Steptoe

Episode 234: The California Turing Test

Stewart Baker: [00:00:05] Welcome to Episode 234 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking about technology, security, privacy, and government. I'm your host, Stewart Baker, and we're joined today by Gus Hurwitz, who teaches law at the University of Nebraska, and Dr. Megan Reiss, who has three titles. I skipped over Gus's multiple titles, but Megan is the Senior National Security Fellow at the R Street Institute, a Senior Editor of Lawfare, and not-yet-senior-but-no-longer-a-visiting Fellow at the National Security Institute.

Megan Reiss: [00:00:47] Yes.

Stewart Baker: [00:00:48] Congratulations. I hope some of those jobs pay.

Megan Reiss: [00:00:51] Only one.

Stewart Baker: [00:00:52] [Laughter] Yeah, that sounds right. I was a Distinguished Fellow at CSIS, and I think the "Distinguished" meant that I wasn't supposed to get paid.

Megan Reiss: [00:01:03] Excellent. Excellent.

Stewart Baker: [00:01:04] Alright. We've got an enormous number of stories. Let's jump right in. The story of the week kind of slightly coming undone by today was the claim in *Bloomberg* that Supermicro, which is a Chinese motherboard supplier, had put a tiny piece of hardware on their motherboards that would have enabled an attack on any computer that had this on it. Megan, is this true?

Megan Reiss: [00:01:40] I don't know, and I don't think anyone knows at the moment. So Amazon and Apple and even DHS now have come out and said this is unequivocally

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

not true. That being said, there's some room to say they actually have reason to deny these claims.

Stewart Baker: [00:02:01] Right.

Megan Reiss: [00:02:02] So it's a little bit of a he-said-she-said.

Stewart Baker: [00:02:09] But less entertaining. [Laughter]

Megan Reiss: [00:02:11] But less entertaining. So the original story – of course *Bloomberg* is a well-respected outlet, so you give them at least some benefit that there was fact-checking that went behind it. There are 17 sources.

Stewart Baker: [00:02:23] That's what they say.

Megan Reiss: [00:02:24] Seventeen sources is a lot of sources.

Stewart Baker: [00:02:27] Although one of the sources went on Patrick Gray's podcast and said, "Well, if I was a source for this, I'm not completely comfortable with how they used what they heard from me."

Megan Reiss: [00:02:37] Being described as a source. Yes. And so questions are coming out. Did this discussion... was it all confirmation bias? They wanted there to be a story, so when they talked to the sources, they confirmed everything that they were asking. They didn't ask Apple explicit enough questions for them to confirm or deny.

Stewart Baker: [00:03:00] Although it looks like Apple denied, denied, denied.

Megan Reiss: [00:03:02] Denies unequivocally now. But going back to some other stories, you know when the Snowden stuff happened, there was some denial that they were able to deny explicit...

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:03:13] Deny without denying.

Megan Reiss: [00:03:16] Deny without denying.

Stewart Baker: [00:03:16] Yeah. So there could be something. Right. Everybody in this story has a reason to obfuscate, even *Bloomberg*.

Megan Reiss: [00:03:27] Yeah.

Stewart Baker: [00:03:27] Once they publish, they are stuck with this story.

Megan Reiss: [00:03:30] Yup.

Stewart Baker: [00:03:30] They're not interested in taking it back. So Nick Weaver, who is often on here – I'm sorry he's not on today – has said you know this is doable for sure. And it is the wave of the future, and we're going to see these attacks whether or not this was a hardware attack that uses China's massive supply chain advantages to achieve cyberespionage capabilities. So whether this is true or not, it's going to be true.

Megan Reiss: [00:04:06] It's still a big deal. You want the FBI on the record because that's the agency that supposedly did this investigation. And you also want more generally people to know whether or not this is possible, whether or not it will be done in the future. And in light of Mike Pence's major speech on China last week, you have to think about this in terms of what is China doing or wanting to do and would they be able to do something like this in the future.

Stewart Baker: [00:04:36] So we'll just have to sit and wait to see what emerges as these stories get checked and various people come out of the woodwork. The good news we've discovered about he-said-she-said debates is sooner or later other people come out of the woodwork to shed light on the he-said-she-said debate. Okay. The FAA. You know Congress wasn't just watching the Kavanaugh hearings. They actually have been doing stuff. The FAA bill has this massive new bill authorizing the FAA, and

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

it's gotten now through conference. I didn't think they had conferences anymore, but it's gotten through conference, including with a provision that DHS had asked for which allows them to go after drones as a threat. Gus, how big a deal is this?

