Steptoe

Episode 228: Best idea yet for derailing the Kavanaugh nomination

Stewart Baker: [00:00:03] Welcome to Episode 228 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. And our last for four weeks, so enjoy. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government. And today I'm joined for the interview by Noah Phillips, who's a commissioner of the Federal Trade Commission and an alumnus of Steptoe & Johnson. In between those two jobs, he was chief counsel to Senator John Cornyn on the Senate Judiciary Committee where he advised on, well, everything the Judiciary Committee worries about. Noah, welcome.

Noah Phillips: [00:00:43] Thank you. Good to be here, Stewart.

Stewart Baker: [00:00:45] It's a pleasure to have you here. And for our News Roundup, we've got a great lineup. Matthew Heiman, who's the visiting scholar at the National Security Institute at George Mason, formerly with the Justice Department. Matthew?

Matthew Heiman: [00:01:00] Good to be with you.

Stewart Baker: [00:01:01] Okay. Gus Hurwitz on the line from Nebraska where he teaches law at the University of Nebraska. Gus, good to talk to you again.

Gus Hurwitz: [00:01:09] Great as always.

Stewart Baker: [00:01:10] And Dr. Megan Reiss, senior national security fellow at the R Street Institute, visiting fellow at the National Security Institute, senior editor at Lawfare. And does the "doctor" mean you're not a lawyer?

Megan Reiss: [00:01:25] Well, I have an LLM, but not a lawyer.

Stewart Baker: [00:01:27] Okay. Alright. And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. Going to jump right in. Kind of a little bit ahead of schedule, at least for recent years, the National Defense Authorization Act is going to pass maybe as early as this week if the Senate gets around to it. And it's a big deal. It always is a big deal, but this year they have added more stuff than usual. An entire CFIUS review has been added to the NDAA. It was tinkered with in the House and weakened I think a little, but probably not significantly. This is a big deal for people who do investment reviews. It means a massive increase in the number of filings that people are going to have to make because it gets rid of the concept of control, it gets rid of the concept of passive investment, and looks much more closely at what kinds of information people are going to get. This is really a tribute to Senator Cornyn in his effort to deal with problems that were first flagged at the end of the Obama administration. And it is you know practically the only bill in a freestanding sense that has been passed with bipartisan support in years, right?

Noah Phillips: [00:02:51] I don't know that I would go quite that far, but there's a lot of truth to it. One of the great things about Senator Cornyn is at the end of the day he's a legislator.

Stewart Baker: [00:03:03] Yes, he is. That's right. He wants to write laws that solve problems.

Noah Phillips: [00:03:08] Correct.

Stewart Baker: [00:03:08] Yeah. It's impressive. And it also shows I think — and I won't ask you to confirm this, Noah — that it's not really possible to write legislation in committee that will likely pass. You have to have somebody from leadership who takes a personal interest to make a bill move. Otherwise, it's just too easy to stop. That's my theory. Okay. So it's been attached to the NDAA. The House has agreed to it. The Senate is not showing any signs of not adopting it. And so FIRRMA — the Foreign

Investment Regulatory Review and Modernization Act — is going to be law. It'll take about 18 months to get all of the funding and other procedures in place, but this is going to be a big deal, especially for those of us who do CFIUS. And that's not all. Megan, there's a Cyber Solarium Project in here. I think this is Senator Sasse's work, but there have been a lot of supporters.

Megan Reiss: [00:04:25] Yes.

Stewart Baker: [00:04:27] What is the Cyber Solarium Project or board or commission, and why should we care?

Megan Reiss: [00:04:35] Well, full disclosure: I worked for Senator Sasse, so I may be a little more on board with this than the average listener. But Cyber Solarium is based on Eisenhower's Solarium Project where Eisenhower looked at the information he was getting from folks at his NSC and just felt like the rigor wasn't there in figuring out how to deal with the Cold War, nuclear threats, the Soviet Union. And what Senator Sasse and his team — Klon Kitchen over at Heritage was pivotal in this — they interpreted that cyber defense and cyber strategy in the US is not as rigorous as it needs to be. So what the point of this is, is to kind of force, through legislation, big actors in the government and in Congress to sit down and spend enough time to develop a real rigorous strategy that's going to get us through not just the Trump administration but four or eight years out, the next administration, and the one after that, and it's going to kind of guide how we deal with cyber threats in the future.

Stewart Baker: [00:05:45] Okay. I see. So it does make sense, although putting all these political actors in the room kind of makes it hard to have a detailed discussion on these topics.

Megan Reiss: [00:05:58] Oh, yes. And actually, one of the parts of this that I know Klon Kitchen is really worried about is that they'll come back and it's going to look like any of these other reports where...

Stewart Baker: [00:06:09] "Oh, we need a public-private partnership!"

Megan Reiss: [00:06:10] Exactly. Exactly. Or there was a report that came out a couple years ago on cyber deterrence that I, as a deterrence person — it defined "deterrence" differently in each section because I could tell they couldn't quite agree what it meant.

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

Megan Reiss: [00:06:24] And so there's always that concern, but I think what they should do is if they get it back and it doesn't look good enough, just send it back to this committee or reform another committee in September of next year and say, "Do it again. Not good enough."

