: But I figure - we've got a lease for a few more years. And I figure by that time we'll want a new studio, so.

Steve: No. No one's ever - you are never moving.

Leo: Well, you know...

Steve: Can you imagine? Can you just imagine doing this again, Leo?

Leo: Yes.

Steve: Everybody would have a nervous breakdown.

Leo: You forget, you forget, I have a whirlwind of a business partner, Lisa Kentzell, who does this in her sleep. She could do it, I mean, seriously, I have no qualms.

Steve: The Indians would revolt. The Indians would...

Leo: No, they wouldn't. They'd stay here, and suddenly one day we'd say, okay, don't come to work, come to the other place, and there would be a new building and a new studio.

Steve: Just magical.

Leo: Well, and the other thing that has to happen is technology moves fast. You know?

Steve: Yeah, but what I really love about the way you built that place is it's modular.

Leo: Right.

Steve: You really can upgrade it incrementally. I mean, it's really cool the way you have that basement that you can just drill right down to and run wires wherever you need to.

Leo: Yeah. And so it's true that we could upgrade technology. In fact, you know, one of the funny things we were looking at at this point, we had a big engineering meeting, is the issue of whether to stay with Macintosh and Final Cut, or to look - because our Mac Pros that we edit with and we render with - you need a high-powered fast machine for rendering, it takes a lot of time, so the more cores the better - are getting a little outmoded. And the new Mac is going to - I'm waiting to see, but I think it's going to be very pricey and not very...

Steve: With that weird little cylinder thing?

Leo: Yeah, because it has no storage. So you have to add Thunderbolt 2 devices, which don't even exist at this point. And it's pretty limited. It certainly doesn't have any upgradeability in terms of video cards.

Steve: You're talking about going pro, outside of the PC world?

Leo: No, we have to go PC. And what it means is we have to abandon Final Cut and go to Adobe Premiere, which is - we'll have to talk to the editors. But I think we'll probably end up doing that because we're really getting to the end of the line on these Mac Pros. So anyway, what happens - and they don't tell you this in the book, build your own studio book. Stuff, it doesn't just stop. Time moves, marches on. And so we'll wait here for a few more years, for sure. But eventually, I think, we'll be moving.

Steve: Would you think you would - the only reason I could ever justify a move is if you

physically outgrew the space. That, I mean...

Leo: Oh, we've already physically outgrown the space.

Steve: No kidding.

Leo: Oh, yeah. They just took my wardrobe. I used to have a nice closet where all my shirts were. They just took it away from me so that Patrick Delahanty has a place, has an office, has a place to be a programmer. So he's in my closet now.

Steve: Oh, okay.

Leo: Well, the reasoning was programmers don't need windows.

Steve: No.

Leo: We put a glass door.

Steve: Sometimes that distracts them. If girls walk by, they just...

Leo: No. Focus. Head down.

Steve: Exactly.

Leo: So Patrick's happy, and I and my shirts are in the back. We literally, we have, Steve, actually - we can't hire many more people. We've actually outgrown it. Now, we're subletting a third of the space to Pixel Corps. But they don't...

Steve: They're still over on the other side.

Leo: They're not showing any sign of moving, so I don't know what we're going to do. Enough about me. Let's talk about - what are we going to talk about today?

Steve: Well, I didn't know what to title this, so I titled it - well, okay. I titled it "Inflection Points" because I'm feeling like from time to time in history there are periods where there's, like, a lot going on. And in fact to sort of kick off the discussion of that in the second half of this podcast, I tracked down, because I wanted to get it exactly right, that recent and sort of famous now Rahm Emanuel quote, "You never want a serious crisis to go to waste." And what I mean by that, says Rahm, what I mean by that, it's an opportunity to do things you think you could not do before. So I want this week to, because this is still, I mean, every blog that I care about, every security site that I look

at, I mean, we're still seeing the people working to understand what the Snowden revelations were about and what the NSA's position means. And believe it or not, it hasn't all been said yet. I've got some really interesting new things that I want to share.

And while I really want to keep us focused on technology, and obviously we were just two weeks ago. We were talking about perfect forward secrecy and what that means with regard to, for example, the notion of traffic being stored and then decrypted later." We'll get back. But I almost feel like it would be wrong for us not to look at what's going on right now, to take a couple weeks when we have to, to say, okay, these things are still happening, so let's discuss some of this, what is still breaking news, essentially. And Bruce Schneier has been writing some fabulous blogs and has some really, I think, insightful analysis of this that I want to share and then we'll discuss.

Leo: You know, it's funny, people say, oh, let's not talk about PRISM anymore. But it's such a story, such a huge story, such a big tech- it is a technology story. If we don't cover it, I mean, you know CNN's moved on. They've got the Zimmerman trial to talk about, the birth of Baby Boy George. And so they've moved on. But I think it's so important that we continue to talk about it, what it means, the ramifications.

Steve: Well, and then I see, even this morning, I start getting tweets from people saying, yep, Steve, you were right again. And it's like, what, what?

Leo: Yeah, the more that comes out, the more accurate your analysis seems to be, yeah.

Steve: Well, and it turns out, I mean, we were just discussing, last week or the week before, this theory I had about SSL keys, the pressure that would be put on. And now comes this morning the story, and we'll be covering it here in a second, that in fact these major providers have been under pressure to turn over their SSL keys.

Leo: Oh, my god. Really?

Steve: Yes. Yeah, you were doing Google this morning while this was happening. And so we have multiple confirmed sources.

Leo: Well, this is it. This is the subject matter of the day. I don't think there's any reason to hold back. Let's launch into it.

Steve: Okay. So first of all, I didn't know where to put this piece because this is crazy. And I didn't want to, like, wait till the end because it might be all anybody remembered, this is so loony tunes. And in fact, almost it's like that crazy - the pilots' names that the station in San Diego made up that got them in so much trouble? My buddy sent me the link to...

Leo: It was local here in San Francisco. I wish it weren't true.

Steve: Oh, was it?

Leo: Yeah, it was KTVU Channel 2.

Steve: Ah. Anyway, I didn't believe it. I thought it was...

Leo: No, I thought it was The Onion.

Steve: Cannot be possible.

Leo: No, yes.

Steve: It could not be possible.

Leo: How could anybody be that stupid?

Steve: Well, in that vein, exactly. If Bruce Schneier, whom we've spoken of often, who is a world-class cryptographer, who has designed several ciphers which are among the best, written several books - "Practical Cryptography," "Secrets & Lies," and there's a third one now that I can't remember the title of. But, I mean, mainstream guy. And so if this wasn't from him, I wouldn't believe it. So this is July 17th. The title of his blog was "DHS" - of course the U.S. Department of Homeland Security - "Puts Its Head in the Sand."

And Bruce wrote, "On the subject of the recent Washington Post Snowden document, the Department of Homeland Security sent this email out to at least some of its employees." So someone forwarded this to Bruce. Bruce redacted the "From" and the "To," and he had to remove some information from the "CC" also. But the subject of this actual - and again, if it weren't from Bruce, I'd go, uh-huh, good, that's funny. But no, this is real.

"Subject: //// SECURITY ADVISORY //// NEW WASHINGTON POST WEB" - this is from the DHS to its employees: "NEW WASHINGTON POST WEBPAGE ARTICLE - DO NOT CLICK ON THIS LINK." The letter reads: "I have been advised that this article is on the..."

Leo: [Laughing] I just read it [laughing]. Go ahead. Sorry.

Steve: I know. Can you believe it? "I have been advised," says this letter, "that this article is on the Washington Post's website today and has a clickable link titled 'The NSA slide you have never seen' that must not be opened."

Leo: If you're in the Department of Homeland Security.

Steve: Right. If you are in the DHS, you cannot click this link....

Leo: Why not, Steve?

Steve: ...on the Washington Post's website. The letter goes on to explain why. "This link opens up a classified document..."

Leo: Yes.