Gus Hurwitz: [00:05:35] So I think this is as little a deal as almost anything or maybe everything that we're talking about this week, which is to say the press coverage has been pretty terrible and has made this sound much bigger, much worse than it is. So the actual legislation, the actual text of the statute – which none of the articles I've seen actually links to, you need to go through and do your own research to actually find the act that's been put into the FAA Reauthorization Act – it does allow DHS to take action against drones under certain circumstances and for specific purposes. So the way that the press has been covering this is DHS is going to be able to shoot down drones left and right if they determine there's a credible threat.

Stewart Baker: [00:06:24] Right.

Gus Hurwitz: [00:06:25] That sounds scary.

Stewart Baker: [00:06:26] Yep.

Stewart Baker: [00:06:27] But the statute says credible threat needs to be defined by the attorney general and secretary of transportation beforehand. It has criteria in the statute for what factors go into that definition. And it only applies to drones that are threatening the security of what's called a "covered facility or asset" in the statute. And again there are definitions in the statute that limit the scope of what can be protected. So this is not, as the press has been covering it, a bill that says, "Hey, DHS can shoot down drones because they want to." It's DHS can – they actually talk about there's need to be a risk-based assessment and a definition of what is a credible threat. So it's much more narrowly tailored, as you usually find, as you often find at least with legislation. It's a much more narrowly tailored authorization than the press has been discussing it.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:07:24] So this is just the journalist, Lefty technology group complex at work.

Gus Hurwitz: [00:07:32] Now, there's no need to be partisan here, Stewart. The Right also gets its press coverage very bad pretty often.

Stewart Baker: [00:07:38] [Laughter] You're right. Yeah, you're right. When I'm being careful I call it the Left-Lib Axis because that's what it is. And those of us on the Right have our libertarian cross to bear as well. But not surprisingly everybody is shouting, "There should have been warrants," as though you know you see a drone hovering over an airstrip and you're supposed to call up a judge and ask for the warrant. It was a bizarre set of objections. Alright. Sticking with the judiciary. ZTE has now, it looks like, a second or a monitor imposed – really they'd already been imposed, but it was extended by a US federal judge because ZTE was on probation for having violated US law and while on probation, Megan, had actually violated the terms of the probation agreement and got it extended.

Megan Reiss: [00:08:50] Yes. So if you remember back, this was a big story in the spring. ZTE had shipped American supplies to Iran, which obviously is under a whole bunch of US sanctions preventing them from receiving telecommunications and other technology. And instead, when this was found out, they agreed to a bunch of things, including having these 35 people who decided to do the scheme within ZTE. So instead of being fired or disciplined, they got bonuses. So ZTE was under ban for a while in the US. That was lifted in July. But going back to these 35 people that had violated the terms of this agreement, this judge in Dallas actually came out and said, "You know, we're actually going to extend the initial monitoring that had been put in place to go through 2022 for an additional two years." So it's not a huge addition to what they've already had to do, which is an additional $1 billion fine. But it does indicate that we're going to keep monitoring them and making sure that they don't do something like this again.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:10:02] So they've got two American monitors in this Chinese company.

Megan Reiss: [00:10:07] Yes.

Stewart Baker: [00:10:07] It cannot be a comfortable thing –

Megan Reiss: [00:10:09] No.

Stewart Baker: [00:10:09] – as they try to come back from basically having shut down for several months.

Megan Reiss: [00:10:13] Yes.

Stewart Baker: [00:10:14] Yeah. Okay. I find it hard to believe, but the Trump Administration is following in the Obama Administration's footsteps after a fashion, going back to the UN, reopening talks about what the norms for cyber conflict ought to be. Gus, is this really just the same old wine in new bottles, or are they taking a different approach?