Stewart Baker: [00:06:40] So I am contributing to this. I didn't know that, but about two weeks ago when we were talking about the Russians being in our grid — and we're still talking about that — I said, "Well fine." You know I never want to hear somebody again say, "Well, denial is deterrence," because we ain't denying anybody access to our grid. That we needed to come up with unthinkable options. We needed to think the unthinkable. And so naturally I called it the Itheberg Project because we're rooting for the itheberg. And I have now 15 to 20 in many cases truly unthinkable options for responding, many of them kinetic or quasi-kinetic. You know hopefully they won't kill anybody. My favorite was the one that says, "Dear Vlad, we see you've put Black Energy in our grid. In response, we've put mines outside your commercial harbors. But don't worry. Good news is they're all at the bottom of the sea. Bad news is — and they'll stay there as long as our satellites keep sending them signals to stay there. Bad news is the device that sends the signal is plugged into our grid.

Megan Reiss: [00:07:59] So if you attack our grid, bad things are going to happen. I mean it's creative thinking. It is making sure... Look, supposedly there's never been an act of cyberwar against the US, according to our officials. But okay, so what does that mean for deterrence? Does that mean we don't have the authority to do anything yet? No.

Stewart Baker: [00:08:19] This is a complete waste of time to ask whether it's an act of war.

Megan Reiss: [00:08:23] Yeah.

Stewart Baker: [00:08:23] The question is: are we going to tolerate this as a great power?

Megan Reiss: [00:08:27] Yes.

Stewart Baker: [00:08:27] And the answer ought to be: no, and we ought to have options and they ought to not just depend on trying to shut down computers, but disabling ships, mining harbors, setting off EMPs. If somebody messes with our grid, we're going to want to do all of those things, and we should have a real list of...

Megan Reiss: [00:08:51] ...viable...

Stewart Baker: [00:08:51] ...truly scary options.

Megan Reiss: [00:08:52] Yep. And my guess is that's what this commission is going to come back with.

Stewart Baker: [00:08:55] Oh, well they can all be part of the Itheberg Project. Anybody who wants to, you can send me — two deals for listeners: you can send me proposals for the Itheberg Project. If you send really good ideas, I'll give you credit as a member of the project. And if you send just extraordinary ideas, you can take your name off the project. Alright. Gus, what else is in the NDAA?

Gus Hurwitz: [00:09:22] Oh, there's a whole lot in there. There are 12, 13, 14 different sections of the NDAA that really get into the weeds on cyber stuff, some of which, Stewart, you might really like. A couple of the high-level smaller things I think are

interesting. First, it's expressly calling for DOD to craft express policies relating to what the US is going to do in the cyber domain. The policies that we come up with probably are going to be garbage. We've done this sort of exercise before, but now we're being directed to actually come up with real policies, which at least we get to see what stupid ideas we're going to put down on paper. A couple possibly better small things: there's a call for DOD to offer assistance to small manufacturers and supply chain. This is reflective of ongoing thinking, which is I think a positive change, that we need to focus on supply chain issues in cybersecurity, and this is going a step further.

Stewart Baker: [00:10:28] Didn't I see that the Defense Department has also come up with a list of do-not-buy-these products that is aimed at trying to clean out the supply chain of companies that they believe are deeply under the influence of our adversaries?

Gus Hurwitz: [00:10:46] Right. So DOD has come up with that list, and the NDAA is going to require DOD to adhere to the DHS list as well. So there's going to be some alignment between those different government components. The NDAA also is putting in place a pilot program to simulate critical infrastructure impact. Unclear where that's going to go. It's just a pilot program that is being called for, but that's interesting. Now there are a couple of higher value things in the NDAA, the first of which I think you're really going to like based on your comments from the Cyber Solarium discussion with Megan. The NDAA basically recognized that "cyber activities are really just a new form of traditional military activities." And it says expressly that "use of all instruments of national power" in response to cyber activities are going to be considered and on the table. So we're no longer in the realm of "Oh, you did something cyber to us. We're going to do something cyber back to you." Maybe you take out our satellites, we'll mine your harbor.

Megan Reiss: [00:11:53] Can I ask you real quick? That's technically been our policy the whole time. Do you think this will change anything?

Gus Hurwitz: [00:11:59] I hope that it will end a lot of silly debate over whether or not that is actually our policy.

Megan Reiss: [00:12:06] Yeah.

Gus Hurwitz: [00:12:06] We've spent the last 10 or 15 years arguing over this, and over the last three or four years, everyone I've heard talk about this issue says, "Yeah, we don't need to respond in kind." A "cyberattack" — whatever that is — is an attack. It doesn't matter that it's cyber, so we can respond in some other appropriate way, or we could use cyber capabilities in response to non-cyberattacks. It's good. I think that at a statutory level the new congressionally directed understanding of this question is there's no question anymore. Get over it. We're going to respond however is appropriate. The last really interesting thing in there — which could be if anything is a stumbling block for the NDAA, this could be the stumbling block — it directs — and the word "direct" is important — Cyber Command to take appropriate and proportional action against Russian cyber efforts to disrupt US institutions. And this actually goes beyond Russia, but the Russian Federation is called out by name. I mean the reason this is potentially challenging is this is directing DOD to take activity that really is traditionally within the ambit of the executive. So there could be some understandable discomfort on the part of the president here. And if there is a veto, I expect it could come from this provision. I expect ultimately it will go through, but it is interesting that Congress is saying, "Cyber Command, you are directed to actually engage in some form of activity to disrupt these efforts to disrupt us."