Steve: "...which will raise the classification level of your unclassified workstation" - we're not making this up, folks - "will raise the classification level of your unclassified workstation to the classification of the slide, which is reported to be TS" - that's top secret - "/NF. This has been verified..."

Leo: Now, wait a minute. Now, wait a minute. Wait a minute [laughing]. Okay, keep going.

Steve: "This has been verified by our mission partner and the reason for this email. If opened on your home or work computer, you are obligated to report this to the SSO as your computer could then be considered a classified workstation."

Leo: Mine is because I opened it.

Steve: My god. "Again, please exercise good judgment," says this guy, "when visiting these web pages and clicking on such links."

Leo: Yes.

Steve: "You are violating your Non-Disclosure Agreement in which you promise by signing that you will protect classified national security information. You may be subject to any administrative or legal action from the government."

Leo: Oh, I would just quit. I would just say, you know what, I can't work for somebody so stupid. This is it. I'm leaving now. Here's my response. Is it okay if I click the link and my eyes are closed? Does he, now, he's not implying that the mere display of this JPG will somehow trigger this in my computer?

Steve: Yes. Your computer would then have it in its cache, and this is top secret, and you are not allowed to be in receipt of this information.

Leo: No, you cannot.

Steve: Despite the fact that the Washington Post and everybody else in the world...

Leo: We all have seen it. But it's top secret.

Steve: Yeah, and apparently you have to walk around also with your fingers in your ears because, my god, somebody might echo, they might read it to you, or they might want to discuss it with you.

Leo: This is ridiculous.

Steve: So Bruce says...

Leo: I'm embarrassed.

Steve: This is true.

Leo: These are the people protecting us, ladies and gentlemen.

Steve: Yeah, yeah. Bruce says, "This is not just ridiculous, it's idiotic. Why put DHS employees at a disadvantage by trying to prevent them from knowing what the rest of the world knows?"

Leo: Because it's top secret. They don't know it.

Steve: Bruce says, "The point of classification..."

Leo: Morons. Morons.

Steve: "...is to keep something out of the hands of the bad guys. Once a document is public, the bad guys have it. The harm is done. Can someone think of a reason for this DHS policy other than spite?"

Leo: Oh, wait a minute. Oh, we've got to send out a new memo. Do not watch Security Now!. The slide's on Security - oh, no! Close your eyes, if you work for the DHS. Close your eyes right now. Oh, too late. You've now seen the slide.

Steve: Confess your sins.

Leo: Call the SSO. You're going to have to be...

Steve: You have to go confess.

Leo: You've got to go confess. This is the most - this is the most embarrassingly stupid thing I've ever seen.

Steve: Just unbelievable. Now you know why we had to lead with it, because we couldn't finish with it. The rest of the podcast is serious. But this is just loony tunes. So...

Leo: That makes me sad.

Steve: I had to share it.

Leo: These guys are supposedly protecting us, folks.

Steve: Okay. So CNET this morning, our friend Declan McCullagh - and you might want to click the link, Leo, and look at the page: news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys.

Leo: Yeah, oy oy oy. This is what you said.

Steve: Yup. "Feds put heat on web firms for master encryption keys." The subheading: "Whether the FBI or NSA have the legal authority to obtain the master keys that companies use for web encryption remains an open question, but it hasn't stopped the U.S. government from trying."

Leo: So explain to us what having these keys would do.

Steve: I'm going to share the story here.

Leo: Go ahead, go ahead.

Steve: He really covers it. And then we'll discuss if there's any loose ends. He says, "The U.S. government has attempted to obtain the master encryption keys" - and he'll disambiguate all this in a second - "that Internet companies use to shield millions of users' private web communications from eavesdropping. These demands for master encryption keys, which have not been disclosed previously, represent a technological escalation in the clandestine methods that the FBI and the National Security Agency employ when conducting electronic surveillance against Internet users.

"If the government obtains a company's master encryption key, agents could decrypt the contents of communications intercepted through a wiretap or by invoking the potent surveillance authorities of the Foreign Intelligence Surveillance Act (FISA). Web encryption - which often appears in a browser with a HTTPS lock icon when enabled -

uses a technique called SSL, or Secure Sockets Layer. 'The government is definitely demanding SSL keys from providers,' said one person who has responded to government attempts to obtain encryption keys. The source spoke with CNET on condition of anonymity.

"The person said that large Internet companies have resisted the requests on the grounds that they go beyond what the law permits, but voiced concern that smaller companies without well-staffed legal departments might be less willing to put up a fight. 'I believe the government is beating up on the little guys,' the person said. 'The government's view is that anything we can think of, we can compel you to do.'"

Leo: They might not - go ahead.

Steve: "A Microsoft spokesperson would not say whether that company has received such requests from the government."

Leo: They can't, by the way. We should just point out they probably can't.

Steve: Yes, precisely. "But when asked whether Microsoft would turn over a master key used for web encryption or server-to-server email encryption, the spokesperson replied: 'No, we don't, and we can't see a circumstance in which we would provide it.'

"Google also declined to disclose whether it had received requests for encryption keys. But a spokesperson said the company has 'never handed over keys' to the government, and that it carefully reviews each and every request. 'We're sticklers for details, frequently pushing back when the requests appear to be fishing expeditions or don't follow the correct process,' the spokesperson said. A Facebook spokesperson declined to answer questions."

Leo: Oh.

Steve: I know. "One person familiar with Facebook's internal procedures predicted that the company would vigorously fight a request for encryption keys. Apple, Yahoo!, AOL, Verizon, AT&T, Opera Software's Fastmail.fm, Time Warner Cable, and Comcast all declined to respond to queries about whether they would divulge encryption keys to government agencies."

And anyway, so the article goes on to explain what we already all know, which is this is precisely what we were talking about in the last week or two.

Leo: And to clarify, the real import of this is not so much that they could then watch you live now, although that would be one thing. But more, if they get the old expired keys, that they could go back through the data they've been dumping and decrypt it post facto, ex post facto.

Steve: Yes. So exactly as we were talking about when we were talking about perfect forward secrecy, the adoption of perfect forward secrecy - which is as yet incomplete.

The technology is there. But remember it requires both sides to agree. That technology means that having those master keys would not allow them to decrypt because the master key in an ephemeral key agreement is not used to encrypt the key itself. It is used in all SSL, virtually all today. It's only when both sides agree to this not-yet-in-high-use approach, the so-called, the ephemeral Diffie-Hellman that we talked about extensively - we did a podcast on it - only then would the master key not help. So what they're talking about, and there's still this question, again I will - as I said, the thing that really creeped me out was the idea that all the encrypted traffic is being stored. And when old keys expire, I could just easily see the government, I mean, what we're talking about now is the current key, the key in use.

Leo: Their denial is relevant to the current key only? They might have handed over older keys? Or that just depends on how they parse it?

Steve: Exactly, how you parse the language. If they said, "We have never in our history turned over any encryption keys," then that's broader than "We've never turned over the keys we're using," for example. But you can almost see, and this is why it's so creepy, you could see the government making the case for we don't want to decrypt what you're doing now.

Leo: Yeah, we don't care.

Steve: We want your old keys.

Leo: Yeah, what about the old stuff?

Steve: But what this story says, the government is actually saying, well, and, Leo, get this. I mean, the only reason they want those keys is they're tapping. This also - this is...

Leo: Right. Unless they have the data, you don't need the key.

Steve: Right. This is perfect confirmation that what the government is getting is encrypted data, which also confirms the theory, and we're seeing more confirmation of this coming around, that they're tapping the Internet, and then they're going to the people whose communications is doing the encryption, like Google, and saying we need the keys. And Google is saying no.

Leo: And I think there's legal, and I'm not a lawyer, but legal precedent for getting older keys because you remember that one of the stories was that the law deems email older than six months old as abandoned, that there is no right to privacy to anything older than six months old. It's not yours anymore. It's abandoned. And so I would bet, and again, I'm not a lawyer, but I'm just trying to think logically, that that would be a justification, hey, what we're asking for the keys for is abandoned. It's nobody's email. It's just old stuff. And I think it'd be harder to fight that in court.