Gus Hurwitz: [00:10:43] They're taking a curious approach. So they've gone back and reengaged with the Group of Governmental Experts, minus two. So in the new round of discussions that they're trying to start, it's basically the same old, same old group of folks, except oddly Russia and China aren't included. So I don't really know what the purpose of these discussions is going to be other than to get the like-minded, like-ish-minded nations of the world to come together and say, "Here are our norms that we generally already hold. And we're just going to tell Russia and China what we already believe." I'm not fully sure that we can or should expect anything novel or interesting to come from this. Though, I will add a news item on the fly to the Roundup for today, which is yesterday's report that the UK apparently has been wargaming attacks to launch against Moscow to turn its lights off. So perhaps this could be a turn towards less focus on US active operations in cyberspace and more towards let's work with our

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

partners to internationalize these operations so that if anyone does anything that violates these norms, we can all say, "Hey, we decided to do this together."

Stewart Baker: [00:12:04] Yeah. So if I were selling this in the Trump Administration to John Bolton, I would say this is just like the Proliferation Security Initiative, where we got together the people who are like minded. We set up some rules and we gradually expanded to others until the outliers felt enormous pressure to get with the program. So maybe that's the plan. God bless GCHQ. You know it is true that the Russians have been particularly contemptuous of UK national security, using chemical weapons on their territory. And so doing something probably is more appealing to the UK even than to the US. It may be that you'll have to turn the lights out in Moscow for Putin to start to get the feeling that maybe he's let GRU go too far. Let me ask, speaking of going too far, California –

Gus Hurwitz: [00:13:09] Yes, they've gone too far.

Stewart Baker: [00:13:10] Exactly. [Laughter] So they have a couple of new laws. They've got this net neutrality law, and I'm hoping you can unpack it or at least summarize it and then give us your sense because it's now being challenged in litigation brought by the federal government as well as a bunch of carriers. Is there really any prospect that a state net neutrality law can survive that onslaught?

Gus Hurwitz: [00:13:39] So it all really depends on what happens to the appeal, the challenge to the FCC's reclassification in the Restoring Internet Freedom Order that went into effect earlier this year. So the California legislation was adopted in response to the FCC saying, "Hey, everything that we said under the Obama Administration we were going to do about net neutrality, we're not going to do that. It's our policy and the policy of the federal government and the policy for how the federal government is going to regulate this nationwide network – so listen in, states, this applies to you – to take the hands-off deregulatory approach. And we think that this preempts any state regulation." In the Restoring Internet Freedom Order it expressly says this preempts state regulation. California is one of several states that have been working to and that now

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

have enacted some form of net neutrality legislation or regulation. California's goes further than anyone else's. In fact, it goes further than the 2015 FCC order prohibiting ISPs from doing things that the FCC in 2015 had only said, "We're going to take a look at this stuff if you do it. It may or may not be problematic." So California went and said, "Okay, we're putting this back in place." And the big surprise here was that the Department of Justice [DOJ], within hours of the bill being enacted – it doesn't go into force until January 1st – but once it was passed, DOJ brought suit challenging it on preemption and other grounds.

Stewart Baker: [00:15:19] Is this tied to doing business with the state of California, which struck me as at least plausibly escaping preemption?

Gus Hurwitz: [00:15:30] So it would apply to ISPs that are in the state, operating in the state of California.

Stewart Baker: [00:15:35] They're toast.

Gus Hurwitz: [00:15:37] Yeah. This isn't like we've seen one state passed legislation and several states through executive order say if you are doing business with the state, if your government contracts, you need to comply. This is if you're doing business in the state, you need to comply. What most people expect is going to happen is that the legislation will be enjoined pending the outcome of the challenges to the Restoring Internet Freedom Order because if that order is overturned by the DC Circuit or the preemption provisions are overturned by the DC Circuit, that makes the case that this isn't preempted, the California legislation isn't preempted. It makes it stronger. Still really, really weak. But it does make it stronger.

Stewart Baker: [00:16:26] Well, so if South Carolina is forced to take down all of their statues of John C. Calhoun, who came up with the nullification doctrine, maybe Sacramento will want to put them on the state house grounds there because that's where California appears to be going.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Gus Hurwitz: [00:16:44] And one of the fascinating things about this case is, in addition to pure preemption arguments, there are a number of dormant Commerce Clause arguments being made. So one state affecting another state not just through preemption by the Supremacy Clause grounds but interfering with interstate commerce concerns. They could be live in a way that we haven't seen in a lot of these cases before.