Stewart Baker: [00:13:58] So the president doesn't like to — presidents don't like to veto the NDAA, and I would have thought you could solve this with a signing statement just saying, "Yeah, when you said 'direct,' we think that's direct in the sense of providing directions, steering, giving us guidance, encouraging us to do those things which we want to do." And if they just ignore the word "direct" or treat it as guidance, they can sign the bill and go on their merry way, right?

Megan Reiss: [00:14:34] Yeah.

Gus Hurwitz: [00:14:34] That is likely the path of least resistance, and as you say, NDAA is always understood as must-pass legislation. But also as you say, we are surprisingly early in the process this year.

Megan Reiss: [00:14:47] I will say though, President Trump last year at the signing of the NDAA actually made a pretty strong statement on — I can't remember which cyber provision it was — saying, "This should be my authority. I disagree with what this is, but I'm signing anyways." So it will be interesting with that longer time frame if he'll take that same stance on this and then push it back. I'm guessing no because they need to get a judge confirmed. They don't want to distract. But it'll be interesting. I'm guessing at least there will be a pretty strong pushback during the signing statement.

Stewart Baker: [00:15:23] Alright. From the heights of policy and grand thinking about cyber to what I have to call "the depths of lawyerly concern" about cyberattacks. The question is: if somebody spoofs an email to you saying, "Please send money to the following account. (Signed, the CEO.)," and it's not the CEO and it's not coming from his account really, is that covered by a[n] insurance policy that allows you to recover if fraud is committed on you using a violation of the Computer Fraud and Abuse Act? Matthew?

Matthew Heiman: [00:16:06] So I take issue with "the depths." I mean the heights of the nuance of standard form insurance policies I think are burning answers to all Americans.

Stewart Baker: [00:16:14] And this is going to the Supreme Court! It's a circuit split.

Matthew Heiman: [00:16:16] It is. And it's a wonderful example of a common law at work trying to figure out what these terms mean. So you're right. There are two cases that have come out during the month of July: one out of the Second Circuit called *Metadata Solutions v. Federal Insurance Company*; the second one came out about 10 days ago out of the Sixth Circuit called *American Tooling Center, Inc. v. Travelers*; both saying the same thing which is the insurance company took the not surprising position that, well, you've got a computer fraud provision in your business loss insurance policy,

but it doesn't apply to these phishing attacks because this wasn't direct. And so we went down the road of — as lawyers often do — the cold sweats over the *Palsgraf* case and what is "proximate cause" and what is "direct." And the courts in both cases said the same thing: this is direct. The insurance company said, "Well, it's not direct because you've taken the act to send the money, as opposed to someone getting into your system and forcing your system to do something you didn't want it to do."

Stewart Baker: [00:17:15] And there is a plausible argument that this doesn't violate the Computer Fraud and Abuse Act, right? If you make all the changes to the emails on your system and then send it in, it doesn't have any effect on the system. It just has an effect on the humans who populate the system.

Matthew Heiman: [00:17:29] Right. But I think, as courts often do, when you're in a new area and you've got insurers providing coverage in a marketplace, they will put the risk on the risk experts which are the insurance companies and say, "Go back. Rewrite your clauses." And some insurance companies have done that. They've carved out phishing because there's a product sale opportunity here, and they're starting to offer social engineering coverage policies...

Stewart Baker: [00:17:58] ...as a separate product, of course...

Matthew Heiman: [00:17:59] ...as a separate product from the computer fraud provisions.

Stewart Baker: [00:18:01] Yes. Okay.

Matthew Heiman: [00:18:02] So I mean where this in my view ultimately winds up is they will craft new tighter language, and new footnotes will get added to those really exciting insurance treatises where every word has a footnote with 40 cases cited as to what that word means, and this is part of that sorting out process.

Stewart Baker: [00:18:19] Fascinating. Who would have guessed that the Supreme Court's principal contribution to cyberlaw next term could be insurance coverage determinations?

Gus Hurwitz: [00:18:31] I have my hand up in the air right now because I would have guessed that. Just saying that we have a number of cyber policy insurance cases that are bubbling up, and this is a really important area for the industry. So I'm really excited about this in-the-weeds legal issue.

Noah Phillips: [00:18:50] I just want to echo Gus in that regard with a particular FTC angle here. We spent a lot of time dealing with our organic statute that requires in the cases of unfairness substantial harm. And what that means and what economic grounding you can give for various kinds of cyber losses is like a major discussion among policymakers, judges, lawyers. Insurance policies written specifically for something are a really good indication from the market of where harm exists and what it costs. So I actually look forward to see how that market develops and what it means for what we do.

Stewart Baker: [00:19:25] Okay. Alright. So it wasn't "the depths" at all. Lightning Round. Let's see if we can do these all in a minute each. The ACLU said it's shocking how bad AWS's Rekognition face recognition software is because when they ran Congress against 25,000 mugshots they found about 28 matches at an 80% probability. Gus, isn't 80% kind of sad as a test?

Gus Hurwitz: [00:19:58] Yeah. So this was a wonderful stunt on the part of the ACLU. Of course the ACLU, like most privacy advocates, they're really up in arms and concerned about facial recognition. Eighty percent is the threshold that Facebook uses for the sort of thing that tagging photos and recommendations like that, where [inaudible] the criminal law or government law enforcement context and we have a user in the loop.

