SECURITY NOW!

Transcript of Episode #378

Microsoft: Security, Privacy & DNT

Description: After catching up with an interesting and varied grab-bag of security news and paraphernalia, Steve and Tom further examine the controversy surrounding Microsoft's decision to enable the Do Not Track (DNT) "signal" header in IE10 and share some insights gained from a recent Microsoft Executive VP Keynote presentation about exactly this issue.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-378.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-378-lq.mp3

SHOW TEASE: Coming up on Security Now!, I'm getting to fill in for Leo for another week. And Steve Gibson and I have got some great stuff to talk about, including Microsoft's Do Not Track. They have it on by default. Why is that? We'll get into that, plus a look at the interesting story of John McAfee and a Skype vulnerability. All that and more coming up.

TOM MERRITT: This is Security Now! with Steve Gibson, Episode 378, recorded November 14th, 2012 - Microsoft: Secrecy, Privacy and DNT.

It's time for Security Now!, the show that helps you learn about all the dangers online and take some action and maybe keep yourself a little safer, at least as safe as you can try to be. I'm Tom Merritt, filling in for Leo Laporte for a couple weeks while he's off on a cruise. Which is fun for me because I get to talk to this man right here, the brains behind GRC.com, Mr. Steve Gibson. How's it going, Steve?

Steve Gibson: Hey, Tom. It's great to be with you again, for the second week in a row. And we've got one more next Wednesday, the Wednesday before Thanksgiving.

TOM: And we've got some good stuff to talk about today. We're going to get deep into Microsoft and Do Not Track.

Steve: Yeah. What happened is a couple things came together for me. They released, and I tweeted yesterday on my Twitter feed, the link to their preview of IE10 for Windows 7. So we had heard that they were going to make IE10 available for Windows 7. It's now in preview. I wanted to experience this, what does the user see when they install IE10, because we heard that there's, like, some opportunity to turn off the default-on DNT header. So that was one aspect, and we'll talk about that, and where the setting is, and how well buried it is. It's sort of a compromise between Chrome, where you just cannot find it, and Firefox, where it's really where it should be. My hat's off to Firefox.

But then the other thing that happened was, in digging in, I found a couple weeks' old transcript of a relatively short, it's probably about 10 minutes, keynote which was given at the recent 34th International Conference of Data Protection & Privacy Commissioners by Microsoft's general counsel and exec VP who's in charge of all this, Brad Smith. So, and what I loved about it is it gives us a rare insight into what Microsoft is really thinking, that is, why they've done this, what they think about it, and why. So I want to share that with our listeners and discuss it, and then also some of the other things which have come up, like the fact that Apache's decision to strip this from client queries was anything but smooth. It was very controversial. And of course we have all of our news of the week. So all kinds of good stuff.

TOM: Yeah, I'm looking forward to that. Some interesting news. We've got a Skype vulnerability to talk about that's kind of come and gone this morning, or how gone it is, we'll talk about that. And also the strange adventures of Mr. McAfee to talk about, as well. So let's start off with Patch Tuesday stuff. What should we know about this Patch Tuesday, Steve?

Steve: Well, it's your generic second Tuesday of the month. We do seem, I don't remember now, somebody observed that we seem to see an alternating pattern, and it's holding up now many months. This is another month where we're seeing an alternating pattern of large and small Patch Tuesdays, this month being a big one. So I guess it's the odd months that have the large Patch Tuesdays. And so far, for like the last running six or seven months, the even months have not had very much going on. So this is one of the big ones. Everything requires that you reboot. So sometimes you can get some things like the .NET v4 stuff can update without requiring a reboot in some cases. No chance this time.

TOM: Yeah, I know. Those are rare pleasant moments when that happens; right?

Steve: Yeah. So four of their updates are rated critical. And in this case that means they all provide for the attacker who exploits these vulnerabilities, the ability to remotely execute code in your machine. So one of the updates fixes three privately reported vulnerabilities in IE. Which, being in IE, it's your standard "visit a page and get pwned." Another update repairs two privately reported vulnerabilities in Windows Explorer. And this is kind of weird. This one is, if Windows Explorer browses a specially malformed Windows Briefcase file...

TOM: I'd almost forgotten about Briefcase. Do people still use that?

Steve: Microsoft is slow, or I would say never, except they don't support 16-bit code anymore, to my annoyance, in Windows 7. But they're slow to ever stop doing anything they used to do. And since they used to have Briefcases, they still have Briefcases. And here's a perfect example of old code which is biting us on the butt because, as you said, who does that anymore? Yet it's there because they want to be backward compatible. And in fact all of these updates affect every supported version of Microsoft operating system, and even those that are no longer supported, but we don't care about those because that's what "no longer supported" means.

TOM: Yeah, right.

Steve: So the second of these critical ones was, if someone sent you a malformed Briefcase, and you browsed it in Windows Explorer, not Internet Explorer, the standard Windows Explorer, the Windows drive browser...

TOM: Yeah, file Explorer...

Steve: Yeah, that could take over your machine. Then there were five privately reported vulnerabilities in the .NET framework. And the most severe of those is another one of these weird things. If your system encounters a malicious proxy autoconfig file, then someone, some clever person found a way of taking over your computer by planting a malicious proxy autoconfig file. So that is able to then inject code into the currently running application and take over your machine. So that's not good.

TOM: No, not at all.

Steve: And then - although it is kind of obscure. And then finally, the last of the four critical updates fixes three privately reported vulnerabilities in the kernel's handling of TrueType files. And this is another one of these where it's like, okay, the kernel, no OS kernel should be involved in rendering fonts. But that was a decision Microsoft made, back when we didn't have enough performance, to move the GDI, the graphics device interface, down into the kernel for the sake of performance so that you didn't have as many user space to kernel space transitions of code crossings, each of which requires some substantial overhead. So they decided to do that. And now they're paying the price of a very high level of complexity, which is what TrueType rendering involves, where little mistakes get found and can be leveraged. And if it were in user space, it would be, like, your app would crash. In kernel, you get to have your OS taken over.

TOM: Just because you weren't using Arial.

Steve: Exactly. So anyway, so they fixed those big four things. Then there was what they call an "important" update, even though - that is to say, not critical, just important in this criticality rating system that they have now. Even though it's a remote code execution, for whatever reason, it didn't rate critical. However, it seems bad to me because there's four privately reported vulnerabilities which this important update fixes in Excel, where your standard opening a specially crafted Excel file, the attacker is able to obtain the same rights as a currently logged-in user. Maybe that's why, because you don't get system privileges. You just get current user privileges.

TOM: That would make sense, yeah.

Steve: So you don't have that much power. So it's like, yeah, it can execute code, but so it pops up Notepad. Okay, who cares? And so, and finally, the least significant one was just a so-called "information disclosure" vulnerability which they rated as moderate. However, one of them was public, and one was supported privately. And this is, interestingly enough, in Microsoft's web server, IIS.

The more severe of the two, and it wasn't clear to me whether that was the publicly reported one or the privately reported one, but it could allow what Microsoft calls "information disclosure," and that's not disclosed any further, if an attacker sends a series of specially crafted FTP commands to the server. So you first of all have to be running the file transfer protocol, FTP, of IIS, not just web, HTTP and HTTPS. You have to have it as an FTP server. And apparently someone figured out how there's a way you can ask it some things through FTP and gain information which you're not supposed to be able to gain. So that's our Patch Tuesday. Basically just do it. Find a good time to do it. Probably sooner would be better than not.

TOM: Usually.

Steve: This all came out yesterday. When I turned on my Win7 box, which I'm using here, where I have, for example, IE10 now installed, I was told that there were seven things that needed updating. So that was the intersection of those updates and my particular system characteristics. Various people will have different numbers that need to be updated.

TOM: Right. If you don't have Excel, they're not going to patch Excel.

Steve: Exactly, exactly.

TOM: Okay. So I'm really interested in this Skype password reset issue. The Next Web is where I saw it this morning. They said they had alerted Skype about it a few hours before they posted it. But essentially it was dead simple. All you needed to know was an email address.

Steve: Well, okay. This is, first of all, what's troubling is that it had been posted two months ago in a Russian online forum. So for two months some subset of Russians, Russian speakers, knew about this. And that information didn't get to Microsoft, that of course as we know famously purchased Skype a couple years ago. And this is a classic mistake. This is not buffer overrun. This is the sort of mistake - and by the way, I agreed with your CNET reporter who you had on just before this podcast. He was sort of musing about asking the question, how much other stuff like this exists? But I'm getting ahead of myself.