Stewart Baker: [00:17:07] I think that's probably right. California's got a new law that says if you are headquartered in our state, you have to have – and you have six board members, three of them have to be women. They don't seem to be saying that that's about people who use California to incorporate. They appear to be applying it to Delaware corporations that are headquartered in California. I'm guessing Delaware will bring that lawsuit, claiming there is a dormant Commerce Clause problem with the statute. The GRU. How bad must it feel to be a GRU official? Those guys, they can't do anything right, can they, Megan?

Megan Reiss: [00:17:47] They can't do anything right. There was so much that came out this past week about GRU. I'm going to start with the crazy one about the 305 cars.

Stewart Baker: [00:17:59] Oh this is just delicious.

Megan Reiss: [00:18:03] I mean what were they thinking? They registered all their cars to the same place.

Stewart Baker: [00:18:08] Right.

Megan Reiss: [00:18:08] And so now the US, the UK, Germany, everyone knows who all of their spies are. What were they thinking?

Stewart Baker: [00:18:15] They were thinking it was the Soviet Union and nobody had access to those records, is my guess.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Megan Reiss: [00:18:20] That is accurate.

Stewart Baker: [00:18:22] But yes, that was hilarious. This is Bellingcat.

Megan Reiss: [00:18:24] Yes.

Stewart Baker: [00:18:25] They really deserve a lot of credit.

Megan Reiss: [00:18:26] Good job, guys.

Stewart Baker: [00:18:27] They have outed the real identities of both of those bozos who did the Skripal killing.

Megan Reiss: [00:18:35] One of whom was a doctor, and I'm pretty sure has an obligation to not poison people.

Stewart Baker: [00:18:40] Yeah.

Megan Reiss: [00:18:41] Regardless if he's Russian.

Stewart Baker: [00:18:43] My guess is he thinks he should just poison them really well.

Megan Reiss: [00:18:47] Really well.

Stewart Baker: [00:18:47] Yeah, it's remarkable. I think I said on the last one that the UK may well have an active debate inside MI6 whether it's appropriate to assassinate these guys. I mean they say killed people on British soil.

Megan Reiss: [00:19:04] Yeah, well, but then there was the big story coming out in addition to all of this stuff, which was again DOJ indicting a number of GRU officials for a plethora of things. Everything from doping – basically during the Olympics they got caught doing this complex doping scheme –

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:19:30] And then to cover it up, they wanted to break into the anti-doping headquarters.

Megan Reiss: [00:19:38] Oh, yeah. And they conducted a pretty big disinformation campaign to say everyone does it. It's not the Russians. The Americans are doing it. The Brazilians. Everyone's doing it. So disinformation, cyberattacks. But then the other big cyberattack revelation is that they travel. We probably should have – I should have realized this – but if they weren't able to access a system remotely, they physically went to hotels, for instance, to conduct cyberattacks over public Wi-Fi.

Stewart Baker: [00:20:11] Right.

Megan Reiss: [00:20:11] Which is a big scary thing. They also attacked the Organisation for the Prohibition of Chemical Weapons and a nuclear energy plant here in the US in order to – of course, related to the chemical weapons attacks abroad and Skripal. Gosh, they just did a whole bunch of stuff they got caught for.

Stewart Baker: [00:20:37] Yeah, absolutely. And it's not just the US. The Germans, the Brits, and the dowdy Dutch, who have done more to pwn the GRU than much larger nations, all have been attributing attacks to these guys.

Megan Reiss: [00:20:58] The Dutch intercepted an attack while it was happening! And the Russians didn't do a good job of taking their equipment with them. There was some weird, weird things that happened. I highly recommend reading the entire indictment.

Stewart Baker: [00:21:13] Yes. It's a great – I won't call it a how-to, maybe a how-not-to.

Megan Reiss: [00:21:20] How-not-to.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:21:20] Alright. California has another law. God bless them. This is a law that says if you're a bot and you're dealing with a California resident, you have to announce yourself as such. You can't mislead people into thinking they're dealing with a person if you're trying to sell them something or influence the election. I kind of was wondering whether this was a sort of easy version of the Turing Test because you only have to fool Californians.

Gus Hurwitz: [00:21:53] [Laughter]

Stewart Baker: [00:21:53] But, Gus, what do you think this law actually amounts to?