Steve: Yeah.

Leo: Anyway. It breaks SSL in the sense that you're encrypted for everybody who doesn't have the key.

Steve: Yeah. I'm thinking that, once I get SpinRite 6.1 launched, I'm going to have to do something I haven't ever done before, which is it's time to do some browser add-ons.

Leo: Well, and look at this. This is from SSL Labs, that SSL report on Google.com. They are supporting a Google.com forward secrecy with modern browsers.

Steve: Yes.

Leo: So your Google searches are protected if you use a modern browser.

Steve: Yes.

Leo: And so getting the keys if forward secrecy is implemented is meaningless.

Steve: Well, so, but here's the problem. Well, almost. Remember that, because most servers don't get implemented on the server side, and only some browsers implement on the browser side, it's only when they both agree that it happens.

Leo: Ah.

Steve: Now there's the possibility of a so-called "downgrade attack" where, when that first packet of ciphers goes off towards the server, somebody who's doing a man-in-the-middle just removes the Diffie-Hellman ephemeral ciphers from the list of ciphers the browser will support, in which case the server will choose one that doesn't have that, and you won't get perfect forward secrecy, even though both ends could.

Leo: Wow.

Steve: Yeah.

Leo: You've got to figure they're working on stuff like that.

Steve: Yeah.

Leo: Every time a more secure system comes up, or a system they can't break into, law enforcement starts to whine "We can't wiretap these people," and starts making moves to getting access to that data once again.

Steve: Yeah. So we're going to come back to this in the second half of the show, some of these issues. I did want to mention the news - and I'm surprised at the persistence of this, Leo. It was last Thursday that Apple announced that the developer site was hacked at Apple.com. And this morning I went there, and the notice is still up, and the developer site is still offline. What's Up says "We'll be back soon." Now, this is almost a week now.

"Last Thursday an intruder attempted to secure personal information of our registered developers from our developer website. Sensitive personal information was encrypted and cannot be accessed; however, we have not been able to rule out the possibility that some developers' names, mailing addresses, and/or email addresses may have been accessed. In the spirit of transparency, we want to inform you of this issue. We took the site down immediately on Thursday and have been working around the clock since then." So now we're at seven days.

"In order to prevent a security threat like this from happening again, we're completely overhauling our developer systems, updating our server software, and rebuilding our entire database." Which this raises more questions for me than it should. They say, "We apologize for the significant inconvenience that our downtime has caused you, and we expect to have the developer website up again soon. If your program membership was set to expire during this period, it has been extended, and your app will remain on the App Store. If you have any other concerns about your account, please contact us. Thank you for your patience."

So it's like, wow, you know, a week. I can't imagine the nature of this, but it doesn't sound like a small problem. It sounds like maybe this never really got the attention it deserved. And when they gave it the attention it deserved, like when maybe some smart people said what happened, the looked at what was there and said, oh, my lord, how has this been allowed to be up for so many years? So apparently they're just rebuilding the whole thing.

Leo: Yeah, from scratch.

Steve: Yikes. Yeah. Now, and so who knows how long. They just said "soon." They're not projecting a time they'll be back.

Leo: Coming up on a week now.

Steve: Yeah. So security, the SC Magazine, that bills themselves the "Security Magazine for IT Professionals," carried an interesting article, not very long, and very frightening. So, and I really can't paraphrase it without changing it, so I'm just going to share it with everybody.

"Hundreds of millions at risk from SIM card vulnerability." This is Monday, two day ago. "Berlin-based Security Research Labs flipped the mobile security market upside-down recently when they published reports about just how vulnerable SIM cards are to cyber

attacks." You know, SIM cards obviously are the little identity cards that many of our phones have that contain their identity.

"Karsten Nohl, founder of Security Research Labs, said his company had been working to crack SIM cards for three years, and they finally found a way to do it - most notably without raising alarms. 'We have a way of breaking SIM cards remotely,' Nohl told SC Magazine on Monday, 'without any evidence and with no way of preventing it or even noticing it.'" So this sounds like a major SIM card security breach, which is effectively all SIM cards.

"An attacker who takes advantage of the vulnerability, Nohl said, will be able to download software onto the victim's SIM card, locate the phone, send texts and make phone calls to any phone number - including pricey premium numbers - and ultimately operate the device as the normal owner would.

"Anything else stored on the SIM card, such as credit card information, is also accessible, said Nohl, adding some finance groups are looking to move transaction payments to phones and that it might represent additional problems since the information will be stored on the SIM.

"What is opening up this kind of vulnerability to hundreds of millions of mobile phones worldwide, out of nearly seven" - okay. Hundreds of millions, oh, out of...

Leo: It's about one eighth of all existing phones. It's not a huge number.

Steve: Okay, "seven billion SIM cards in existence..."

Leo: Sorry. It is a huge number, but it's still a fraction.

Steve: A fraction, "is the use of antiquated DES. That's the Data Encryption Standard technology for over-the-air Short Message Service" - that's SMS - "transmissions used by mobile carriers." So it's not all phones. It's hundreds of millions that apparently haven't moved from using DES.

Leo: It's not any modern phones. It's not the iPhone. It's not modern phones. It's older phones. The problem is there's a lot of older phones in use.

Steve: I'd ask the question, is it older SIM cards, or is it older phones? So it may be the technology in the SIM card.

Leo: Yeah, but if you have an old SIM card, it doesn't work in a modern phone.

Steve: Ah, okay. And so, that's right, so you're getting a newer phone, it's like, oh, sorry, you can't use that SIM card, you have to use the new guy.

Leo: Yes, yes.

Steve: Anyway, so what's going to happen is at the end of this month, at the upcoming Black Hat Conference, we're going to find out more about this. They have notified - they did full responsible disclosure. All the cell phone companies were notified many months ago in order to identify and remove these cards from service and/or upgrade the firmware, do whatever they need to in order to close this hole because a few weeks from now, actually I guess it's next week, we're going to be finding out how to do this.

Leo: Triple, I mean, DES has been cracked for years. Nobody uses DES. It's old. We use 3DES now.

Steve: The problem is the key is too short. DES is a 56-bit key. And so Triple, or 3DES, Triple DES, all it is is three DESes in series, and the key is concatenated. So you take each of the 56-bit keys, and you stick them together to form a composite key that is three times as long, and then you run your plaintext through the first one with the first third of the key, through the middle one with the middle third of the key, and through the last one with the last third of the key. So, I mean, so it's not that DES was ever really a bad cipher, but it's a classic case of it being so old that a key length that used to seem secure is laughable these days.

Leo: Right. This is not probably an issue in the U.S. But in the Third World, and especially in continents like Africa, where they use their phones for e-payments, using things like M-Pesa, that could be huge.

Steve: Yeah. And it must be that this is more than just a short key, or there must be some sort of a hack because, I mean, even if it's an over-the-air attack, it still would be burdensome to do any sort of a brute-force hack. So it can't be that. We'll find out in a week. But, you know, because, I mean, we say, oh, 56 bits, that's nothing. Except remember that 32 bits is 4 billion. So this is, even though it's short relative to any kind of contemporary brute-force attack, you're trying to brute-force something over a cell phone connection. That's still a lot of hacks. So it's something other than a brute-force attack. We just don't know yet. But as you say, it's not to be laughed at.

Okay. Now this is - I got a bunch of tweets from people, and so I was made aware of this. And this is worrisome. The BBC carried the story that the U.K. was proposing requiring ISPs to default block online pornography.

Leo: Isn't that nice.

Steve: Yeah.

Leo: Thank you.

Steve: So...

Leo: It's okay, though. You can go to your ISP and say, hey, I want to see porn.

Steve: Yeah. It's sort of interesting. It says, "Most households in the..."