TOM: Yeah, makes you wonder, for sure. How does it work?

Steve: The hack was not a coding error. It was a design error.

TOM: It almost makes you want to hesitate to call it a hack because it's a design issue that people just figured out how to take advantage of.

Steve: Right. So if you know - okay. I should say "knew." If you knew. I'm using the past tense because this no longer works. Microsoft shut down the vulnerability, the aspect of vulnerability, which was password recovery. They took that part offline immediately, then looked at the problem, understood it, fixed it, and then brought password recovery back. So that's what I mean by this being a design problem. As soon as someone told them, they're like, oh, my god. And so it was easy to fix. So here's what it was. All you had to know was somebody - and so my point is, nobody is at risk now. So this is informational.

TOM: Right.

Steve: This is not anything anyone needs to run around and change anything or do anything. And Microsoft's logs did notify them of where this may have happened, and so Microsoft is proactively notifying Skype users who may have had this happen to them. So if you don't get email from Microsoft, then you're okay. And probably apparently most people are okay. I mean, this - somehow this existed for a couple months and didn't cause a huge problem.

So knowing some Skype user's email address - and so here we have the instance, again, of unfortunately an email address being less easy to just make up at random than a username and password. Those we can make up at random. And any savvy Internet user knows you don't want to reuse passwords. But email addresses, there are some services that let you create them. And we've talked about, for example, in Google Mail you can put dots in them, and the dots aren't lexically important for the parsing of the name in front of the "@" sign. So you can kind of come up with different hacks for inventing email addresses for yourself. But typically people who register for Skype will use their main email address.

TOM: The email address is not supposed to be something you need to defend against.

Steve: Precisely. So it turns out that Microsoft was allowing somebody to create a new account with an existing email address.

TOM: First mistake, right there; right?

Steve: Yes. And it would notify you. So you create a brand new Skype account with an email address of your target victim. And Microsoft says, oh, this email address is already in use...

TOM: So they knew.

Steve: ...by somebody else. Are you sure you want to proceed? And so the hacker says, absolutely.

TOM: Of course.

Steve: Yes, please. And so it creates your account. Then you log into the Skype client with your new account that you just created with this other person's email address. And then you say, oh, I need to reset my password, and I don't remember what it is. So the password reset response, because it's more than email, there is an email sent to that user's email address.

TOM: So unless you've hacked into the email address at this point, you shouldn't get a reset token. Right?

Steve: Well, no. Because what happens is...

TOM: Uh-huh.

Steve: It also, being helpful, it also sends a reset link and reset token to the client, to your currently logged-in Skype client.

TOM: Now, I guess the thinking there is, if you're already logged in and authenticated, it's guessing that you are the actual user. But because of this earlier problem where they said, hey, we see it's the same address, so but we'll let you make an account anyway, that's not secure anymore.

Steve: Yes. Exactly. So what happens is you then get a link to reset your email address. Click the link, provide - you're forgiven for not knowing the old password. You provide the new password. And you have now taken over that user's Skype account and locked them out, since they no longer know the new password you've just set. Whoopsie.

TOM: Yes. I mean, at least it was easy to fix; right?

Steve: Yeah. And again, it was, I mean, this is a mistake, in trying to be helpful and friendly. And this problem probably has always existed. I don't know - I don't remember ever having done this. I've never forgotten my Skype password, so I haven't done a Skype password reset. But I wouldn't be surprised if, 10 years ago, this functionality was there, and this same thing probably happened. This is one of those problems, and this is the point that your CNET reporter guest made in the prior podcast, was these sorts of things are around. I mean, you might argue, for example, that some of the way Mat Honan got hacked was this sort of exploit, where it's a series of decisions which, when put together in a particular way, allow the hacker to obtain rights that they were not meant to have.

TOM: Well, exactly. It's found. It's fixed. Everything's okay now. But it does raise that little niggling worry that there may be other things like that.

Steve: Well, and it's a perfect, I mean, for this podcast it's a perfect case in point. We talk about these sorts of things all the time. Here's a clever hack around some features that took advantage of that.

TOM: Now, this next story gives me the heebie-jeebies. Scanning a CAB file with Symantec Antivirus actually leads to a system compromise?

Steve: Yeah, this is the danger, of course. It's not as if the A/V software is immune from coding errors. I mean, why would we think it would be? Writing software...

TOM: Why couldn't it have a coding error, yeah.

Steve: Writing software that is flawless is really, really, really hard and really, really, really expensive. So almost no one does. Everyone would like to. But it's not cost-effective, frankly. So it doesn't happen. So here was a case where a hacker discovered that an earlier version, which apparently is still widely deployed, this is the Symantec Endpoint Protection 11, is using an older scan engine than their current release, which is 12.1. They are not going to fix 11.

So there is action required on the part of any individual or corporation who may still be using the v11 of the Symantec Endpoint Protection System because a deliberately malformed CAB file - which is sort of Microsoft's format for ZIP files. It's a large-buffer, high-compression packing of executables and other files. CAB is short for cabinet. It's sort of like their equivalent of a ZIP file, their own format. And so naturally A/V needs to look into this compressed archive in order to see if there's bad stuff in there. Well, some small detail of the way they're doing that, it was exploitable in this v11 of the Symantec Endpoint Protection such that, when the antivirus scanned a virus, it got owned.

TOM: So it's like opening the can of peanuts and then it just comes right out at you.

Steve: And the gotcha here is that the attack would be specific for this particular problem, meaning that, if you weren't scanning the CAB, or if you didn't have Symantec Antivirus, this Endpoint Protection v11, this bad thing couldn't hurt you. It's only if you were looking for it, would it then say, aha, I got you, and take over your system. So a little reverse on that one.

TOM: So what do you do to fix it?

Steve: You just need to update to 12.1.

TOM: Okay. That's easy.

Steve: So anyone using 11 - and it wasn't clear about 12. There was some - let me see. Oh. Symantec also reports that Symantec Endpoint Protection 12.0 is affected. So that was later on in the news. So 11 and 12 are a problem. You need 12.1 in order to be safe.

TOM: Got it. All the way up to 12.1.

Steve: Yeah. And there is a US-Cert note about this for anyone who wants to pursue that further [kb.cert.org/vuls/id/985625]. I'm sure Symantec has some stuff, too.

Now, a bunch of our listeners have been asking me about a cloud-based Amazon - and actually Amazon is just one of many cloud providers that a Windows-based archiving tool known as CloudBerry supports. The reason this has come up is that I've talked about several times now ARQ, which is Mac-specific, only runs on the Mac. And the author of ARQ has on his home page that, if you're a Windows user, you might want to go look at CloudBerry. So a bunch of people have tweeted, and I've seen email, people saying, hey, Steve, can you tell us, did they do it right? It apparently supports encryption. Is it secure?

The other event is that it supports the newer Amazon S3 super-inexpensive, long-term archiving system. Remember we talked about it. We talked about it actually with regards to ARQ because ARQ added support. And that's only a penny per gigabyte per month. So it's super nice if you want to stuff things away in the cloud that you do not need real-time access to. The way you do it is you submit a request to the Amazon S3 system, and they say between three and five hours later they then make it available for you to download. So that's great for, like, long-term archiving.

TOM: For stuff that's not time sensitive, it's perfect.

Steve: They had reached out to me back in May, that is, the CloudBerry folks had, and then again last month. And I had just - it's one of those things where I've got so much going on. I had intended to get back to them. But the recent pressure from Twitter followers saying, hey, Steve, what about CloudBerry, I finally replied, apologized for not getting back to them sooner. And I said, okay, so I need to know what's going on with your crypto. How have you done it? Because, I mean, it's all very pretty-looking user interface. It's got the checkboxes with all the bells and whistles. But all they say anywhere is "We do encryption." Okay, yeah.

TOM: Is it ADS? Are you hashing, or is there salt...

Steve: Oh, I got it. I mean, very much like everything else, there's one way to do it right, and every other way is wrong in some way. So it's just not easy. So just late last night - I had this dialogue, I guess, at the beginning of the week. So they were pretty quick in responding. Late last night I got a note from my contact there and also the name and address of their crypto guy. And so it's a good sign that they even have a crypto guy.

TOM: Yeah, that's true.

Steve: It's almost like, here's our crypto guy.

TOM: That would be very worrying, if you're like, what's your encryption like? None of us really know.

Steve: Yeah, we just turned the checkbox on when we built the app. Anyway, I did a quick glance over what they're doing. And so this is not my endorsement yet. You get that next week. But the good news is I think I'm going to be able to give it next week because everything I saw and everything they said, though I literally just scanned this document, looks exactly right. So all the buzzwords were there. PBKDF2 and hashing and separate initialization vectors and all the right things. So I will spend time with it this week, make sure that it - and I've got a good guy now to ask questions of.