Gus Hurwitz: [00:21:58] Nothing.

Stewart Baker: [00:21:59] Yeah.

Gus Hurwitz: [00:22:00] This is a weird law. As you say, it makes it illegal to be a bot, whatever that means. Okay, I'm not being fair there.

Stewart Baker: [00:22:09] It does tell you.

Gus Hurwitz: [00:22:10] It gives you some more detail. I just spoke about the FAA Reauthorization Act and said you need to get into the actual language of the legislation. It says that bots can't be designed with the intent to mislead another person about its artificial identity for the purposes of knowingly deceiving them. So this sounds like standard consumer protection sort of stuff. Deceptive behavior we can criminalize under certain circumstances –

Stewart Baker: [00:22:37] And it was probably already –

Gus Hurwitz: [00:22:38] It's unenforceable. Yeah, exactly.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:22:38] It was probably already a violation of standard fraud law. So this is just kind of foot stamp: we really mean it. Don't try to defraud us with bots.

Gus Hurwitz: [00:22:50] I think that's right. It's virtue signaling. It's pretty meaningless. Don't mess with our elections. And it's unenforceable on the national scale. Now the interesting thing I think about it is what's going to happen to it. Is this legislation going to be one of those bills that gets passed and just dead letter the moment it's passed, no one ever does anything with it? Or is it going to be challenged? There could be some really interesting First Amendment challenges in here. It's trying to regulate speech in some interesting sort of ways that could be pretty interesting and go interesting places. I expect probably folks are just going to ignore this law and it's never going to be enforced, so we won't have any challenges of it.

Stewart Baker: [00:23:33] I don't know. I would look forward to a lawsuit: *Alexa v. the State of California*.

Megan Reiss: [00:23:40] [Laughter]

Stewart Baker: [00:23:40] Yeah, I think it probably does not end up producing much, although you know it isn't just consumer protection because it also applies to electioneering. And so you can imagine California going after Twitter for not having stopped the bots from supporting some candidate that Californians don't like. Alright. More California litigation. This is an effort by the – this is sort of rumors of litigation, but the rumors are pretty clear that the US government sued Facebook under a Wiretap Act trying to get them to take action to effectuate wiretaps against some MS-13 folks. All of this has been under seal, and it's just been leaks that we've been getting. Gus, what do you think is the underlying claim here?

Gus Hurwitz: [00:24:41] So I expect this is a new iteration effectively of San Bernardino, except instead of a terrorist shooter we have MS-13, a violent gang, that the government is trying to use as the wedge probably to use the All Writs Act to force assistance on the part of Facebook in compliance with the wiretap order. But it's really

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

frustrating, this case, because we know about it but we know nothing about it other than that it's happening. The details are going to matter a great deal, but it sounds like it's a big win for the tech industry in the ongoing fight between the federal government and the tech industry for backdooring or otherwise being able to access encrypted communications.

Stewart Baker: [00:25:33] Yeah, I'm guessing it's not the All Writs Act. I'm guessing that this time they were using some wiretap authorities which are much more directed at carriers and intermediaries. There's very specific language about intermediaries being required to assist in wiretaps. And then CALEA [Communications Assistance for Law Enforcement Act] has added a gloss for certain kinds of telecommunications services and substitutes for the plain old telephone system that actually requires them to modify their systems to enable wiretaps. So either of those two statutory requirements could also have been in play, which might be why the US government would have thought that they had a shot at winning this even after San Bernardino.

Gus Hurwitz: [00:26:21] Yeah, the provisions of § 2518, the Wiretap Act's assistance provisions, are really pretty broad. I would love to see the details of this case: how the requested activity was being characterized. Was this treating Facebook or Facebook Messenger as a telecommunications carrier or equipment provider for the purposes of CALEA? Or was this just purely under the Wiretap Act? So much matters in the details for this case. And the implications could be very broad, either for the industry or for future legislation that Congress tries to push through.

Stewart Baker: [00:27:03] Yeah, or I think DOJ could probably go back to the FCC and ask for a ruling on the scope of CALEA, which is what they've done a couple of times already.