Stewart Baker: [00:20:24] Yeah.

Gus Hurwitz: [00:20:25] So that's really not the right level of confidence to be looking at. The even bigger issue though is the focus here on this stunt was on a false positive. Really this technology is going to continue to evolve. It's going to continue to be developed. I actually want government and law enforcement to be involved in that process because there are problems with the technology. There are racial disparities in it, for instance. And if it's just Facebook developing this, less likely that really equal protection concerns are going to be considered as the technology develops. But really the false positives aren't the problem for the technology. It's false *negatives*. I don't care so much about: hey, when you run that group of people mugshots, are you mismatching good actors against bad? I care: is this technology actually capable of matching bad actors against those mugshots? So what's the false negative rate? And this doesn't really tell us anything about that. And that's where the technology improves. So this technology is going to continue to develop. Let's find ways to develop it well instead of trying to throw obstacles in the way.

Stewart Baker: [00:21:37] Alright. And just for people who are following the ZTE matter, China was holding hostage — Qualcomm was a viewed as a big US 5G standard bearer, and it had wanted to merge with NXP, another chip maker, designer. Everybody in the world — eight different competition authorities had approved that. And China said, "Yeah, we're kind of waiting to see on that" — presumably waiting to see how ZTE turned out. ZTE turned out fine for ZTE, and China just let the clock run out on the NXP deal which has now collapsed, and Qualcomm had to pay NXP $2 billion. So it's like the Chinese have imposed a $2 billion fine on Qualcomm because the US raised the ZTE issue. Ugly. Gus, I'll ask you about this. Should I say the same thing is happening in the People's Republic of New York as they say that they're going to throw I think Charter out of the — they're going to undo the merger because Charter didn't live up to its promises made when the merger with Time Warner occurred?

Gus Hurwitz: [00:23:07] Yeah, this is an unprecedented move in modern history. The state Public Service Commission has decided to revoke their conditional approval of the merger back in 2016. It's a really shocking development. What's really going to happen

here in the long run? Well, it's going to be challenged administratively and then appealed. The real issue seems to be: has Charter built out to the number of homes that they promised that they would build out to when they got the merger approval? And there is a disagreement over what it means to have actually built out to the homes and which regions and territories of the state count for that. So there's a lot to be litigated here. It's a really shocking development. And we're starting to see a lot of states in the telecom space try and do some kind of loopy sort of thing like this. I'm thinking the Net Neutrality and privacy efforts in particular where they're not happy with the national scale policies. And of course in the antitrust context and in the case of mergers, the states have always played an important role. But to unscramble the egg is an extreme remedy, and it's going to be really interesting to watch how this plays out.

Stewart Baker: [00:24:29] Well, we had this problem in CFIUS too, and I actually did unscramble an egg once because I thought the parties had made promises that they then — actually, I guess in that case the parties hadn't filed, and I said you should have filed. And we ultimately said, "You got to sell the company that you acquired." It happened that this was socialist Venezuela's biggest election company had acquired one of the biggest American voting machine companies. And I said, "I don't think so," and indeed the entire CFIUS said that. And then we had to force a sale. But doing it in this case is much harder because they've probably combined a lot of their activities. On the other hand, if you can't enforce — if you are going to accept deals from people in which they say, "I will do the following 12 things," you have to have some mechanism for enforcing it. So it was either this or some big fine.

Noah Phillips: [00:25:38] I think you would all read with interest an early speech given by Assistant Attorney General Makan Delrahim on, in antitrust, the preference for what we call "structural remedies over behavioral remedies." Structural remedies are like "Take that business and sell it."

Stewart Baker: [00:25:53] As opposed to "I promise to be really good and send a Christmas card every Christmas."

Noah Phillips: [00:25:59] Precisely.

Stewart Baker: [00:26:00] Okay.

Gus Hurwitz: [00:26:02] Yeah, and I was just going to actually reference that speech and queue up a question for Noah exactly on that question and how he would think about this. As Stewart says, the companies have probably consolidated a lot of operations, decommissioned or sold off switches and the like, so it's really hard to separate these. It's unclear. Will they undo the merger? Will they sell off territories to another small competitor or entrant in New York State? How will they satisfy what the PSC wants them to do? And how is that going to benefit consumers if the problem is they're not building out quickly enough? This is just going to slow down deployment if anything. Really I hope that what this will do in the long run — I hope the PSC won't be successful, but what will happen is this will clarify the conditions that state PSCs and DOJ since — Noah doesn't need to worry about the common carrier mergers. That's the FCC. But the specific terms that DOJ and the state put on these build-out requirements in order to make sure that there's real clarity moving forward in the future.

Stewart Baker: [00:27:17] Alright. And while we're on the topic of imposing massive fines on American companies for displeasing foreign regulators, GDPR took most of the blame — or GDPR compliance took most of the blame — for a 20% drop in Facebook and Twitter stock over the week. Kind of a big deal. Matthew, one sentence on this?

Matthew Heiman: [00:27:43] Yeah. Well, bad regulation has bad consequences.

Stewart Baker: [00:27:46] Yeah. And yet, as we'll talk to Noah about this, my guess is that if you were smaller than Twitter and Facebook, the hit was even bigger.