And so I expect next week to be able to give a solid security-facing endorsement about CloudBerry. Which does meet my other criteria. You buy it once. You're not renting it. You buy it once, and then you - with nice terms and conditions, there's a trial period. It's $29.95, and it gives you access to a huge array of cloud-based services, not just Amazon's S3 service. So I'm very pleased by what I saw. So I wanted to close the loop for our listeners, that I saw your tweets, and I'm on it.

TOM: Good. I can't wait to find out about it. I'm always interested in more of these things. I want them, ideally, to be cross-platform because I work in so many different operating systems. But I understand that's not necessarily typical. So I usually have to wait a little while. Tell you what, the one nightmare, though, is authentication, and I use things like LastPass. They're a great, sophisticated Band-Aid over the problem of authentication. But I want to heal the wound. I want OneID. Do we have an update? Do we have another contender here?

Steve: Well, okay. So I've been aware of the service known as OneID for a while. I've met its founder, and he describes himself as a "serial entrepreneur," Steve Kirsch, who's well known up in Silicon Valley.

TOM: Heard the name before, definitely.

Steve: I met him at a privacy conference a year or two ago. He's born in L.A., actually on Christmas Eve. He's one of those poor guys whose birthday is the 24th, so their birthday and Christmas were always stuck together.

TOM: Saved money on presents for some people, yeah.

Steve: Yeah. And went to MIT. I remember his name first from a company he founded called Mouse Systems. And Tom, you were probably still running around having birthdays with single digits at the time.

TOM: Mouse Systems, huh? Yeah, I don't remember that one.

Steve: Mouse Systems. It was a very nice, the very first optical mouse. It was a square device with - I think it was a three-button mouse. And it needed, unlike current optical mice, it had its own optically encoded mouse pad.

TOM: I was 12. I'm looking it up. In 1982, when it came out, I was using my TI-99/4A.

Steve: Anyway, it was my favorite mouse. It's the mouse I used. It was state of the art. It had a higher resolution than other devices at the time. It had sort of a two-tone grid that it used. But anyway, he was the first. And he has a patent on that technology, the first optical mouse. Mouse Systems were the people who did it. He was also behind FrameMaker with Frame Technology Corp., another successful company.

TOM: Oh, yeah, I used FrameMaker, definitely.

Steve: He was a founder of Infoseek.

TOM: Oh. I used Infoseek, too, yeah.

Steve: Yup. And also two companies, Propel and Abaca. And so now he's on to the question of identity. Now, hope springs eternal. I mean, how many times, I mean, identity is probably the No. 1 big topic on this podcast because I recognize it's a problem we have to solve. The advantage that LastPass has is that it works now on everything. It does so by running in the browser, leveraging JavaScript to cryptographically store and safely fill in the fields prompting you for data on websites. What Steve and his gang have done is they've decided to try to obsolete user logons and passwords.

TOM: All right. Sounds like OpenID so far.

Steve: Well, the challenge is - and I would just blow it off if this wasn't Steve Kirsch because he tends to succeed at these things. I don't know if he can succeed at this. Which is why all I can say is I'm hopeful. Because it requires that every site that you use it with modify itself for OneID. So this is not a solution that you can get and start using all over the Internet. Instead it will be a matter of, like, Amazon being convinced to do this, and then they will say we support OneID. And Facebook, and MSNBC, and CNET, and CNN, and...

TOM: Well, then, if Facebook would get onboard, conceivably that could take a bunch of sites who use Facebook as their login credential with it. So that could be good.

Steve: Well, yeah. So if you replace, if you completely replace the existing authentication model, such as it is, which really amounts to who are you and what's your password, if you just say, well, we're going to ignore all that and come up with a better system, well, then, frankly, it's not hard to fix this problem. And they're offering a solution.

So this comes up because I've had a lot of people asking me about it. And the technology looks solid. They've got crypto guys. They've got a cute little animated presentation on YouTube. It's got arrows pointing in each direction, and there's, like, nine of them, and it bounces around between things. And I'm not even, I mean, it's like, okay, that sounds good.

I've asked them for formal crypto documentation and never received any. I think there isn't any, or they just haven't had to do it yet. I don't know how they could exist without that, but apparently it doesn't exist, or they don't want to share it with me. I don't know. But it doesn't really matter because, unless it achieves critical mass, then it will be another proprietary attempt at doing this. And then there's the - at no point does it cost the user anything. And Steve's been a little cagey about that, where it was like, well, in the beginning it doesn't, until you start really using it a lot or something. It's like, okay, well...

TOM: That's interesting.

Steve: Well, so this isn't - they're sort of like, oh, don't worry about the man behind the curtain. So it's like - so I'm hopeful. We'll keep our eye on it. We'll watch it. We'll see how it does. If it starts to gain traction, then that would be a good thing. The problem is it is a recentralization of authentication. And that's my only real objection. We have a problem. But the idea is, do we want some one company to own authentication for the Internet? We all know the answer is no.

TOM: Yeah.

Steve: Of course not. We want a solution which is not a proprietary service of one company. So that's a concern. Steve would like to own authentication for the entire Internet.

TOM: I suppose anyone might, yeah.

Steve: Yeah. So I understand that. But that, to me, it's like, okay, that's going to be a heavy lift. But we'll see.

TOM: As soon as we're done with Security Now! today, I have to rush right across the hall to Pixel Corps and shoot the latest Sword and Laser, which is my sci-fi and fantasy show I do with Veronica Belmont. But I get a little taste of sci-fi right now. You've got some sci-fi stuff in the lineup today.

Steve: Well, it was just - yeah. It was a tweet I got from Joe Kelley, who tweets as @sandpvrr from the Great State of Maine, as he puts it. And I just saw this come by, and I wanted to share it with our listeners. He said: "@SGgrc Audible has the 'The Lost Fleet' series in their 50% off sale. I got all six," he tweeted. And that started six years ago, in 2006, was "Dauntless." Then two novels the following year, "Fearless" and "Courageous." Then one, "Valiant," in '08; "Relentless" in '09; and "Victorious" in 2010. And I have spoken of this series many times before. I really enjoyed it. And what was fun was that, although it maybe got a little tedious, I think I'm only saying that after the fact because I had to have more.

And this doesn't give away anything of the plot to say that somebody who was in cryo sleep for a hundred years is brought back to consciousness and a little more slowly to full health. And it turns out that the war he participated in the beginning of is still raging, a hundred years later. Yet everyone has forgotten how to fight space battles where you have acceleration and inertia and speed-of-light delays because all the people who used to know how to do that got killed. And junior officers replaced them, and they've ended up with this dumb strategy of just charging head-on into your opponent and firing all phasers.

And so this guy comes along at an inflection point and says - and, oh, oh. Because he's a hundred years old, he's got seniority, even though he's been out of the game for a hundred years. So he doesn't know what button to push on the console because that's all changed. But what he understands, he has sort of classic space combat training. And let me just tell you. None of this disappoints. It is really good because he sets up situations and strategies and puzzles and solutions which all involve thinking ahead and dealing with the fact that we just can't beam ourselves from Point A to Point B. We don't have science fiction technology. We have actual, you've got to start accelerating and slowly increase your speed. Now you're going fast, and you can't stop instantly, so what are you going to do? So anyway, really interesting stuff. So I wanted to share the fact and thank Joey for sharing that with us. And for anyone who likes to listen rather than read visually, Audible has all six of these half-off right now.

TOM: Buy six for the price of three, essentially. We've still got a little bit of news to get to. I want to get to the John McAfee stuff. But we do have some IE10 news we need to talk about first?

Steve: Well, this really bears on today's topic. I encountered a couple days ago the fact that there was a prerelease preview of IE10. I have installed it this morning because I wanted to get the install experience, as I mentioned at the top of the show, to see what it was that Microsoft showed us about the Do Not Track header, which is the main focus of this podcast, once we catch up with all of this week's interesting news. And actually we have gossip here in a minute.

But so I did tweet the link. It's a little hard to find, actually. I should have just looked at my own Twitter feed to get the link because I tweeted it a day or two ago. So you can easily find it if you just go to Twitter.com/SGgrc. And it's one of the top, most recent tweets from me, anyone who wants to play with IE10. It looks exactly like IE9. But I am in Windows 7. I'm not in Windows 8. So I'm not having any Metro experience, although the scroll bars went flat on me.