Leo: [Laughing]

Steve: I know. "Most households in the U.K. will have pornography blocked by their Internet provider unless they choose to receive it," said David Cameron in a speech a couple days ago. He said, "In the balance between freedom and responsibility, we have neglected our responsibility to children."

Leo: No.

Steve: "Mr. Cameron warned in a speech that access to online pornography was 'corroding childhood.' Mr. Cameron also called for some 'horrific'" - his words - "Internet search terms to be 'blacklisted,' meaning they would automatically bring up no results on websites such as Google or Bing. He told the BBC he expected a 'row' with service providers who, he said in his speech, were 'not doing enough to take responsibility' despite having a 'moral duty' to do so. He also warned he could have to 'force action' by changing the law and that, if there were 'technical obstacles,' firms should use their 'greatest brains,'" as he put it, "to overcome them.

"In his speech, Mr. Cameron said family-friendly filters" - which is hard to pronounce - "would be automatically selected for all new customers by the end of the year, although they could choose to switch them off. And millions of existing computer users would be contacted by their Internet service providers and told they must decide whether to use or not use 'family-friendly filters' to restrict adult material. The filters would apply to all devices linked to the affected home Wi-Fi network" - and presumably wired networks - "and across public Wi-Fi networks 'wherever children are likely to be present.'

"Customers who do not click on either option, accepting or declining, will have filters activated by default, said the Tory MP Claire Perry, Mr. Cameron's adviser on the sexualization and commercialization of childhood," when interviewed by the BBC. "The U.K.'s biggest Internet service providers have agreed to the filters scheme, meaning it should cover 95% of homes."

Leo: Unbelievable. Why be a parent? We can let the government do it. You know, let the government raise your kids. That's a good idea.

Steve: So apparently also during this, "Other measures announced by the prime minister included new laws, so videos streamed online in the U.K. will be subject to the same restrictions as those sold in shops; search engines having until October to introduce further measures to block illegal content; and experts from the Child Exploitation and Online Protection Centre being given more powers to examine secretive filesharing networks." Okay. So...

Leo: That should scare people.

Steve: Yeah, I know.

Leo: How would you do that?

Steve: I know. And there was one quote that really gave me a chill, only because this demonstrates the slipperiness of the slope. This Ms. Perry, Claire Perry, who's this advisor on "sexualization and commercialization of childhood," she was quoted saying former child exploitation and online protection center - oh, no, that's the wrong quote. Oh, here. "Ms. Perry argued filters would make a difference, saying that the killers of schoolgirls April Jones and Tia Sharp had accessed pornography before moving on to images of child abuse." So, I mean, it's like, this is all horrible. But as you said, Leo...

Leo: Not to mention millions of other Britons who'd never kill anyone.

Steve: Right, right. It's like the argument...

Leo: And who decides what's porn? Is 500px porn? Is Flickr porn?

Steve: I tweeted this morning, because I was reminded of the famous Supreme Court Justice Potter Stewart, who in 1964 said, when this was at the Supreme Court, "Well, I can't define it, but I know it when I see it." And it's like - and so what I tweeted was "'I know it when I see it' is not a computer algorithm."

Leo: Oh, lord.

Steve: And that's the problem. And then, of course, every time we've tried to do filtering, we've found problems. I was doing a little poking around, and I found a reference to an example under the topic of "Can filters work effectively? Filtering pornography is fiendishly difficult to do accurately. Although the technology is improving, filters set up in hospitals several years ago had to be switched off after doctors were unable to access clinical studies on breast cancer."

Leo: Well, that's got boobs.

Steve: Exactly. Can't have that.

Leo: You can still have Page 3, but you can't have boobs.

Steve: From a programmer's standpoint, one of the worst, one of the most insidious

things - and this is not even programming, but even the law - is a fuzzy definition. I mean, a fuzzy definition gets you in all kinds of trouble. Once upon a time, boy, back in the early history of the podcast, I did a podcast on, like, some of the problems that programmers have. And one of them was fuzzy definitions. If you ever define, like, a variable, and you give it a bad name, that is, you don't name it exactly what it means, or if you're writing something really complex, and you as the programmer aren't absolutely sure what it means, then you're in danger. Whether it's a year later you come back and try to read your code, or even a week later when you're still writing the code, you could interpret its meaning differently. And that's - it's a constant source of bugs is a funny definition of something.

And in the law we see this. You see legislation all the time passed where you have to wonder if they couldn't have gotten it passed with a firm definition, so they softened it, kind of with a "wink wink" to the opposition, saying, well, let us have this, but look at the way we worded this. This won't really be a problem. Which ends up being what they fight over is exactly the fuzziness of that.

Leo: So one of the ISPs in Britain, TalkTalk, is using a system called HomeSafe, which is created by - are you ready? - Huawei, which is owned by the Chinese government. It harvests every URL visited by TalkTalk customers, follows them to each web page, scans for threats, creates a master blacklist and a whitelist of dangerous and safe URLs.

Steve: Wow. So it's full-on spyware also.

Leo: Yeah, among other things.

Steve: Yeah.

Leo: And, by the way, Ms. Perry's website apparently has been hacked and loaded with porn [laughing]. Okay.

Steve: Yeah, in researching this, I mean, it's - as you said, Leo, the question is where is the responsibility. And as you push responsibility upstream, away from the parents of children, I mean, I recognize this is a problem. I mean, there is awful stuff on the Internet. There's horrific imagery that you and I were not exposed to as children. But the problem is unintended consequences. And what's funny is, as I was thinking about this, again from a technology standpoint, the problem, the fundamental problem is the Internet was never designed for filtering. I mean, and in fact just the opposite. The Internet interprets filtering as a problem and routes around it. I mean, it's designed to get data through.

And so it's like, in all these case studies, any time filters have been put up, people get around them. They use proxies. They use VPNs. I mean, the Internet itself is ill-designed to be an enforcement mechanism, which is something we've talked about, come at from all different angles over the years in this podcast. So you're inherently asking it to do something it's not designed to do.

Leo: Well, let's hope it fails in this case.

Steve: Yeah. I mean...

Leo: I feel sorry for Britons. And, frankly, it just makes your country a Third World nation if you filter the Internet. So in the long run it's a very poor strategy.

Steve: Right. If suddenly Google results don't give you the same things because your government has decided you're not mature enough to handle the consequences of the search criteria that you put in, yeah.

Now, this is interesting. I only found one reference to this. But I'm hopeful. And again, Declan McCullagh at CNET does his homework. The headline was "Google tests encryption to protect users' Drive files against government demands."

Leo: Oh.

Steve: I know. And this was Declan. So he said in the subhead, "The search giant is seeking ways to armor user files, sources say, a move that could curb government surveillance attempts. Google has begun experimenting with encrypting Google Drive files, a privacy-protective move that could curb attempts by the U.S. and other governments to gain access to users' stored files. Two sources told CNET that the Mountain View, California-based company is actively testing encryption to armor files on its cloud-based file storage and synchronization service. One source who is familiar with the project said a small percentage of Google Drive files is currently encrypted. The move could differentiate Google from other Silicon Valley companies that have been the subject of ongoing scrutiny after classified National Security Agency slides revealed the existence of government computer software," blah blah blah.

So we know nothing about this yet. But I will definitely keep my eyes open for this. We know that the only way this can be done in TNO style is if there is software in the client and/or in your web page to pre-Internet encryption. And it's entire doable. I mean, and Google's in a perfect place to do this. And the other really significant factor, I tried to - I saw a link somewhere, and I tried to find it again, and I was unable to track it down again. But, and this is really significant: If the provider does not have the keys, then they are not required to hand over any information.

Leo: Ah.

Steve: And so that's the way the law is today.

Leo: Well, and they couldn't. They couldn't, right, if they don't...

Steve: They can't, yeah. I mean, they can...

Leo: Require all you want.

Steve: Yeah. I mean, here's a blob.