Matthew Heiman: [00:27:57] Yeah. You're probably close to out of business.

Stewart Baker: [00:27:59] Yeah. So what surprises me: Google? No sign of a GDPR dip.

Megan Reiss: [00:28:06] So stay on the line for more GDPR conversations.

Stewart Baker: [00:28:09] Yeah! We will have more on that just after this break! No, we don't have a commercial sponsor. Last topic: India is leaning on WhatsApp to start providing access to authenticate to the sender of messages. It's getting the usual WhatsApp line which is that they value their users' privacy, but they're in an awkward spot because people are getting killed because of rumors. And so this is putting WhatsApp in a position of basically saying, "Yeah, these people are engaged in hate speech and fake speech, but we can't tell you who they are." Going to be a tough fight. My guess is the Indians, who are nothing if not self-confident regulators, are gonna squeeze WhatsApp pretty hard.

Gus Hurwitz: [00:29:05] Yeah. The fascinating thing about this case — these are really tragic stories. It's kind of even worse than the cases of SWATting in the United States, where you call a SWAT team — a false call on someone — and the SWAT team shows up and throws a grenade in someone's house. This is sending rumors about someone that create a lynch mob, and they go and literally kill the person. So it's really a tragic sort of fact pattern. And the fascinating thing from the encryption debate perspective is this isn't about decrypt the contents of the communication. It's about tell us who sent the communications and be able to trace back the communications to the sender so that when the sender is causing these real harms intentionally, we can find out who they are and take action against them. So it's a metadata debate about end-to-end encryption, not a content debate about end-to-end encryption, which I think from the standard discussion perspective makes it different and pretty interesting.

Stewart Baker: [00:30:09] Yeah. And tougher for WhatsApp to hang tough on, though I'm pretty sure they're going to take a lot of incoming on this. Alright. That's our news. Now on to our interview with Noah Phillips. So Noah, it's really a pleasure to have you back.

Noah Phillips: [00:30:31] It's such a pleasure to be back.

Stewart Baker: [00:30:32] Alright.

Noah Phillips: [00:30:33] I'm not sure the listeners all know, Stewart, that I used to work in part for you.

Stewart Baker: [00:30:37] Yes, you did. You did. You have overcome the disadvantage that that conferred on you many times, but...

Noah Phillips: [00:30:45] Therapy is a great thing.

Stewart Baker: [00:30:48] It was a lot of fun. In fact, I think I worked with you for like a year without even knowing you're a Republican, which is probably prudent in a large law firm. But it's great to see how well your career has blossomed. And one of the things that you worked on — or at least heard me yelling about — was the EU, GDPR, and of course my hobbyhorse PNR, which is the data that the American government collects from incoming carriers to know who's coming on the flight before they arrive here so that they can make decisions about whether they want to screen them or not. And that has been in dispute with the US and Europe really since 2002. And there currently is an agreement that PNR data will be gathered with some restrictions imposed by the EU, but the European Court of Justice has thrown a monkey wrench into the debate by saying, not about the American standards but about the Canadian standards, that they just don't meet the high standards of the European Court of Justice has for being adequate under European law. And so we've got a fight coming, I think. Maybe the European Commission will be on the US side this time because they have woken up to the value of PNR. But the FTC plays a role in these discussions that I think'd be useful to hear about from your point of view.

Noah Phillips: [00:32:29] Sure. And thank you for the opportunity to speak to that. Obviously the FTC doesn't play a specific role with respect to PNR, but I think it is very safe to say, as you did, that we play a very important role facing the Europeans and other countries abroad with respect to the US and privacy. The first role that I think we

play is we are and have long been the most important federal agency when it comes to enforcing consumer privacy. We have a series of risk-based statutes and regulations from financial data to data about children that we enforce and we also, as I mentioned earlier, have our organic statute, and we have brought privacy cases for decades under all of those laws. That's the first point. The second point is that in the course of doing all that enforcement and in meeting the test that Congress laid out for us over 100 years ago to sort of be an educated and informed agency that in turn educates and informs the public, we and the great staff at the FTC have done incredible work thinking about privacy and thinking about the application of privacy law: how it helps consumers, how sometimes it can hurt competition, a whole host of different factors. And I think we have a lot to teach others. I think we have a good message that we can bring. And then I'd be remiss if I didn't also mention: there are certain specific instances — and I'll pick on another agreement that I know you're very familiar with, that's the Privacy Shield and its predecessor the Safe Harbor Agreement — we brought about 50 cases to enforce those and CBPR, the APEC agreement. And it's important that we do that where there are violations because that's an important part of meeting our international commitment.

Stewart Baker: [00:34:29] Because the European Union thinks of you as the equivalent of their data protection commissions. That is to say independent and able to take action without the oversight necessarily of the elected chief of government. And even though you don't have a mandate from Congress that has "privacy" and "data protection" in the words of the statute, they've more or less accepted you as the equivalent of their data protection commissions.

Noah Phillips: [00:35:02] That seems to be how things have shaken out, yes.

Stewart Baker: [00:35:05] So Julie Brill used to play a role as a commissioner engaging with the Europeans on all of these topics and bringing such prestige as a data protection commissioner would have to the debate. Is there some formal assignment of role to a particular commissioner to take that job, or does it just sort of fall to whoever is most interested in going to Paris?