TOM: Does it update both IE10s, the Metro and the desktop version in Windows 8? I assume so.

Steve: Well, I don't know because I'm still using Windows 7 on this machine. And in fact one of the links I went to when I was looking for the IE10 prerelease preview tried to upsell me to Windows 8. And I was surprised. I think it was, like, $29 or $39 or something. It was like, oh, that's not that bad. So they're certainly trying to move people forward. So I just wanted to let people know IE10 exists now in prerelease form for Windows 7.

TOM: I just asked a stupid question earlier, by the way, because Windows 8 ships with IE10. So, exactly.

Steve: So the other bit of confusion, when I tweeted this, I got some tweetback saying, what? IE, come on. Now, it's like, hold on, listeners. We all know I'm using Firefox. And if Chrome ever gives me fabulous tabs like I have with Firefox, then I'll be probably switching to Chrome because Chrome's feature set is moving along nicely. Although I did mention last week how Chrome is now offering per-site settings for, like, script management, for taming JavaScript. And we talked about how you can change the defaults to not run JavaScript unless I permit it for a particular site.

And I did see feedback, it was either a tweet or mailbag, from someone saying, ah, but, Steve - I think it must have been a tweet because it was since then. He said, "Ah, but don't you wish it also had 'Enable it for this session only'?" And it's like, oh, I do wish that because that's one of the things I love about NoScript over on Firefox. I use that all the time, where I'm never going to come back to this site, but it's doing something annoying. It's broken without JavaScript. So let me turn on JavaScript just for now, but I don't want to clutter up my list of persistent permissions with endless domain names of places I'm probably never going to come back to. So I use the "Yes, enable it just for this session" all the time in Firefox.

So anyway, I'm telling people about IE10 because it still has 54 percent of the market share. I mean, it's an important browser. It's what everyone who doesn't know better uses.

TOM: Yeah, and everyone on a Microsoft Surface is using it, too, because they don't have any choice. That's the only thing they can use.

Steve: Right.

TOM: This story of John McAfee down in Belize, I don't know whether to be entertained, amused, horrified, sad. He's on the run. His neighbor was shot and killed. He fears that he's going to be accused of the murder. The Belize police say no, he's just a person of interest, they want to bring him in for questioning. What do you make of this?

Steve: Well, I actually encountered John before the world knew him. It's a strange story. I was writing the TechTalk column for InfoWorld magazine, and now we're talking 25 years ago. And this was a time before we knew that viruses existed. That is, there wasn't even the name had been coined, "virus." What I remember was that on CompuServe, which there was like The Source and CompuServe were the two major "use your modem to dial into a big BBS in the sky" systems. On CompuServe, which was the more sort of, much more techie of the two services, there was sort of - there were rumors of software that you might download, and it would, like, do something to your computer. Which was, at the time, science fiction. It was like, wait a minute.

TOM: How could that happen?

Steve: Yeah. I mean, it's like, huh? What? Huh? And, now, the sysops, as we called them, on CompuServe were adamant about this being untrue, that absolutely that was the most ridiculous thing they had ever heard. Now, they had a vested interest in it not being true because the last thing they wanted to imagine was that software they were encouraging people to download and that they were responsible for would hurt people. So they were just the great deniers of this. And I took some umbrage to that because I knew it was possible. I mean, I'd never seen a virus. I didn't know that they existed. But as a developer myself of assembly language code, and at the time you pretty much needed to be down at that level to do these things, I knew I could create one if I had any incentive to, if I wanted to. It's like, I mean, I knew how a virus would work, if it existed. But I didn't know that it did.

So at sort of this inflection point in the industry, I had my weekly column. I decided to write a series of three columns in InfoWorld about the anatomy of a computer virus. And I never said whether I had seen one or not. I just wrote sort of factually, this is how computer viruses work. And I did it, as the column did at the time, and very much like this podcast, with lots of detail, everything explained and filled in and fleshed out, so that a reader came away thinking, whoa, holy crap, that's scary stuff.

And after the second of the series of three columns ran, the office got a phone call from someone I had never heard of. He was asking for me. They transferred him to me. This person said - he identified himself as John McAfee. And I said, okay. And he said...

TOM: Weird to think that name wouldn't mean anything at any point in time; right?

Steve: No one had ever heard of him before. And I said, okay. And he said, "Steve, I had no idea you were down there." And I'm thinking, what? What? Who is this? And he said, "Well, we've got to compare notes. This is fantastic." And I said, "What are you talking about?" And he said, "Your columns, the last two columns you've written in InfoWorld about viruses." He said, "Based on what you've written, it's clear that you've been capturing these, too, and analyzing them." And I said, "Oh."

TOM: You're like, what, huh?

Steve: And he said, "You've got everything exactly right. So maybe we have some that you don't, and you've got some that we haven't found. So let's collaborate and share our information." And I said, "Oh. John, I've never seen a virus." And I could tell he didn't believe me. First of all, he didn't want to believe me.

TOM: Now, were you calling them "viruses" by that point? Do you recall? I'm just curious.

Steve: God, you know, that's a very good point, and I don't know whether that term had been coined. Mal- things, that all came later. Malware was meant to be more of an umbrella.

TOM: Len Adleman apparently coined the term in 1983, from what I've read. He was talking to Fred Cohen at University of Southern California.

Steve: You know, I've got the columns. I'll see if I can - that was early on, in the first five years of - and I think that they would have been in the Passion for Technology book set that I did.

TOM: I'd be interested to know that. But anyway...

Steve: Yeah, now I am, too. Anyway, so I could tell, I mean, first of all, he was just crestfallen. I mean, he really sounded disappointed. And I think he thought I wanted to keep them to myself. Like I don't think he believed that I could just make up something that was as accurate as apparently the columns were. I was delighted that I got it right because I was just writing fiction; but it was based on the engineering of software, so it was software engineering-driven fiction.

TOM: How crazy.

Steve: And so, yeah, so that was my introduction to John McAfee. And of course we all know him famously after that. Now, I do remember, and I was thinking about this and Leo because, Leo being more my contemporary, and with the memory that he has, which is amazing, there was some strange stuff about McAfee back then. And it's funny because I was talking to some friends of mine about how you cannot do research that predates the Internet because this was pre-Internet. And if anything happened after the Internet, then it would all be online. You could find it.

But anyway, McAfee was involved in some - I don't know what they were. I sort of remember maybe it having to do with HIV and AIDS and Bulletin Board Systems, BBSes, because as like I guess I was saying, that was the technology at the time. There was no global network or even local networks. It was all modems dialing in to central points. But I'll bet you that Leo would remember this. And there's no way to find out because it was pre-Internet. And it's sort of an interesting phenomenon of our life that things that predate the Internet, unless someone goes and puts literature or old copies of magazines on...

TOM: There's a lot more out there than you think. When I was researching "Chronology of Tech History," you could find stuff pre-Internet. But it's at one point more difficult, but also more reliable than what you find post-Internet. It's kind of amazing some of the things that have disappeared from the Internet post-Internet, that websites just purge and get rid of pages.

Steve: Yeah. So anyway, a listener of ours and a friend of mine, an online friend of mine who both participates in GRC's newsgroups and tweets a lot, Simon Zerafa, I've mentioned on the podcast often because he sends interesting stuff. I got a kick out of what he said. He said, and I guess he was quoting seeing it somewhere else, but he tweeted, "If McAfee is truly innocent as he claims, he now feels our pain over false positives."

TOM: Oh, yeah. You knew that had to come.

Steve: Uh, yeah.

TOM: So Cyberdog in the chatroom was making a joke about the judge giving him a 30-day trial.

Steve: Okay, yeah, I guess there's going to be lots of that. Anyway, there is a really interesting interview from this morning of John McAfee speaking to a reporter with Wired magazine, Joshua Davis. Apparently John called Joshua at 4:30 our time, 6:30 in Belize, where John is currently hiding from the Belize police. And apparently John had 11 dogs, in his backyard or at his house, and there had been a problem with his neighbor historically over the dogs barking and really upsetting his neighbor. And then I read something about five of the dogs being shot, no one knows by whom. But the presumption would be the neighbor had finally gotten fed up. And what we do know is that the neighbor of John McAfee was found dead with a 9mm Luger slug in the back top of his head.

TOM: Yeah, face down in a pool, apparently, yeah.