Leo: Well, wait a minute. They could get the encrypted blob.

Steve: They could probably get the encrypted blob. They could say we demand this, and then Google says, okay, here you go, but we cannot decrypt it for you. And the point is, in a properly designed system, neither could the government. We have all the technology we need. We just haven't rolled it out yet. And one of the really heartening things about this, I mean, this is why, from the first moment that we covered the Snowden news, I said I'm not unhappy that this happened because in this country we've got to shine light on these things in order to keep this from happening. And as we'll see here in a minute as we continue, this has really raised some ire in important places where I think it needed to get raised.

So congrats, provisional congrats to Google. It would be great if they actually turned Google Drive into a TNO encrypted drive solution. They entirely could. Absolutely, we have the ability to do that, if they chose to.

And I picked up a blurb in the SANS newsletter - this won't come as any news to anyone, but just actually it was a little surprising still - on the horrific state of Java. SANS wrote, and they summarized a bunch of coverage of this, so I'll just use theirs: "According to a study from Bit9" - it's a well-known security organization we've quoted often - "many organizations are running outdated, vulnerable versions of Java." Okay, well, that's not a huge surprise. But here's some numbers: "82% of organizations were found to be running Java 6, which is considered to be the most vulnerable version. Many organizations have more than" - okay.

Leo: I'm glad there's agreement. There's consensus.

Steve: Yes. On one machine. "Many organizations have more than 50 different versions of Java installed on their machines."

Leo: Well, you don't want to get rid of any. They might need them.

Steve: And you wonder, where did those 50 come from?

Leo: Don't they uninstall when you install a new version?

Steve: No.

Leo: No?

Steve: No. This continues, says, "This is due to the fact that the Java installation and update process does NOT remove older versions of the software."

Leo: Unbelievable.

Steve: It just piles up in there.

Leo: Just keep it all.

Steve: You just wonder where those gigabytes of your hard drive are going. Oh, goodness. "Companies would be well-advised to update to the newest Java release, Java 7, Update 25," and counting. And here is the final one: "Less than 1% of organizations were found to be running this latest version of Java."

Leo: What?

Steve: Yeah, 1%.

Leo: One percent, wow.

Steve: And we keep seeing Java exploits are the way people are getting into things.

Leo: Well, we know companies are conservative about, and IT departments, about installing software. But this is one place where it would be better not to be.

Steve: Ooh, boy. So I wanted - one of the things I have on my short list of topics is we're going to go in-depth into PGP because...

Leo: Great, great, great.

Steve: Yes, we need to cover...

Leo: Now, when you say "PGP," we should mention, PGP is a commercial product which is, I think, owned by Symantec now.

Steve: Okay. Then, okay, the PGP protocol.

Leo: You're going to talk about OpenPGP, which is the open source version of that.

Steve: And GPG.

Leo: Which is the GNU Privacy Guard, which is the one I use and a lot of people recommend. And by the way, I've been getting a lot of encrypted email from people, saying, hey, does this work?

Steve: Ah, cool.

Leo: And I'm glad to be the other end of that.

Steve: Well, there is a very slick-looking - I have not vetted it, so that needs to be said - but a very slick-looking $2 app on iTunes for either the iPhone or the iPad, called iPGMail. And you can go to iPGMail.com to get introduced to it. As they say in their description: "iPGMail is an iPhone/iPad app for sending and decrypting PGP-encoded messages. With governments and corporations increasingly infringing upon our privacy, we must take steps to protect our private communications and files. With PGP encryption, you can secure your messages and files to ensure that only the intended recipients are able to read them." So this is TNO for email point to point.

Continuing their description: "PGP is a well-established protocol for protecting data with strong encryption using public key cryptography. It is widely used throughout the world for protecting private exchanges." That's, for example, how Edward wanted to communicate with Glenn at the Guardian. "And now it is available on your iOS-based mobile device for a nominal price, $1.99 U.S.

"With iPGMail you can exchange encrypted and digitally signed private messages with others in your PGP chain of trust from your iOS device. iPGMail is fully functional. It's not crippled with limited functionality to entice you to purchase add-ons, nor does it present you with ads or other nuisances. The app supports key generation, public and private key import and export, and both encryption and decryption of files or email messages. iPGMail supports Dropbox as a way to import or export keys or files..."

Leo: Ah, that's where I keep my keys, good.

Steve: Yup, "...from the app and to enable easier sharing among your devices and computers. iPGMail integrates with the iOS Mail application and" - oh - "integrates with the iOS Mail application and makes the process of sending or receiving secure private messages simple." So I've not checked it out yet. I will. But I wanted to let everybody know. It looks very nice. I mean, they're saying all the right things. $2 is the right price. And for iPhone and iPad, with integration, they also have a developer API where they register their own URL schema, x-ipgmail:, and that allows other apps to interact with it, so they may be able to create an ecosystem around this. And they've fully published it. So it could also become a standard.

Leo: I don't understand how it will work with iOS Mail. I'm downloading it right now and installing it, so...

Steve: Yeah. I haven't yet. But we're going to get into this because this is, sadly, becoming increasingly important.

Leo: Yeah, all right.

Steve: And a very interesting-looking item on Kickstarter that I wanted to give our listeners a heads-up to: an NFC ring that you wear on your hand. You can just Google "NFC ring," and you'll find not only the link to Kickstarter, but a lot of coverage about this because a lot of people are interested. And I expected the thing might be a big, bulky, clunky thing, but it's actually very nice-looking. It's got 25 days to go still, and it just shot past its funding goals. It uses - oh, and Leo, if you want to play the video, it's pretty short. The TechCrunch link there in the show notes, that's got the best of the videos. The Kickstarter video has the guy explaining in much more detail. But the TechCrunch-linked video is very short and has some nice sound in it.

Leo: I like them. They look like wedding rings. You have the U.K. version, but there's a U.S. version, as well.

Steve: Ah, good.

[Begin clip]

NARRATOR: Introducing the NFC Ring, wearable technology that can be used to unlock doors and mobile phones, transfer information, link people, and much more. If you've not heard of NFC, it stands for Near Field Communication, a wireless technology that can transfer data over very short distances. Built into the ring are two tiny transmitters, one for public information, the other for private data. That's all. No batteries. No need for charging. No fuss. Just a low-profile ring that can be worn all the time to help perform everyday tasks simply by touching your hand against an NFC-enabled device.

So, what can it do? It can unlock your NFC-enabled phone without the need to enter a PIN or even touch the screen. Grab yourself an NFC door lock, and it can lock and unlock your door. [LEO: Ooh.] [STEVE: Uh-huh.] Use it to share information, WiFi passwords, link to websites or photos, contact information, or anything else you think is suitable to be shared with your friends' devices. It can be set to hold your public Bitcoin address, for example [LEO: Ooh.] so you can receive payments. Or you could use the NFC Ring to automatically launch apps with custom settings, making it a really easy way to personalize app experiences to match your ring.

On top of all that, the software we've developed is open source, so you're free to invent your own uses and create applications to have it act however you want. This is just the beginning. We've got big plans for the NFC Ring, and we believe that this tiny piece of wearable technology can make a big difference. Thanks for watching, and thank you for your support.

[End clip]

Leo: So does it all make sense?

Steve: It does. There are several things that I like about it. First of all, it is beautiful. I mean, it's just a thin band.

Leo: It looks like a little carbon fiber on the edges.

Steve: The idea is it has an orientation to it, so there is some coloration. About half of the circumference is the public side, which you wear on the outside of your hand, facing the back of your hand. And the inner side is much narrower, about a quarter of the circumference, and that's private. So there's actually two separate NFC systems there, the idea being that the inside of your hand is the personal side, and so that's what you would grab the doorknob with to open, to unlock a door. That's what you, when you hold your cell phone, the ring is up against the back of it, so you're communicating your personal side. But the cool concept is the antenna is much larger on the public side. So any attempt to query this from a distance would get the public signal more strongly than the private signal, so it would swamp the private one. Or at the worst, they would mix together and get no reading at all. Anyway, it just seemed like a nifty thing. I'm glad to know that there's a U.S.-based link because, you're right, I had...