Noah Phillips: [00:35:38] Well, in this case Brussels, and that's an important distinction.

Stewart Baker: [00:35:42] That is an important distinction! I can see you're already trying to down sell it to make sure that Sharon doesn't want to do this.

Noah Phillips: [00:35:47] There isn't a formal role assignment. To some extent it has to do with who has the appetite and who has the interest. I think this is an area where you can expect to hear from me in the future. Recently, a couple of weeks ago, the chairman and I met with the LIBE committee crowd who come annually to the United States. They are very concerned about the adequacy of Privacy Shield. We did our best to explain the important role that I mentioned before that the FTC plays.

Stewart Baker: [00:36:17] So one of the things I hope you'll raise with them often is that they only have the right to restrict exports of data under the WTO agreements if they are not acting unreasonably or discriminatorily. And discrimination is measured by what you do, not what you say, not the apparent neutrality of your rules. There must have been 50 disputes with the United States over exports of data on the Internet and related to it in the last 15 years. There have been none with China, even though China is going to be close to or surpass the United States in supplying elements of the mobile Internet in 5G. And there are millions of tourists and others in Europe right now using Chinese apps that send their data home on Chinese phones that send their data home running on Chinese infrastructure that sends its data home to China. And no one in authority seems to have challenged those data exports on the ground that the constitutional protections of China don't measure up to the august standards of the European Court of Justice.

Noah Phillips: [00:37:41] Let me say two things. The first is I'm glad to be able to throw a flag I throw from time to time which is that the "trade" in Federal Trade Commission is not the same "trade" as in WTO.

Stewart Baker: [00:37:51] That's true.

Noah Phillips: [00:37:52] And that is not fundamentally within our remit. Let me say the following. One of the interesting things to me about the discussion back and forth in particular between Europe and the US about commercial privacy — let's leave aside to some extent the national security and law enforcement side — is that they approach the question from kind of a fundamental rights perspective. And I think it's important, by the way, that Americans when we talk to Europeans that we recognize that. They have a different tradition of laws. They have a different history than we do. And so it's — we have to take those into account when we speak to them. And by the same token, when they think about us, they have to understand that our sort of rights approach to privacy is really the Fourth Amendment and the laws that Congress has built around it on national security and law enforcement, stored communications, that sort of thing. So we have, if you will — and I hate to use the postmodern terminology — a little bit of a different lens. But I think given that, it's fair for Americans to ask: if these rights are fundamental to you, why are there inconsistencies, if those inconsistencies exist? I think those are fair questions to ask.

Stewart Baker: [00:39:06] Yep. Okay. So you don't have legislative authority either in privacy or in cybersecurity, which is intimately tied to it and which you've enforced in 50 or 60 consent decrees. The LabMD decision looks to me as though it really — it's creating a serious authority problem for the Commission because the Commission is used to catching people doing something they shouldn't do, squeezing them hard, and then offering them a consent decree in which they promise that for the next 20 years they'll do all kinds of good things, and then enforcing that and telling the world, "Well, if you want to know what you should be doing, you can read our consent decrees." But due to what I think was just dumb stubbornness on the part of the FTC — the last FTC, I should say — it pursued a case against LabMD all the way to the Eleventh Circuit, and the Eleventh Circuit was a shaky case. And the Eleventh Circuit said, "You know we read this consent decree, and we don't see how you could enforce it. People need to know exactly what they're supposed to do so they can be held in contempt if they don't do it, and vague language that requires people to do good stuff isn't specific enough for us to impose sanctions on people who fail to adhere to it." Is this going to require real rethinking of the business model of consent decrees for the future?

Noah Phillips: [00:40:45] The case is, as you know, still technically in litigation, so I'm mostly going to demure on that question. Let me say the following though. The Eleventh Circuit, like any federal court and in particular any federal court of appeals, is something we need to take very seriously. Beyond that, what I would say is: there is something of an irony in that what seemed, at least to my reading of the opinion to concern the court in part, was what it felt was vagueness in the order.

Stewart Baker: [00:41:17] Yes.

Noah Phillips: [00:41:17] I think we can actually quibble back and forth how vague the order was. But there are times when parties with which the FTC deals don't necessarily want check-check-check when it comes to data security. And how this order bears on that tension I think remains to be seen.

Stewart Baker: [00:41:34] I completely agree. You don't really want to be told to do 20 things that make sense today and won't make sense in five years. But the Eleventh Circuit is also saying, "Please don't try to futureproof this with vague language." And I recognize you don't want to discuss the details of that, and I appreciate that. You should take it — the Eleventh Circuit — seriously. The last Commission should have taken seriously their own ALJ decision which said, "No, this is not a good case." And instead I have to say I think this was the bad staff and a Commission that listened too hard to 'em. I'm not going to ask you to comment on that. They should've recognized they had a loser by the tail and cut their losses. But okay. Let's talk about competition law because it ties to this. Silicon Valley is full of what might be evanescent, but which are pretty deep-seated, market niches that nobody is going to be easily pushed out of. Networking effects and the tyranny of code defaults means that you know it'll be hard to dislodge Google for search or Android for mobile phone operating systems or Facebook and Twitter for social media because you know everybody else is there too. So you just stay. And I've been interested — and frankly, so has most of Congress — in the way in which those market dominances are exploited in non-financial terms. And in particular, employees of Twitter and Facebook have, I think it's fair to say, enjoyed the way in

which their market dominance allows them to shut down conservative speech more aggressively than Left-wing speech. And I guess my question is: to what extent is that a legitimate concern of competition policy?