Steve: Yeah. So John is on the lam, as they say. And his position is that the justice system there is brutal, and he would be subjected to torture and interrogation and heinous treatment were he to allow himself to be apprehended. He's claiming his innocence. We don't know anything one way or the other, or at least I don't. If anyone's interested, it's about a 28-minute audio interview. And Joshua explains himself at the beginning. He knows John rather well. He's traveled to Belize over many months and met with John in person. And so John trusted him and contacted him to sort of give him his side of the story. And they talk about all kinds of stuff. So if anyone's curious, it's sort of interesting: wired.com/threatlevel/2012/11/john-mcafee-audio-interview.

TOM: Yeah, Wired's going to do a magazine story in the print version of Wired in January, all about John McAfee's history and how he ended up in Belize and all that sort of stuff. It'll be interesting reading. Before we get to our SpinRite testimonial, we have a PDK update. People's Democratic Republic of Korea?

Steve: Well, or Portable Dog Killer.

TOM: Oh, Portable - actually this bears on our previous story a little bit.

Steve: It strangely does, the dogs barking incessantly and driving the neighbor crazy. Behind me on a tripod is, you can see in the video, a device.

TOM: I was wondering what that was. I was thinking it was awfully boxy to be a camera.

Steve: Yeah, it's not a camera. It is a just-finished new implementation of a high-frequency canine training device, for lack of a better term. I think I called it the Portable Sound Blaster in the Google Group that I created by that name. And you can see an antenna sticking up from it because it responds to a small remote control. This one I built because my best friend's problem with his neighbor's dog has returned. When we were initially looking at the idea of bringing the doggie trainer back to life last summer, the problem got resolved. The neighbor was doing a better job of keeping control of the dog, not letting it out in the backyard, or scolding it and bringing it in if it was barking.

But I was over there a few weeks ago, helping Mark with a media center, setting up a

Windows 7 Media Center-based four-channel media recording system. And the dog was barking all afternoon. And I said, "What is this about?" And he says, "Oh, yeah, this is back. The dog is back. And they leave it in the backyard and drive off and don't know that it's barking, and it just sits there yapping all day." And I said, "Okay, well, we've got to deal with this." So I built one. I wanted to give our listeners a heads-up because there had been a great deal of interest in it before. And I'll go into greater detail once Leo is back.

But I wanted to make a mention of it and give people a heads-up. I did tweet some photos. I tweeted links to some photos of this device on my Twitter feed in the last day or two. So again, if you just go to Twitter.com/SGgrc, you can find the links. And there's also a link to an update that I posted which talks about this, why it's tripod-mounted as opposed to handheld. It's more of an installation-oriented device than a gun. Many people have since said, "Hey, Steve, I was hoping it would be smaller." I'm looking at doing a small one because I learned a lot building this thing, and I have some ideas for how one can be made very small, yet still loud enough to get the job done.

TOM: And it uses sound. If anybody's wondering, it doesn't...

Steve: Yes. Oh, and no dogs are hurt at all. It just startles them.

TOM: "Training device" is a perfect way to refer to it.

Steve: Yes. And I do have a nice story, another story of SpinRite's success with solid-state drives, which I'm pleased about. I'm really pleased that SpinRite is showing so much success repairing solid-state drives. Tim Green sent a note on November 12th with the subject of "SpinRite Heals Stupidity." And he said, "Hi, Steve and team. After several years of using SpinRite for protective maintenance without incident, it's now my turn to send in a 'SpinRite Saved the Day' story. I just bought my girlfriend a new Lenovo laptop, and yesterday I spent the morning setting it up for her. I had purchased a 256GB mSATA SSD drive so that the laptop would have both the SSD for speed plus the large spinning hard drive for lots of data storage. So I had to install the mSATA and clone the system from the hard drive to the mSATA."

And just to take a break for a moment, for anyone who doesn't know, mSATA is a cool little technology. It stands for micro or mini SATA. And it's sort of part of the PCIE spec. But it is a very small little card with an edge connector, and they come in two different sizes, sort of like a half size and a full size. And many motherboards now have one or two of these mSATA connectors on them. And so they're like over in the memory and processor area of the motherboard, sometimes even on the underside of the motherboard, where there's room underneath the standoffs against the case. I have one motherboard, in fact, that has an mSATA drive option on the underside of the motherboard, just because it was otherwise unused territory. So that's what he's talking about here. So this Lenovo laptop, in the same way that you might open up a little door to put memory in, you can open up a different little door, and there's a little connector that you can stick an SSD drive into, which is what he did.

So he said, "Unfortunately, Crucial" - which is the name of the memory supplier - "forgot to pack the teeny-tiny little screw that holds the mSATA drive in place by its top left corner. After searching through all my drawers, I found I didn't have one in the house. So I thought, eh, it's nicely seated in the slot. All I need is to tape it into place with the sticky tape from the two little antenna cables and position them so that the cover exerts a little pressure on the SSD drive to keep it in place. Not smart. In fact, very dumb. Because, as it turns out, the screw in the corner provides the ground connection for the entire SSD.

"Everything seemed fine. But the first time my girlfriend moved the laptop while it was running, everything froze. The movement had been enough, and probably the little bit of torquing of the case, to interrupt the tenuous ground connection of my jury-rigged installation. And on booting into the BIOS, the mSATA SSD drive was no longer visible at all. I realized immediately what had happened; and, if I could have, I would have kicked myself. I was afraid that the drive and everything on it might be completely hosed.

"Luckily, I'm also a Security Now! listener, every week from the very start. So I already knew that it's possible to repair SSDs with SpinRite running on Level 2. I found a screw, reseated and firmly screwed the drive into place, and managed to make it visible again in the BIOS. But indeed it was hosed. But half an hour later, SpinRite had repaired everything on Level 2, and the computer was as good as new again. So as you see, SpinRite can even heal the results of gross stupidity. Thanks for your great product and my ongoing security education. Tim Green, originally British, but located now in Kln, Germany."

TOM: All right.

Steve: And thanks for sharing.

TOM: If only it would work in every case of gross stupidity. But I guess that's asking too much.

Steve: That would be StupidNot instead of SpinRite.

TOM: Exactly. Work on that.

Steve: Okay.

TOM: Get that working. All right. I'm excited to talk about this. I've been very interested in the whole Do Not Track project since it began, and its sort of allegory to Do Not Call. And I was stunned, as a lot of us were, when Microsoft made the decision to turn it on by default.

Steve: Yes.

TOM: Because the whole deal with the advertising agency was, okay, well, as browser makers, we'll put it in, but we'll require a user to turn it on so that your advertisements can still be set for most people.

Steve: As is the case with every other browser currently. Every browser has it now, at varying levels of visibility.

TOM: Which I was surprised that that even happened, alone.

Steve: Yes.

TOM: But so what is Microsoft's reasoning here? How did this policy come about?

Steve: Okay. So what I want to do, this won't take much time, and feel free to interject or interrupt any time, Tom, if something - if this triggers a thought. You can stand in as a proxy for our listening audience.

TOM: Okay, I'll try, yeah.

Steve: They're unable to interrupt. I want to share a relatively short, about 10-minute keynote address which was given by the guy who understands exactly where Microsoft stands, who is Brad Smith, the general counsel for Microsoft and their executive VP. He gave the keynote presentation at the 34th International Conference of Data Protection and Privacy Commissioners, which was recently, on October 23rd, just a few weeks ago, held in Uruguay.

So he says, "Thank you so much for the opportunity to be here this morning. I've made many trips to Latin America before, but I suspect like most of you I've never had the opportunity to experience a cyclone firsthand." To which he got some laughter. I guess they had some weather down there, a little bit later than we got Sandy here in the U.S. He says, "I suspect that a year from now you may not remember a word that I utter this morning, but I guarantee you that every one of us in this room will remember the weather when we got up. It's been that kind of day.

"We come together to talk about an important topic, privacy. But despite the evident importance to all of us, I think it makes sense to start by asking a question: Does privacy still matter? It seems obvious to us that it matters. After all, we came all the way to Uruguay to have this conversation about privacy. Clearly it must matter.

"But as you may know, I work in an industry where one frequently encounters people who actually want to debate whether it matters. They want to talk about how it matters, they want to talk about why it matters, and they want to talk about whether the way it matters has, in fact, changed over time. They point out, for example, that if you look at big data, privacy must not matter as much as it used to." And by that, well, he uses the term "big data" several times in this keynote. So he's referring to huge archives of data collected by organizations about their customers or clients or Internet users.

He says, "So they point out, for example, that if you look at big data, privacy must not matter as much as it used to. After all, look at all the information that people are sharing. Look at all the good ways in which it's being used. Or sometimes I meet people who say, look, privacy must not matter, at least not the way it used to. After all, look at Facebook. There are a billion people in the world who are sharing all kinds of personal information about themselves. How can Facebook be such a success if privacy still matters?