Leo: No, there isn't. I was mistaken. Because it's a U.K. project, I guess everything's in British pounds.

Steve: Ah, okay.

Leo: But it'll convert. I mean, I'm signing up right now. I can't decide, though, if I want the beefy man size. Because it's one size, unfortunately.

Steve: No, no, no. In the small size you do get a range. So you are...

Leo: Ah, okay.

Steve: You're able to tell them what your ring size is.

Leo: And then so the basic, the 18GBP version's gone, but the 22GBP, plus 3GBP to ship, so 25GBP, which is about $35. That's not bad.

Steve: Yeah. Yeah, I don't think it's bad at all. And it's potentially very cool.

Leo: I should warn people, having had some experience with Kickstarter, you don't always get what you pay for.

Steve: May not work out. May not. But, I mean, I would say go there, look at all the videos. The guy's very sincere. He's been, yeah, he's been doing a lot of engineering and forming. He's got a whole boxful of prototypes that he's been putting together. So it

looks like it could happen.

Leo: You can have custom covers. A custom message engraved on the inside of the ring. All for different levels, you know.

Steve: Yes.

Leo: Yeah. Be a good wedding ring.

Steve: NFC ring.

Leo: Give your spouse-to-be your PGP key. She gives you hers. And then you can go off encrypted into the future.

Steve: So today, on Amazon, there are a couple free books offered for the Kindle. One is the very first Honor Harrington book.

Leo: Oh, good.

Steve: "On Basilisk Station." And, Elaine, you'll be glad to hear that I pronounced it correctly.

Leo: Have you been pronouncing it wrong?

Steve: No, no. I didn't know - I think I was originally pronouncing it wrong. And when she heard my horrific pronunciation, she corrected me. Apparently it's, what is it, it's some sort of a...

Leo: It's like a gargoyle. It's an evil creature.

Steve: I thought it was an amphibian thing. I don't remember now.

Leo: Well, you know, there's the basilisk in Harry Potter. But I think it's like half-dragon, half-lion, half - let me look it up on Wikipedia.

Steve: Anyway, it is a great book. If you have a Kindle, if you have not already plowed into the Honor Harrington series, here it is for free. And believe me, this is a tease because you'll end up with the rest of the books, at least the next 14 of them or so.

Leo: In European bestiaries and legends, a basilisk is the King of Serpents, said to have the power to cause death with a single glance.

Steve: Wow. So I don't know how that's relevant to the book because...

Leo: Clearly has nothing to do with the book at all.

Steve: There's no basilisks there. But anyway, it's a great book, it's free right now on Amazon for the Kindle. As is an interesting little, very short story, believe it or not. This sounds like an oxymoron, a Peter Hamilton short story. But actually it is, it's like 39 pages. It's titled "If At First."

Leo: [Laughing] I don't think Peter can really - that's not even a prologue for Peter. That's...

Steve: No, it's not.

Leo: I don't know if he can get started in that short a space.

Steve: Yeah, yeah. And it's a neat story. It's fun. "If At First." It's also free today. And I'll talk about Peter in a second. But since we last spoke, I've read another book, Leo.

Leo: Wow, two. You're good. You're way ahead of the game now.

Steve: Yeah.

Leo: Oh, just teasing.

Steve: I read cover to cover a book titled "House of Suns." It's by a Welsh author, Alistair Reynolds. And he's a well-known sci-fi author. He's known for his Revelation Space series. The first book is titled "Revelation Space," and then he's written other books set in the Revelation Space universe. "House of Suns," I really enjoyed it. And what's cool about it - and I'm always careful never to spoil, and this doesn't. But this explores the idea, not so much of deep space as deep time. Which is a cool idea. In this universe, there is no warp drive. There's no FTL, no faster than light; no wormholes, none of those gimmicks. Einsteinian laws and relativity exist, and they've never been broken. And so humanity has never succeeded in doing anything other than use vast amounts of power to really come close, 99.99999, some nines, close to the speed of light. Well, we know what happens then. You get relativistic time dilation so that...

Leo: I hate it when that happens.

Steve: Oh, don't you? Unless you've on the ship, in which case you come back to the Earth, and everyone you ever knew is just gone, of course.

Leo: Yeah, everybody's dead.

Steve: So the idea, of course, with relativity, is that time appears from the outside frame of reference to be moving very, very slowly at the frame of reference on the ship. So imagine a next, I mean, a culture where the humans are spending a large portion of their time moving around the galaxy at very close to the speed of light. And during the time that they're doing this, civilizations rise and fall. And so they end up at some point at the other end of the universe's or the galaxy's life, and the galaxy is filled with the leftovers. I mean, like, massive huge engineering projects of civilizations long gone and all kinds of cool stuff. So anyway, it was a really interesting read, and I enjoyed it. So if anybody is looking for something, there's that. But, Leo, I have started in on the trilogy.

Leo: Uh-oh.

Steve: Yeah.

Leo: Something else I'm going to have to read now?

Steve: Well, "The Dreaming Void."

Leo: Oh, yeah, I've read that. Thank goodness. Whew.

Steve: Yeah.

Leo: That's a long-ass trilogy, I might add.

Steve: Boy. So everyone knows that Peter Hamilton has never written a short book.

Leo: This is not my favorite, by the way. I'd be curious what your...

Steve: Yeah. I'm...

Leo: There's good stuff in it.

Steve: Yes. I'm enjoying it. I'm 75% through book one. And it's definitely a sequel to "Pandora's Star" and "Judas Unchained," those books, because there's lots of references back to those books. So those are fabulous. I mean, unreserved recommendations for those. But I'm enjoying these. So we'll see. And what are you thinking about "[Great

North] Road"? Or are you still pursuing...

Leo: It's long. I've already - I'm already, like, 20 hours into it, and only about halfway through. I don't know what that translates into pages, but it's long. And it's good. I love it. If you like Peter F. Hamilton, it's just like living in his universe some more. But it has lots of twists and turns, and it's quite the mystery. So it slowly reveals more.

Steve: That's actually the way "The Dreaming Void" - the thing that put me off is that I thought, that doesn't sound like very much of hard sci-fi. I mean, I want hard sci-fi. And, like, some void of dreaming, that seemed a little bit too bizarre, sort of like where "The [Reality Dysfunction]" stuff all went, remember?

Leo: Yeah, yeah.

Steve: They all, you know, like the people - well, I don't want to give it away. But...

Leo: It might not be quite your cup of tea.

Steve: Well, I'm into it.

Leo: Oh, good.

Steve: And what I like now is, I mean, it takes a commitment because he launches about seven threads that aren't at all connected. And you're learning about these very different sort of people, and you're going, why do I care about him? And why do I care about her?

Leo: You will. You will.

Steve: Yes. Oh, I know. And then, then a little - kind of the threads cross over. And it's like, ooh.

Leo: Which one has Al Capone in it?

Steve: That was "The [Reality Dysfunction]" stuff. That was the very first major set of books. And it started off okay. Then it kind of drifted off course.

Leo: I was so sick of it by the end of it. It was like, okay.

Steve: Yeah, yeah. I agree.

Leo: Yeah, that one, not crazy about. Loved "Pandora's Star."

Steve: Yeah.

Leo: And "The Dreaming Void," well, I'll be curious what you think.

Steve: Yeah. I will let you know. So SpinRite, we're continuing to work on it. That's really all I'm going to say is that...

Leo: Good man.