Gus Hurwitz: [00:27:14] Oh, I hope they don't do that because I hate reading those orders.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:27:17] [Laughter] Alright. Well, from your mouth to Ajit Pai's ears. Okay. Very quickly. Among the other things that Congress did is looks like finally the Senate has passed a bill that would change the obscure agency, the National Protection and Something or Other Division [National Protection and Programs Directorate] of DHS, to the Cybersecurity and Infrastructure Security Agency. So they will actually have a name that people recognize. And when they call, people will not say, "You're calling for who? For what?" And North Korea. Big story about how North Korea is apparently getting rich robbing banks.

Megan Reiss: [00:28:06] This is pretty much a story that has been around for a while. North Korea likes to attack banks to get money to fund its bad, illicit activities through hackers. And it's all –

Stewart Baker: [00:28:17] But they're like covering their tracks by wiping out the hard drives behind them.

Megan Reiss: [00:28:22] Yes, yes. But this goes along with a lot of the different types of hacking and cyberattacks that North Korea conducts. My big question is: so this is all under the Lazarus Group, which is their big hacking unit –

Stewart Baker: [00:28:35] Right.

Megan Reiss: [00:28:35] What does bureaucracy look like within this group? How did they decide to put it in this part? The hacking group versus the espionage group. Yeah, that's the big question there, I think. No, it's all along the lines of bad things North Korea does.

Stewart Baker: [00:28:48] Yes. Alright. But I got the impression that they hadn't done it that much to US banks, that there might be a little bit of deterrence at work.

Megan Reiss: [00:28:57] Deterrence or better... Yeah, yeah. Deterrence by denial, maybe.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

Stewart Baker: [00:29:01] Yeah.

Megan Reiss: [00:29:02] I'm not sure how often we've talked about North Korea trying to hack our banks publicly, so it's hard to know whether or not they're just not good at it or –

Stewart Baker: [00:29:12] That could be. Well, there's plenty of money elsewhere. Right?

Megan Reiss: [00:29:15] Easier to hack into Bangladesh.

Stewart Baker: [00:29:17] Yeah. Okay. Facebook has the usual follow-on troubles from their 50-90 million person breach, even though no one has yet figured out anything really bad that happened. I want to say I had thought that the 40 million additional items might have been third-party you know log-on with Facebook accounts, but Facebook is now saying they don't see any evidence that those third-party sign-ons were compromised. So that actually reduces the likelihood that anything bad is going to happen as a result of this breach. That will not stop the Irish and the Europeans and probably the California authorities from dropping a safe on Facebook's head. But it does make you wonder exactly what the purpose of these privacy acts are. And New Zealand has said that if you come to New Zealand and you're carrying a phone and they ask you to unlock it for them and you say, "I'm sorry. I'm not going to do that," they're going to charge you what looks like $5,000, probably New Zealand and $3,000 USD, for having defied their border inspectors. Predictably everybody's outraged, but this is just part of the ever-tightening screw that we're going to see. The Five Eyes had a statement a couple of weeks ago saying we're going to have to do more about encryption, and countries that don't have big tech companies in their territory are logical places to start clamping down. Okay. Gus, Megan, thank you for participating. This is great. We got through an enormous amount of news in a relatively short amount of time. This has been Episode 234 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. If you got somebody to suggest as a guest interviewee, please send that name to

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.

CyberlawPodcast@Steptoe.com. And if they come on the show, we will send you a highly coveted Cyberlaw Podcast mug. We actually had somebody show up in person who asked for the mug. So they truly are a highly coveted. If you want to get involved – I haven't done this, but I will start. I promise. Maybe not next week, but the week after, I'll start putting some of these stories out on Twitter, @StewartBaker, and on LinkedIn so I can get some comments from people before the show. And if you would, go to Stitcher or iTunes or Google Play or Pocketcasts and leave us a nice review. That is how other folks find us. Coming up: the general counsel of GCHQ will be on. We will be sure to ask him if he's got Moscow's light switch in his pocket. And before the election Chris Krebs, the Undersecretary, formerly of the NPPD but hopefully by the time he appears on the show he will be the proud Undersecretary head of the CISA, the Cybersecurity and Infrastructure Security Agency. So join us for those and other guests. Let me give you quick show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio engineer; Michael Beaver is our intern and makes the entire show run; and I am Stewart Baker, your host. Please join us again soon as we once again provide insights into the latest events in technology, security, privacy, and government.

The views expressed in this podcast are those of the speakers and do not reflect the opinions of the firm.