"Well, the first thing I have to say is this: Let's look at Facebook, and let's look at the Facebook story. I'm not here to be an expert on Facebook's privacy policies, but I can speak as someone who was involved in the decision at Microsoft exactly five years ago today to invest a quarter of a billion dollars in Facebook." Microsoft invested $240 million in Facebook.

"Now, at the time, it was not necessarily obvious that Facebook would ever have a billion users. At the time, Facebook was not even the most popular social network on the planet. It wasn't the first. The first was probably a service called Friendster. It wasn't the second. The second was a social network that became very popular called MySpace. In fact, five years ago, MySpace had 100 million users; Facebook had only 24 million. In our industry it is very unusual for one company to be the first to reach 100 million users and to have four times the market share of its next closest competitor, and then not go on to be the prevalent and most popular service by far."

So of course he's noting there that, for whatever reason, MySpace has gone into decline, whereas Facebook of course now has many, many times the number of users it had at the time. And he has a slide in his presentation that shows sort of an exponential growth curve in green for Facebook and a flatline dropping..."

TOM: Sagging flatline, yeah.

Steve: Sagging, yes. And he says, "But of course the real question here is, what happened? What happened over the last five years? Well, at a certain level I think we all know what happened. MySpace didn't do so well. It has fewer users today than it had five years ago. Facebook has exploded. In five years it has gone from 24 million users to a billion. We've done pretty well with our $240 million investment," he says.

"But I think the most important question for us is not what happened, but why. Why did these two curves take off the way they did in such different trajectories? There are a number of different reasons, but there is one that personally I think probably matters the most. It's certainly one that we thought about when we put $240 million into the company. It's a facet that was captured very well by one of the leading books about what happened, David Kirkpatrick's book, when he addressed why this happened." And Kirkpatrick's book is titled "The Facebook Effect."

Anyway, he says, "And what he said was on MySpace, for people who remember it from five years ago, the default setting was that you could see anybody's MySpace profile. Or, to put it another way, the default setting was anybody could see your profile, as well. But on TheFacebook, and initially it was called TheFacebook, the default setting allowed you only to see profiles of others at your own school or those that had explicitly accepted you as a friend. A degree of privacy was built in at Facebook by default in a way that was simply not the case at MySpace."

TOM: Really interesting to hear Facebook lauded for their privacy in this instance.

Steve: Well, now, okay. I mean, let me just pause for a minute here because I reacted, when I read this the first time, thinking, wait a minute, okay, eh, I guess I can see that. But I know why I was forced to create a Facebook account, and that it's that no one without a Facebook account could see anything inside. It was the classic "walled garden," as it's called, where you had to have an account in order to participate at all. You couldn't be a voyeur without one. And so I would argue that a substantial amount of Facebook's growth was built by the pressure of its early success and then sort of the desire to see what was going on, but you had to join in order to see anything at all.

TOM: So is that where he's going with this, is to say that's behind the justification for Microsoft's default privacy?

Steve: Well, sort of. He says, "So in effect, at MySpace you could change the settings, but by default you shared your information with the world. And at Facebook by default you shared information only with people in your network and the people that you decided to make your friend."

Now, I can see - this is me speaking, again. I can see the power of that, the notion that somebody who is posting personal stuff absolutely wants control. And I coined the term that I've used many times in the last eight years. I call it "the tyranny of the default," which is my way of stating the observation that, whatever the default settings are, most of the time that's what they end up being forever. The tyranny of the default. I have a page on GRC, if you go to GRC.com/cookies/cookies.htm, my site has been for years looking at the cookie-handling habits of everybody who visits. So as a consequence of that, I've been able to develop some statistics. And relative to the issue of third-party cookies that has been known far longer than this issue of the Do Not Track header, you can see there that I look at the number of users.

For example, right now, 85.6 percent of the 57,529 unique visitors to GRC just last week - that's not a running average, that's the total. I update it every Sunday night so that I'm always seeing with no older history a snapshot of what is current. So 85.6 percent of the many users who visited GRC last week had third-party cookies enabled. But if you scroll down to the bottom, I show Apple's Safari visitors separately, and only 30 percent of them have third-party cookies enabled. Why? Because Safari is unique in the industry of having third-party cookies turned off by default. And so this is a perfect example of the fact that the default matters. The default is what people end up leaving their system set to.

Anyway, continuing, he says, "It's not just the votes of consumers in their adoption of Facebook that tells us, in my opinion, that privacy matters to people; that privacy matters to consumers. Consider this: Recently the Pew Research firm did some research in the United States, and what they found was that 56 percent of consumers had decided not to complete an online purchase because of concerns about sharing personal information with the seller that they were going to do business with. They also found that 30 percent of consumers had uninstalled an app from their smartphone because of concerns about the way that app dealt with their personal information. If you put these things together, I think they tell an important story. They tell us that people care about privacy.

"But that's not the whole story, because I think they also tell us that people are thinking about privacy in new ways. And if we're going to do our jobs well, whether we come to this meeting from industry or from an NGO or, most importantly, from a government and as a regulator, we need to really think about the new ways that people are thinking about privacy."

He says, "To start with, I would say in many ways this is not a new phenomenon." It's funny, in his slide presentation he shows an old-style bellows camera.

TOM: Yeah, looks like a tintype-taking kind of machine.

Steve: Exactly. And he says, "The history of technology is a history of societal change. Typically, one sees a pattern. The pattern starts with the invention and then the increasing adoption of new technology. That is then followed by a second step in the process. That second step involves new consumer needs and new consumer views about what to do with respect to the technology. And then, finally, there's a third step. The third step is about what all of this means for laws and for regulation and public policy. And indeed, the story is well documented.

"The truth is, as many of you are aware I appreciate, the whole global discussion about privacy really began with this invention on the screen, the camera, in the 1800s. And interestingly, as the camera became more popular, as it was found throughout society, we saw this pattern take place. By 1890 there was a famous law review article in the Harvard Law Review written by Professor Louis Brandeis, who would go on eventually to become a justice on the U.S. Supreme Court. And it was in this article that Professor Brandeis coined the famous phrase, 'the right to be let alone,' a phrase that many people who work in the privacy field every day are familiar with. But interestingly, that phrase is at the end of a sentence that starts by talking about technology.

"What Professor Brandeis recognized was that the camera had changed society. And because the camera had changed society, people could no longer walk out of their front door without the risk of being photographed. And, of course, this was before there were lenses that could see someone a kilometer away. And he recognized that, because of this invention, there was a new legal right that needed to emerge to protect people the way they had always been protected in the past before this technology had entered the scene.

"And we see, 122 years later, the leaders of our day in the United States and around the world grappling with similar phenomena. It was in the State of the Union address this year and in other reports at the start of the year that President Obama started to address these issues. I think he captured part of this issue for us very clearly, because what he said is that we live in an era where people are sharing more information, but that does not mean that privacy is an outmoded value.

"What we really need to focus on, in my opinion, is how to reconcile these two aspects. And indeed, we meet in the year 2012, when people around the world are doing just that. Personally," he says, "I think that perhaps the single most important statement in the United States this year came in a case from one of our current Supreme Court justices, Sonia Sotomayor. The case involved Jones v. the United States and the question of whether the police needed a warrant to put a GPS tracker on a car.

"As many of you may know, there is a constitutional right to privacy under the Fourth Amendment to the U.S. Constitution, and that protection always turns on whether people have a reasonable expectation of privacy in a particular situation." So that's this notion of a reasonable expectation of privacy. "But Sonia Sotomayor, Justice Sotomayor, had something very interesting to say. She said that, for over a century, people in the United States had always looked at the Constitution and, in fact, said that there was a reasonable expectation of privacy only if there was a reasonable expectation that people could keep certain information secret.

"And, in fact, I think, if you read much of what had been written about privacy over the last 50 years, in many, many instances, perhaps most, if you substitute the word 'secrecy' for the word 'privacy,' the meaning of a sentence or the meaning of a paragraph is unchanged." This is the sort of test attorneys use and learn. "When people were talking about whether they could keep something private, they were, in fact, talking about whether they could keep something secret. Certainly in the United States that has been at the core of our legal evolution. But I think the question that Justice Sonya Sotomayor posed, while focused on the Constitution, was in fact far broader than that: Is secrecy still a prerequisite for privacy?