Steve: Yeah, all the PCI enumeration is done. We spent the last week - when I say "we," I mean I and this great team that I've got working with me in the newsgroup. Over last week SpinTest 8 and SpinTest 9 were produced. The problem is that the PC goes back now about 25 years. And some of the things I want to do have questionable levels of support in the BIOS. For example, now we can find all the hardware, but it's necessary to understand what the BIOS sees that SpinRite has found and to associate the BIOS drives with the PCI controllers so that SpinRite can present a coherent picture because you could have devices which are not on the PC bus, which older machines would have, but which the BIOS knows about, so SpinRite needs to. You could have devices which are on the PCI bus, but the BIOS doesn't know about. Remember, famously, Greg spends a lot of time telling people, if the BIOS can see it, SpinRite can work on it.

Well, SpinRite 6.1 won't really care whether the BIOS can see it or not because it'll just nail it right down at the hardware level. But we still - we can't ignore the BIOS. We need to integrate them together. And so there are a number of poorly supported APIs in the past which were giving us grief last week, and we've got it all tamed and nailed down now. And so I'm working on the next iteration of this, which is going to pull it all together. So work is proceeding, and we're going to have a good next release of SpinRite. Which, as I have said before, will be free for all SpinRite 6 owners.

Leo: Aren't you a wonderful feller.

Steve: It's the right thing to do.

Leo: All right. Let's talk about whatever it is. Whatever this means.

Steve: Yeah. I mentioned Rahm Emanuel's famous quote, "You never want a serious crisis to go to waste," which he got a lot of flak for saying, but then that's Rahm.

Leo: A little too honest.

Steve: Yeah. What I think we're going to see - and it's too early to know because we

need to see how this settles out. But certainly there are lawsuits filed. There are hearings being held. The question which we don't have the answer to yet is, post-9/11, was there legislative and law enforcement overreach? That is, did that crisis allow the forces of surveillance in the United States to obtain more power than we wanted them to have? And the arguments are that, fundamentally, due to the secrecy aspect of this, which is, I mean, and this is the dilemma because we're trying to have an open democracy, yet there is a really good case to be made for the fact that some of what is being done needs to be kept secret, maybe, I mean, that's a question, in order to catch the bad guys. I think that's actually not as clear as the surveillance system would like it to be because they would absolutely like to operate with absolute secrecy and just a big "trust us." And the problem is, as we've discussed in the past, that's not worked out well often.

So I feel like we're - the reason I called this podcast "Inflection Points" is it feels like we're at one again, we have been before, a period where there are competing forces and competing motivations and also time is a factor. I remember famously, for example, after the horrible school shooting at Sandy Hook Elementary in Newtown, Connecticut, I was watching the talking heads. And they were all very aware of the fact that right now everybody, you know, emotions were running high. Everybody was upset. Who wouldn't be?

But if the forces that wanted to use this as their big opportunity to further constrain gun rights were going to be able to succeed in doing so, they had to do it quickly. The point was people would forget. As you said, Leo, CNN has moved on to babies from Snowden, and royal births and all of this. So unfortunately this is what happens. I mean, this is the nature of that.

And so on a much larger scale, post-9/11 the country was in shock. And there was a sense of, you know, we didn't - remember, I mean, like restaurant sales dropped because nobody was going outside. We were all watching television. And there was a real concern about what's going to happen next. So it's natural for us to perhaps over-grant rights to law enforcement during that kind of time because we're scared, we're afraid, which essentially is the crux of what Rahm was saying when he says "Never let a serious crisis go to waste." The point is you can use fear. People, forces, can use fear to achieve. Over time we recover. That's what humans do is we understand the way the world has changed, if it has. We accommodate a reality which is different than what we had before that event.

And maybe that accommodation has us always being somewhere else. For example, maybe we will reach the decision that, yes, we want surveillance because we maturely accept the fact that that's the cost of dealing with asymmetric warfare and terrorism. Or maybe we'll say, well, we don't want that much surveillance. Or maybe we'll say we want - you can have it, but you've got to tell us about it. We made a mistake allowing it to be secret. Who knows? I don't know. And I really don't even have a horse in this race. I have no control over it. I'm an observer and interested to see how this turns out.

So just Friday, Ars Technica reported a headline that caught some people's attention: "Snowden be damned: Government renews U.S. call record order." I don't know how that makes sense. But their subtitle is: "Again, feds argue there's no 'legitimate expectation of privacy' over metadata." And so what happened on Friday, and this is interesting also, the Director of National Intelligence, our friend James Clapper [clearing throat], released a statement saying that its authorization, the DNI's authorization to compel telephone companies to share metadata has been renewed by the Foreign Intelligence Surveillance Court.

So what's significant, and I'm skipping down: "The move is particularly noteworthy and

unusual as this type of data sharing had previously been kept from the public." But now, on the other hand, why bother keeping it secret now? The cat's out of the bag. "But now one of the country's top intelligence officials is publicly acknowledging that the FISC" - that's the court - "has sanctioned continuation of its powers. In the new statement, Director of National Intelligence James Clapper wrote that he had declassified some information 'in order to provide the public with a more thorough and balanced understanding of the program.'

"In its new statement, the DNI also wrote, 'Consistent with his prior declassification decision and in light of the significant and continuing public interest in the telephony metadata collection program, the DNI has decided to declassify and disclose publicly that the government filed an application with the Foreign Intelligence Surveillance Court seeking renewal of the authority to collect telephony metadata in bulk, and that court renewed the authority.'

"Meanwhile, the government has formally responded to a lawsuit" brought by the ACLU versus James Clapper, suing - the ACLU, the American Civil Liberties Union, sued James Clapper, arguing "to halt the nationwide metadata spying program. In its federal lawsuit filed on June 11th, the ACLU argued, 'This surveillance is not authorized by Section 215,' which we discussed in our first podcast, 'and violates the First and Fourth Amendments. Plaintiffs bring this suit to obtain a declaration that the Mass Call Tracking is unlawful; to enjoin the government from continuing the Mass Call Tracking under the VBNS order" - and that must be Verizon Business something or other - "order or any successor thereto; and to require the government to purge from its databases all of the call records related to Plaintiffs' communications collected pursuant to the Mass Call Tracking.'"

So this is what I mean when I say we're beginning to see the chips falling and lawsuits being filed and the government responding. And I think, again, this is all good. This is what has to happen. And then at the same time, actually I think this was Monday, so a couple days later, two days ago, the New Jersey Supreme Court unanimously ruled that warrants were needed for phone tracking. Computerworld reported that "Cell phone users have a reasonable expectation of privacy of their cell phone location information, and police must obtain search warrants before accessing that information, the Supreme Court of New Jersey ruled" - oh, I'm sorry, this was Thursday, also last week.

And this was important. They said, although the great quote's here at the end, they said: "'When people make disclosures to phone companies and other providers'" - so this is the court - "'and other providers to use their services, they are not promoting the release of personal information to others,' wrote Chief Justice Stuart Rabner in an unanimous ruling on an appeal. 'Instead, they can reasonably expect that their personal information will remain private.'

"The issue of boundaries in the use of cell phone data by law enforcement agencies has figured in other courts and state legislatures." Yeah, no kidding. "The Montana legislature passed a law recently requiring police and other agencies to obtain a search warrant from a court before tracking a person using location information from an electronic device. Federal courts have been divided on the issue of cell phone tracking by law enforcement. But historically, the New Jersey Constitution has offered greater protection to New Jersey residents than the Fourth Amendment to the U.S. Constitution, Rabner observed. The Fourth Amendment protects against unreasonable searches and seizures."

And so here's the key line in this: "'Under settled New Jersey law, individuals do not lose their right to privacy simply because they have to give information to a third-party provider, like a phone company or bank, in order to get service,' the judge wrote. Evaluating the legal implications of cell phone technology, the judge wrote that, 'as a

general rule, the more sophisticated and precise the tracking, the greater the privacy concern.'"

Well, so that's interesting because it is specifically this notion of third party that the government is using. The end of that Ars Technica story says: "In short, the government is relying on a well-established, but increasingly challenged, part of American case law known as the 'third-party doctrine.' This notion says that, when a person has voluntarily disclosed information to a third party - in this case the telephone company - the customer no longer has a reasonable expectation of privacy over the numbers dialed, nor their duration. Therefore, this doctrine argues, such metadata can be accessed by law enforcement with essentially no problem."