Noah Phillips: [00:43:55] Let me start by saying outside competition policy that may very well be a legitimate concern. With respect to competition, though, there are two things that I would note. The first is that even though it doesn't often seem like it on any given day or even in any given year, the market does have ways of correcting things. So if there is demand for a product that isn't being offered and the demand is real, the market can offer that product. Maybe one of these companies sees the value in that competing product, and maybe that's how that the issue gets solved. That's the way that competition, not quite competition policy, may solve the problem. With that said, personally I am reluctant to get antitrust law into the business of addressing problems, however real they may be, but that are ultimately exogenous to the concerns that animate antitrust law. One of my concerns is that it may leave us without a clear rule of decision. So choosing between a diversity of voices and efficiency, where do we go?

Stewart Baker: [00:45:09] Right.

Noah Phillips: [00:45:09] There may be no answer to that question. The second is: I am concerned that you entrust folks like me who may not be experts on those questions or like our staff or what have you with trying to make decisions on those bases. And I think there's an accountability problem there, and there's a practical problem there. So I'm a little bit leery of dropping competition law into that particular issue.

Stewart Baker: [00:45:36] Although as you as you lay it out, you might say that is a harm that might be part of the consumer harm that would justify structural changes designed to ensure greater competition. You might say, "Well look, these guys are taking their monopoly profits in moral preening," let's say, "as opposed to more income. But we can account for the fact that there is still a market dominance and an extraction from at least some part of consumers. And therefore, we're going to weigh that along

with the consumer harm from lack of competition for advertising dollars in deciding whether we have a basis for pursuing a breakup option."

Noah Phillips: [00:46:30] Look, I'll say the following. There are a lot of folks out there today who look at a lot of different problems and say that's something antitrust can address. I mean really the list grows daily.

Stewart Baker: [00:46:40] Yes, every day.

Noah Phillips: [00:46:42] I am concerned about adding to that particular pot.

Stewart Baker: [00:46:44] Okay. So then it probably troubles you that the Chinese seem to have decided that this is just an all-purpose way of asserting themselves in global markets and showing that they are not without weapons in trade wars. I don't see another explanation for the decision to let the NXP deal expire. And that raises the question — we've also seen this $5 billion dollar fine against Google on grounds that they don't compete with Apple apparently, which again seems a little questionable — it raises the question: what can US competition authorities — you and the Justice Department — do when you think that foreign countries are abusing competition law to achieve completely unrelated purposes?

Noah Phillips: [00:47:47] So this to me is the most important reason not to allow into our antitrust law all those sorts of exogenous concerns. When you cross that Rubicon, what will result is more of that kind of conduct from other countries. I'm not going to speak to the merits of what the Chinese did on NXP or the Europeans on Google. One of the things that the US has done really well for decades is take our consistent, coherent, rational, and reliable antitrust law and take it to other countries. I've been abroad to help do this — many others have before me, and many others will after me — to show the benefits of the law, the real rule of law, that we have. Once we succumb to the temptation to find other goods, it will be even more encouraging for other countries to do that.

Stewart Baker: [00:48:44] So I hear you, but I wonder if you might not have some second thoughts. At the end of the day, when you go to foreign bureaucrats and say, "Here's a really important weapon. It's potentially fatal to some companies. And you can wield it, and we recommend that you wield it on behalf of this particular cause, which is efficient markets." Once you get handed them the weapon, you can't be sure they're actually going to take your advice about how to use it. And we are now in a position where there are a dozen countries or more that can kill a deal. I'm beginning to wonder whether deals are ever going to get approved at all.

Noah Phillips: [00:49:26] Let me say one thing. I think they've had the weapon.

Stewart Baker: [00:49:30] Yes. Okay.

Noah Phillips: [00:49:32] You know to the extent antitrust law is a weapon. But fundamentally, I don't think it should be a weapon, and I do think we have a role to play in explaining to them why an antitrust law that is an important weapon for consumers and for competition isn't well used in other regards. You want to attract foreign direct investment? You want your markets to operate efficiently? You want a good market for corporate control? This can help you. If it's whimsical, if it's up to the government to pursue exogenous policies, those may not work out as well.

Stewart Baker: [00:50:06] Okay. You know you gave a talk Friday to the Internet Governance Organization. I was also there, and I read your remarks. And the thing I was struck by was the theme or the concern that you expressed that privacy is going to cement the advantages that big companies have because they can throw a thousand, well Filipino, contractors at a particular problem and solve it even if it feels like excessive regulation, whereas their struggling competitors don't have those kind of resources. Is there more to be said other than to be careful what you wish for?

Noah Phillips: [00:50:58] I mean I think that's a really important point. I think there's a lot more to be said on privacy. We're hearing it every day. We're going to hear a lot more. But what I wanted to accomplish in that speech more than anything was to say to

people: consider this question when you run ahead. In particular, the United States is having a more and more robust discussion about whether and how we do privacy regulation. It can have this anticompetitive effect. And maybe that's worth it. Right? Maybe we want to trade for all the goodies of privacy the well-being of startups and this sort of thing. But the point is to have the discussion. To pretend that issue doesn't exist is not a good idea.