"I think if you look at the world today, if you look at the story of Facebook, if you look at the story of people using the Internet, one thing is clear: People are less focused on secrecy. Consumers want to share more personal information than ever before. They don't care as much about keeping things secret. But that doesn't mean they don't care about keeping things private because there's a big 'but' involved. The fact is people want to decide who they share information with. People of all generations want to make that decision themselves. And not only that, they also want to determine how their information will be used by the people with whom they choose to share it. That's the new model of privacy, not a model focused on secrecy, but a model focused on what people are saying: They, in fact, want and need the ability to decide who they share information with and how that information will be used."

TOM: In other words, it's not a secret because I might tell a lot of people. It's not just in my house. But I want the right to keep it private so that I decide who I share that secret with. It's not a secret.

Steve: Yes. Yes. You want control.

TOM: It's not binary.

Steve: Yes. Exactly. You want management. It's very much like what websites do I trust to run scripting, to run JavaScript. I want to say, by default, sites cannot run scripting. If I decide that I want to share that privilege of a site giving me script, meaning that I trust what it's going to do with that power, then I make that decision. I want control. And managing cookies is the same way.

So he says, "When you step back and think about this, I believe these are reasonable needs. They are laudable goals." And it's important to understand, I mean, this is a - you can tell by the way he's pitched this, these are global leaders in policy, setting privacy policy at the nation-state level. I mean, this is the audience to whom he's bringing this. And he specifically discusses DNT in a second, as we'll see.

So he says, "From every vantage point, our preeminent obligation should be to help people meet these needs in a world of new technology. Now, life would be simple if that were the only goal we had to meet. But as we know, it's not very simple at all. The reality is we need a balanced approach to address privacy. We need a balanced approach because more is at stake than solely the protection of privacy, as important as that goal and need, in fact, is. There are other goals that need to be addressed and balanced with it.

"For one, it is important to ensure that innovation flourishes. It's important to ensure that innovation flourishes because innovation does so much in the technology space to help people around the world. Certainly in the technology sector this is something we see every day. It's why many of us have chosen to spend our careers in technology. We see it today in the benefits of big data. We see it in ways that are profound. We see it in stories that people in the technology field bring to life every day.

"One recent example, in fact, involves the use of search terms in Bing. It turns out that when the Food & Drug Administration in the United States, like most authorities around the world, approves a drug, it focuses on that one drug in isolation. But it also turns out that millions of people every day, in every country, in fact use more than one prescription drug during the course of 24 hours. No drug authority can possibly test the combination of every drug with every other."

TOM: Too many combinations.

Steve: Oh, my god. "But last year, a researcher at Stanford started looking at the potential side effects of what might happen if people took two drugs together. One was a drug that is an antidepressant. It is an antidepressant that is taken by millions of people in North America and tens of millions of people around the world. The second was a drug that reduces cholesterol levels. In fact, these are two of the most common drugs that doctors prescribe. But this researcher began to become concerned about the possible side effects of what might happen if people took both of these drugs together, side effects that no one had ever diagnosed.

"He began to review certain data that was in the possession of the Food & Drug Administration in the United States, and then asked us at Microsoft if we could share with them, in a de-identified manner, certain search terms that had been entered in Bing. And specifically what they wanted to search for is search terms where people were entering in the name of one or both of these drugs and some of the symptoms associated with diabetes, such as fatigue and headaches. And what they found is that, when people searched for only one of these two drugs, it was unusual for them to include in their search request one of those other symptom words. But when they entered a search request that had both drugs named together, a full 25 percent of the time they were also looking for information about how to deal with a headache or how to address fatigue or other symptoms associated with diabetes.

"And this helped the Stanford researchers along the path to a conclusion that, if you take these two drugs together, you do face a potential side effect of diabetes. There are a million Americans in our country alone that happen to take both of these drugs; and for them, this kind of insight, when shared with doctors and applied with their patients, is something that can save lives. In fact, it's something that can save many lives. And it's made possible in part because of the insights that come from our use of big data and information.

"It's not just innovation and big data, though, that's at stake. There are other things as well. We find every day the use of information is of fundamental importance in our ability to make technology stronger." And this is taking longer than I expected, so I'm going to skip down to where he...

TOM: Yeah, let's get to the DNT part.

Steve: Exactly, where he begins to look at this. Okay. So he says - let me back up a little bit to get some context. Okay. He says, "Even though I represent a technology company, I believe in the importance of privacy regulation. I believe we need clear and fair rules of the road. We need rules of the road that increasingly apply consistently in country after country and continent after continent. We need clarity so that everybody knows what they need to do, and companies that act responsibly are not going to find themselves suffering at the hands of companies who do not, and regulation creates that floor that provides that level playing field. But we don't need regulation alone. We also need self-regulation." And I'll talk about this after we're done because there is some - the FTC has, as I have been predicting, begun rattling their saber a little bit about this.

So he says, "We need self-regulation, especially in the form of industry standards. We need self-regulation that can move technology forward, and we need self-regulation that can move faster and more globally than regulation alone is able to. But even these two things together, in my opinion, are not sufficient. At a time when everyone is talking about standards, it is important, I believe, to remember that we need market-based innovation, as well. With market-based innovation, there's an opportunity for companies to experiment, to try new things, to see what consumers want. And if consumers do in fact want what companies are offering, there's an opportunity for those companies to grow. Market-based innovation is every bit as important, in my opinion, as these two other ingredients, as well.

"All of this makes for a sometimes complicated conversation. And it certainly, in my role at Microsoft, is one of the things that I've come to conclude that we need to come together on. We need to come together to work through the complicated conversations we must have. And there's probably no topic" - now, remember who this guy is. I mean, this is god of, you know, he's the executive VP and general counsel. "There's probably no topic that I've been involved in that has involved more complicated conversations over the last couple of years than three little letters that I've come to know by heart: DNT. And so I'd like to conclude by offering a few thoughts on DNT, or Do Not Track.

"As a company, we have taken a stand, if you will, when we decided earlier this year to turn on the Do Not Track signal in the new version of our browser and the new version of our operating system that starts to ship this Friday. We've had to think a lot about DNT. Whenever you have to think a lot about a topic, I think it helps first to define the questions. And if you're in a business, there is always one question that you had better think about very long and hard. It's this: What do our customers want?

"Well, as a company we, of course, have many customers. There are times when PC manufacturers are our customers. There are times when advertisers are our customers. And we value those relationships with these companies as our customers."

TOM: I think a lot of people in our audience forget that the end user isn't always considered the customer. That's a good point.

Steve: Right. He says, "But at the end of the day, one thing remains very clear: Our customers, more than any other group, are the one billion consumers around the world who pay us money to provide them with cutting-edge technology." That $29 or $39 I was hit up for when I was looking for IE10, and it wanted to give me instead Windows 8, for example.

TOM: Windows 8 upgrade, right.

Steve: He says, "What we need to focus on is this: What do consumers want around the world? So after the DNT issue became a little more dramatic earlier this year, we thought it made sense to go back and see if we could learn a bit more about what customers want. We commissioned some research, and we asked people what they thought about these issues. And what we found in four countries where the research was conducted - the United States, the U.K., France, and Germany - is that most people today believe that online tracking goes too far, and they want an easier way to block it. In fact, in all four of these countries, roughly 80 percent of consumers came down strongly on the side of wanting new steps to block the tracking of their personal information.

"We also talked to people about DNT itself, and we asked them the question that we were asking ourselves: Should this feature be enabled or not when they get a new browser or operating system? And what we found in all four of these countries was that 75 percent or more of the public, in fact, want this feature to be turned on. They want their privacy to be protected. They want it enabled. They want it on by default. The votes are in because these are the people whose needs we have to serve.

"Now of course, again, we recognize that this cannot be only about one thing. We need to balance the protection of privacy with the other interests that I spoke about before. And so we've tried to give a lot of thought about where we go, and we've decided on two things. First, we want to innovate. We want to innovate and deliver new privacy benefits to consumers. We want to build on regulation and self-regulation, and we want to use our research and engineering capacity to build better privacy protection into our products. That's why we believe we made the right decision when we made the decision to enable the DNT signal in the new versions of our products.

"But we also recognize that we need to do more than that. If we're going to move DNT forward, let's face it: We all have a pretty steep ladder to climb. And that's going to take, in our view, four things, not one, to get where we all want to go. First, we need a final and effective DNT standard that is adopted by the W3C." And I'll just mention we don't have that. That is, the DNT standard has not been agreed upon yet. So it doesn't exist. And in fact, at the beginning of this year the working standard did not specify whether a user agent, a browser or operating system, should or should not have DNT enabled by default. That was added, I think it was in April. It was later in the year. So that's a data point. But even so, this hasn't been ratified yet.