So what we have is we have a confluence of opposing opinions and forces that have all arisen as a consequence of the disclosure, which is why I'm glad that this happened. You cannot do this in secret. We have to have this public for our system to operate.

And then today, on this July 24th, just last night there was some argument in the House of Representatives. There's going to be a vote, may have been by this time, on an amendment to the current, still in work, Defense Appropriations Bill to end the authority for the blanket collection of records under the Patriot Act, which would bar the NSA and other agencies from using Section 215 of the Patriot Act to collect records, including telephone call records, that pertain to persons who are not subject to an investigation under Section 215. So I don't know what the vote was on that. To me this seems premature. It probably did not pass.

[Update 7/25: House voted 217-205 to continue phone taps]

But as I said, we always see that we're initially upset, and then we sort of get used to the new status quo. So the question is, how long does this last? Where do we settle down on what we agree as a society to have in this balance of the need for surveillance and the fact that our Constitution wants to protect and give us individual privacy. House Rep. Jim Sensenbrenner said on the 17th, "Section 215 expires at the end of 2015. Unless you realize you've got a problem" - this was during a meeting in the House, so he was speaking to the Intelligence Committee, saying, "Unless you realize you've got a problem, [Section 215] is not going to be renewed. There are not the votes in the House of Representatives to renew Section 215 at this time." So again, 2015 is a long ways away. Who's to say what position we will have been in, we will be in by then?

And then, finally, I'll wrap all this with - back to Bruce Schneier, who has been blogging brilliantly, I think, about these topics. And he did a blog just yesterday, on the 23rd of July, "How the FISA Court Undermines Trust." And Bruce cited a link to two samples. First was Eric Lichtblau in The New York Times wrote, he said, oh, the title of the story was "In secret, court vastly broadens powers of NSA. In more than a dozen classified rulings, the nation's surveillance court has created a secret body of law, giving the National Security Agency the power to amass vast collections of data on Americans while pursuing not only terrorism suspects, but also people possibly involved in nuclear proliferation, espionage, and cyberattacks, officials say. The rulings, some nearly 100 pages long, reveal that the court has taken on a much more expansive role by regularly assessing broad constitutional questions and establishing important judicial precedents with almost no public scrutiny, according to current and former officials familiar with the court's classified decisions." So that's the first point.

Second is in The Wall Street Journal, an article titled "Secret court's broad interpretation of 'relevant' enabled vast spying. This change - which specifically enabled the surveillance recently revealed by former NSA contractor Edward Snowden - was made by

the secret Foreign Intelligence Surveillance Court, a group of judges responsible for making decisions about government surveillance in national security cases. In classified orders starting in the mid-2000s, the court accepted that 'relevant' could be broadened to permit an entire database of records on millions of people, in contrast to a more conservative interpretation widely applied in criminal cases, in which only some of those records would likely be allowed, according to people familiar with the ruling."

Okay. So Bruce then steps back and gives us, I think, just a perfect analysis. He says, "Surveillance types make a distinction between secrecy of laws, secrecy of procedures, and secrecy of operations. The expectation is that the laws that empower or limit the government's surveillance powers are always public. The programs built on top of those laws are often secret. And the individual operations are almost always secret. As long as the public knows about and agreed to the law, the thinking goes, it's okay for the government to build a secret surveillance architecture atop it. But the FISA court is, in effect, breaking the first link in that chain. The public no longer knows about the law itself, and most of Congress may not know, either. The courts have remade the law, but they've done so secretly, without public comment or review." Which I think exactly sums it up.

Leo: Yup.

Steve: So that's really where we are. The one thought that I had in reading all this, the part, I guess the thing that I wanted to sort of postulate as a solution - because we have a problem here. There are even now defense attorneys, Leo, that are trying to subpoena the NSA records because they believe that they will help their case. And so the argument actually has very, like, some strong legs to stand on, is the government has records which it's using to prosecute. But legal precedent says that the prosecution must turn over all evidence, even if it would be exculpatory, even if it would be useful to the defense. And to the defense attorneys are saying, hey, you've got to give it to us. You've got it. We have a right to use it to, for example, demonstrate that our client wasn't where you are trying to say he was, and his phone records will demonstrate he wasn't. So give us the phone records because you've obviously got them.

Leo: Yeah.

Steve: So the only thing I can think, the only way I can, like, say, okay, how do we solve this problem, is maybe to have an escrow. The problem is that the people who want to do surveillance also want to be the people to have it all. And the argument is that we have short-circuited the traditional process of obtaining a search warrant. Nobody, none of the ISPs, none of the big cloud providers, none of them have a problem. If a judge reviews a case and gives the FBI a warrant for the information, it'll be turned over. That's, I mean, that's fine. The problem is that taps have been installed on the Internet, and all of this data is being surveilled without warrant. I mean, famously, "warrantless wiretapping." Now it's warrantless 'Net tapping. So imagine if this was taken away from the NSA. That is, if the - I mean, I can sympathize with a need to build networks, to follow the call traces of possibly known terrorists, who did they talk to, and even to go back in history. Thus the metadata, the big web that the data can be crunched through.

The problem is it has to have oversight. It has to have - it just can't be that the NSA, who wants to perform the surveillance, gets to have limitless access to this information in secret, and just says "trust us." And, I mean, that isn't the way our system works. And

so the only thing I can think of, as I look at the technology, coming again from a technology standpoint, is that there is an escrow; that all of this data is held, and by - give it to the ACLU. They certainly aren't going to turn it over without due process. And then return to the process of a judge saying, issuing a formal search warrant for search of specific individuals in this network, and then turn over that data. That's the only solution I can see. Either that, or we just decide, okay, we live in a world where our government now needs to watch everything we do, and so be it.

Leo: I'm afraid the latter seems the most likely outcome.

Steve: Yeah, well...

Leo: But we'll do our best.

Steve: It gives us lots to talk about on this podcast, about TNO technology and end-to-end encryption and how we can, I mean, I hate the idea of needing to hide from the surveillance state. And again, my favorite quote from someone who tweeted it is when people say, "Well, why do you care about encryption if you have nothing to hide?" To which the response is, "I have nothing to hide from people I trust."

Leo: Simple enough.

Steve: Yeah. That's just exactly it. Yes, I...

Leo: That's a small subset of the total population.

Steve: Yeah.

Leo: Steve Gibson is...

Steve: And we know about the danger of Big Brother.

Leo: Yes, we do, unfortunately. Steve Gibson is at GRC.com. That's his website, Gibson Research Corporation. You can find him on Twitter, @SGgrc. If you go to GRC.com, you'll find of course lots of great stuff, including SpinRite, the world's best hard drive maintenance and recovery utility, and 16Kb versions of this show for the bandwidth impaired. Transcriptions, too, by an actual human being who can spell and say "basilisk," Elaine Farris. You can find full-quality audio and video at our website, TWiT.tv/sn. And of course subscribe. You'll get this show whenever it comes out on our favorite device. There's lots of podcatchers out there now, plenty of ways to get Security Now! automatically.

If you'd like to watch live, we'd love you to do it: 11:00 a.m. Pacific, 2:00 p.m.

Eastern time, 19:00 UTC, every Wednesday. That's when we open the cameras and let you watch us record the show live. And of course the chatroom is always a big part of the show. Hey, thank you, Steve Gibson, for being here.

Steve: Always glad to be.

Leo: If you've got a question for Steve, he's going to do, time and security news permitting, a Q&A episode next week.

Steve: Yeah, we've got to get back to our questions. So we'll do, definitely do listener questions next week.

Leo: So go to GRC.com/feedback and post a question or two.

Steve: Please.

Leo: And we'll answer as many as we can next week. Thanks, Steve. Have a great week. We'll see you next time on Security Now!.