Stewart Baker: [00:51:45] Yeah. So I have made this argument in connection with cybersecurity that we get cybersecurity mainly from companies with very strong market niches. Microsoft does a great job on its operating system. Google does a pretty good job on Android. Apple does, as you might expect since they make more money off of theirs, an even better job with their operating system. And nobody does anything for the Internet of Things because they're $15 devices that no one makes more money on. And I have said you know maybe what we need is an Apple or a Microsoft or a Google to establish a market niche where they are making so much money they can afford to give us some cybersecurity. So I've had that argument for sure. It does make sense at some point. I think the Europeans are uniquely comfortable with concentrated industry. Makes it more efficient to have your lobbying. It's easier to punish the people you hate. You can identify, you can find 'em, and you can fine 'em $5 billion for breathing or being in your market. And remarkably, Google is a stronger company — its market dominance much stronger in Europe than it is in the United States. And I'm not going to ask you to comment on any of that. I do want to ask you about how the Commission's relationships are shaping up. It's been a pretty — I won't say bipartisan — but it has been a Commission characterized by more comity than say — my choice — the International Trade Commission, which seems to always be fighting with each other. Part of that is having a strong chairman, but it's also a tradition. And I wonder whether you see that tradition continuing in the Trump era?

Noah Phillips: [00:53:46] I certainly hope so. Look the history of bipartisanship at the FTC is something of which we are all proud. And when we were all coming through our confirmation processes, the senators were very concerned about that. They wanted it to

continue. I think we all want it to continue. As you know, bipartisanship requires give and take, and I hope we're up to that.

Stewart Baker: [00:54:10] Alright. And so you're going to do a whole bunch of the hearings. Now we've come to the point...

Noah Phillips: [00:54:13] We're going to do a whole bunch of hearings.

Stewart Baker: [00:54:15] ...where you get to promote all of the activities that you want our listeners to participate in. Principal among them was a bunch of hearings on competition policy. Is that right?

Noah Phillips: [00:54:26] They're actually not limited to competition.

Stewart Baker: [00:54:27] Okay.

Noah Phillips: [00:54:28] So they include privacy and some other things. Net Neutrality. The chairman has put out a notice that we are beginning in the Fall going to do a series of hearings that will last months on a variety of different topics. This is an important opportunity for us to begin to grapple with a lot of the big questions that a lot of folks have laid out about almost everything we do at the FTC. I think the comment period closes pretty soon, so for those folks out there who are interested in making sure that we hear from you and speak to the issues about what you care, I think the information is available on our website — how to weigh in.

Stewart Baker: [00:55:09] Okay. Well, I will try to get in my traditional view that the FTC should acknowledge now that it's involved in cybersecurity, which has a big national security component, that it like the FCC will defer to the executive branch on national security issues. It's never said that, and one questions whether it wants to say that. But it would be prudent now for the FTC to be more candid about the ways in which it interacts with national security policy and the ways in which it could serve national security policy. So I will submit that, and I look forward to appearing before you at some

point to testify on that. How about you? Are you going to be giving any more speeches? Off to Brussels, assuming nobody else thinks that Brussels is someplace they want to go to?

Noah Phillips: [00:56:01] Oh, I think Brussels is very much a place I want to go. I was just distinguishing it from Paris.

Stewart Baker: [00:56:05] Yes, yes, yes. I'm sure it's just that nobody's spouse wants to go to Brussels. That's my view.

Noah Phillips: [00:56:12] Having given my last speech three days ago, I don't have anything — I actually probably do have something on the calendar, but it's so far in advance I don't yet want to preview it, but I will let you know.

Stewart Baker: [00:56:25] Alright. Well, thanks to Noah Phillips for a wide-ranging and thoughtful and, in some cases candid but not too candid, set of remarks. I'm going to give a little bit of reader feedback. We got a couple of notes on the Bobby Chesney deep fakes note. Mark Siegel said, "I'm not sure I get the point. It's always been possible to lie, and lots of people do. And we should get used to essentially figuring out what's a lie and what's not." Michael Collins raises the question, which I think is a little bit of an answer to Mark Siegel, which is: what do we do once state actors start faking the watermarks and distributing really persuasive fakes for political goals of their own? And now let me just say thanks to Noah, thanks to Matt Heiman, thanks to Gus Hurwitz, and thanks to Dr. Megan Reiss for joining me. This has been Episode 228 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Remember you've got a month of drought ahead of you unless we decide to start releasing a few of the better interviews with a new introduction. We haven't quite decided on that. So check your feed. Maybe you'll have something to listen to, and maybe you won't. Otherwise, enjoy August. Send us your suggestions for people we ought to interview in September: cyberlawpodcast@steptoe.com. I'll come back in September and start tweeting again about possible stories. Love to get your feedback on that. Love to get your feedback in reviews on iTunes and Google Play. Show credits: Laurie Paul and Christie Jorge are

our producers; Doug Pickett is our audio engineer — I always feel as though I'm NPR when I say that — Michael Beaver is our intern and organizing principal; I'm Stewart Baker, your host. Please join us again in September as we once again provide insights into the latest events in technology, security, privacy, and government.