Continuing, he says, "We need a standard that provides real privacy protection to consumers, and we need a standard that recognizes the legitimate and reasonable needs of all participants in the ecosystem. Second, we believe that the world of privacy will be a better place if we all recognize that browser vendors should have the ability to turn the DNT signal on or off when they ship a product." Okay. So here he's arguing against the notion that this standard should specify that DNT should either be on or off. He's suggesting this ought to be something that can be used for market differentiation.

TOM: And the advertisers have argued the opposite. They said no, the only way we'll agree to abide by this and play by these rules is if it's off by default.

Steve: Well, and that's the - yes, exactly. And that's the wink-wink is because they know of the tyranny of the default; they know, I mean, you can't find it in Chrome. I mean, it is buried. It's hidden under Advanced Settings and Settings and, I mean, you know, and it's off by default. So, yes, you're exactly right, Tom.

So he says, "If you look at standards around the world, they specify the technology, but they don't tell companies whether they have to turn it on or keep it off. That's a decision that is left to companies in the marketplace based on their assessment of the needs of their customers. And we believe that the right approach is an approach that allows vendors like Microsoft and everyone else to make this decision for themselves. But even that's not the end of the story.

"Third, we believe that browser vendors should clearly communicate to consumers whether the DNT signal is turned on or off and make it easy for them to change the setting. We recognize that you cannot have privacy without transparency, and we recognize that we have an obligation to ensure that it is clear to consumers how our product is configured." And I'll just say that nobody does that yet. "And there is room for an ongoing conversation across the industry and more broadly about the best ways for vendors to communicate this information to consumers and the best ways to enable them to change this setting as they use the product themselves.

"And there's a fourth and final piece as well, a piece that has gotten too little attention, in our view. There needs to be an easy and effective way for responsible advertisers and advertising networks to inform consumers to obtain persistent consent for their services, even if the DNT signal is turned on. Just because the signal is turned on does not mean that a consumer wants no services that involve tracking. What it means is that consumers need to be empowered to make their own choices, and advertisers and ad networks need to be able to inform consumers in a well-understood and broadly established manner so that those ad networks that are acting responsibly can inform people and get a user's consent, even while a consumer might choose to withhold that consent from another service."

TOM: Like NoScript; right? I don't want to run NoScript and say no script can ever run ever, and that's my only choice. I want to be able to say, okay, I want to make an exception in that case since I trust that site.

Steve: Right. And one can imagine that a site - say that you had DNT turned on. You might go to a site that receives the DNT signal, but they generate revenue by encouraging or at least allowing tracking. So they might say, hey, sorry for the inconvenience, but you've got DNT turned on. We need you to disable it in order to use the site because we'll generate revenue from the ads, and the advertisers have said we need to track you.

TOM: And that's perfectly legitimate, and you as a consumer get to choose whether that's worth the transaction or not.

Steve: Exactly. Exactly. And it creates a lot of transparency, and that's what he's been talking about. When we've talked about things like Ghostery that, like, shows you this list of all the tracking that's going on on a site. It's like, whoa. I mean, that was a real eye-opener for many people.

So he concludes, saying, "But fundamentally, what the DNT signal does is empower people. It empowers people so that they're able to make that decision themselves. When you put all of this together, whether you're talking about DNT in the narrow sense or privacy more broadly, we're reaching an important moment. We're reaching the kind of time when we can look back and say, yes, technology has changed. It's continuing to change as we meet today. But because technology has changed, we can now say the needs of consumers have changed, as well. The views of consumers have changed, as well. The views of voters and the public at large have changed, as well.

"We need to come together. We need to grapple with those changes. We need to ensure that innovation flourishes, that the ecosystem is healthy, that technology protection is addressed. But more than anything else, we need to address the privacy needs of people around the world. We need to address the privacy needs of people and move privacy forward. That is the opportunity we have in the years ahead." And he says, "Thank you very much."

TOM: Now, I hate to say it, Steve, but we're almost out of time here. So how best should we wrap this up? I know we've covered a lot of the points as we've gone along here.

Steve: Yes, we have. I wanted to mention that the European Commission, the EU, sent a letter from their location in Brussels to the World Wide Web Consortium, that's the W3C, Tracking Protection Working Group. That's the DNT group. And it's a short letter. I highlighted two paragraphs that I wanted to share. And that is, they say, "It is not the Commission's understanding that user agents' factory or default setting necessarily determine or distort owner choice. The specification need not therefore seek to determine the factory setting and should not do so because to intervene on this point could distort the market. Crucially, and as a different matter, the standard should foresee that, at the install or first use of the browser, the owner should be informed of the importance of their DNT choice, told of the default setting, and prompted or allowed to change that setting."

So this is, I mean, the EU matters on the global scene. And their formal position is, essentially, what IE10 represents. When I installed IE10, the very first item in the upper left said "New privacy setting" in blue. And it said, "Websites you visit receive a Do Not Track request when you use Internet Explorer 10. To learn more about this setting, including how to turn it off, see more info about Do Not Track," which you can click, and it takes you to more information. And the location of that setting is where they have that grab bag. I'm sure IE users or ex-users will remember on the Standard Internet Settings dialog, that the last tab is Advanced. And it's this huge potpourri grab bag of checkboxes, a list that scrolls. And down under Security it says simply, "Always send Do Not Track header," and it is checked by default, unless you choose to turn it off.

TOM: Isn't the solution to this to say, with any browser, the first time you run it or install it, it just asks you do you want to have it on or off? In other words, forced opt. You're not opted in; you're not opted out. It just lets you set it from the beginning.

Steve: I think that's perfect. I think that's perfect. And the problem is the advertisers know that people, I mean, if we take Microsoft survey stats at face value, 80 percent of people will say, "No, I don't want to be tracked. Thank you for asking. No." And that upsets the advertisers.

Now, the FTC, the Federal Trade Commission in the U.S., the chairman, Jon Leibowitz, is on record saying, "If by the end of the year" - that is, this year, 2012, and we're approaching that. "If by the end of the year or early next year we have not seen a real Do Not Track option for consumers, I suspect the commission" - meaning the FTC - "will go back and think about whether we want to endorse legislation."

Leibowitz also attacked as delusional the owners of third-party advertising networks who claim that opt-out functionality could damage their businesses, as well as thousands of small businesses who rely on targeted web ads, noting that the same companies continue to operate in Europe, where data collection rules are much stricter. He says, quote, "The notion that they can say, 'The sky is going to fall if you allow a modest opt-out' is just not credible." So that's where we are.

TOM: All right.

Steve: Yeah. So IE10 has happened, and it looks like Microsoft is planting a stake in the ground. I bet you that Yahoo! and Apache are going to lose this one.

TOM: Yeah. It looks like Microsoft's trying to force the debate into an entirely new direction by taking this unpopular stand with the advertisers, saying, look, we don't want this either. We actually don't want Do Not Track on by default. We want an entirely different way of doing things.

Steve: Well, and Microsoft also, I mean, this is a bet. They're waging a bet here because they also, what we heard sort of reading between the lines is they see it as a market advantage for their browser over those other browsers that do have DNT off by default. They believe that their promotion of the fact that Do Not Track is on will, over time, give IE the reputation that you are less tracked if you use IE than if you use any other browser, which will be true to the degree that the Do Not Track header is honored by advertisers who track.

TOM: Well, I'm sorry we don't have more time to talk about this. But I'm glad I'll have more time to talk with you next week, Steve.

Steve: We'll do it. And I imagine that we'll have lots of feedback on the topic. Love to hear from our listeners on this topic. Just go to GRC.com/feedback between now and next week. I'll go through the mailbag and pull a bunch of stuff, interesting, I'm sure, about this topic and no doubt others.

TOM: I know there are folks in the chatroom wanting to hear more about Apache. So great place to ask your questions about that.

Steve: Ah, good, yes, because I do have information about where that stands. And I got a kick out of remembering that the way that web server was named was that it had become so full of patches. It was "a patchy" web server.

TOM: That's funny. I didn't realize. I don't think I ever knew that. That's really great.

Steve: Yup.

TOM: All right. That's it for this episode of Security Now!. Don't forget to visit GRC.com to find out all of the great stuff that Steve's always working on, including SpinRite, including ShieldsUP!, and tons of other projects going on over there. And you can find our episodes at TWiT.tv/sn and live on Wednesdays at 11:00 a.m. Pacific time, right after Tech News Today. Thanks again, Steve.

Steve: Thanks very much, Tom. Talk to you next week.

TOM: Bye now.