Steptoe

Episode 245: “Pay no attention to the guns, the flashbang, and the handcuffs. You’re free to go at any time.”

David Kris: [00:00:01] We have a confession: Culper Partners is actually an AI.

Stewart Baker: [00:00:07] [Laughter] Terrific. So Nate and David are actually sipping piña coladas somewhere in the South Pacific?

David Kris: [00:00:16] That's exactly right, and we programmed these avatars to interact with you in an extremely realistic way. I think we've definitely passed the Turing Test.

Stewart Baker: [00:00:24] Absolutely. Absolutely. [Music] Welcome to Episode 245 of The Cyberlaw Podcast, back for 2019 and brought to you by Steptoe & Johnson. We've been gone almost a month, and so it's a pleasure to be back and to have as many stories as we have. So we're going to skip the interview and just extend our News Roundup to talk about all the stories – or at least the most important stories of the last several weeks. I'm going to be joined by Nate Jones, co-founder of Culper Partners and formerly with both the Justice Department and the National Security Council's counterterrorism office, and by David Kris, who with Nate was a co-founder of Culper Partners and was the Assistant Attorney General in charge of the National Security Division at Justice. Nate, welcome.

Nate Jones: [00:01:20] Thank you.

Stewart Baker: [00:01:21] And David, too.

David Kris: [00:01:22] Thank you very much, Stewart.

Stewart Baker: [00:01:23] And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. I should tell you at the outset we're really pleased that The Cyberlaw Podcast is now available on Spotify. So if you're looking to listen to us on Spotify, you can do that now. Alright. Silicon Valley, courtesy of *The New York Times*, is complaining that export controls on artificial intelligence are going to wreck the AI industry in various ways. Nate?

Nate Jones: [00:01:59] This all stems from a November Advance Notice of Proposed Rulemaking that came out of the Commerce Department in which they listed a pretty long and broad set of categories of technology that they are considering for export restrictions on national security grounds. And as you've noted, they've received some critiques from industry and from the technology industry in particular. And you know obviously that's no surprise. These people have to serve their shareholders and represent their business's interests, and this type of restriction poses some potential threat to certain markets that they currently operate in.

Stewart Baker: [00:02:44] And so my sense on this is, first, this is actually part of the CFIUS [Committee on Foreign Investment in the United States] reform review that kind of to everyone's astonishment achieved bipartisan consensus around a pretty innovative approach in the bill called FIRRMA [Foreign Investment Risk Review Modernization Act]. And part of FIRRMA was to say we also ought to address technology exports using export controls, not just using controls on what companies can be invested in. And because export control law hadn't been updated in 20 years, there was a decision that there had to be a massive update that was going to be driven in part by DOD, in part by Commerce, to find the new technologies, the foundational and emerging technologies, that had to be controlled aggressively in order to prevent China from eating our lunch militarily. And this list is sort of a quick and dirty list of technologies that DOD mainly thinks need to be controlled in some fashion. So this is all part of a relatively large effort to change the legal framework that the US has been using for the last 60 years from the presumption that export controls were not needed since the Cold

War ended to something that says we really need to go on to a much more aggressive adversarial footing in dealing with China.

Nate Jones: [00:04:34] Yeah. I think that's right. And you know I think if you talk to folks in industry, even some of them would admit at least privately that it is a sensible question to ask. You don't want to wake up 20 years from now and realize that you've made a big mistake by not doing something on this front. But I think you know the million dollar question is what to do. Right? And I think if you read between the lines in the Advance Notice, I think it's pretty clear that the administration doesn't really know what it wants to do quite yet.

Stewart Baker: [00:05:07] I think that's exactly right. There's an assumption that something has to be done, but nobody knows exactly what it is. And artificial intelligence is kind of the classic case because artificial intelligence could be anything from simple tools that identify likely parking places and run on your phone to very sophisticated machine learning algorithms that the people who design and use them don't even understand how they work. And figuring out the point at which you're just going to say, "Oh, this is commodity now. This is a commodity, artificial intelligence," is a pretty tricky line to draw.

Nate Jones: [00:05:56] Yeah. It is. And I think you know from whether you're in the government's position or in the industry's, I think there are at least sort of three things that you need to think about and frankly worry about. First is a process issue, which even in the best of times issues of this magnitude and this complexity are hard for an interagency process to grapple with. And when you're relying on the Trump interagency process, it's like hitting cleanup for the Milwaukee Brewers when you're not given a bat. Right? And there are tactical questions, as you were alluding to, about sort of you know even within these broad categories where are the risks coming from. How do you mitigate them, and how do you actually effectuate any policies that you decide to pursue in this sort of nebulous and somewhat hard to control realm of technology? And finally, you have the big strategic question weighing over their heads which is many believe that AI and machine learning and some of the other things listed here are sort of the

next big wave of technological advancements, and whoever wins this race is going to take a giant leap forward and we really don't want to do anything that's going to screw that up. And so the stakes are pretty high for them, and they're facing some pretty mighty daunting challenges in trying to come out in a good place here.

Stewart Baker: [00:07:21] Yeah. It's gonna be very difficult to figure out how to run this process, how to administer regs of this kind, and the enormous lists that have been produced without any real sense of exactly how they will be implemented is just an example of how hard that's going to be. This is an Advance Notice of Proposed Rulemaking, which means there'll be at least one, probably at least two, further rounds of comments. So anybody who has an idea about how to do this or an industry to protect from a bad implementation needs to get in and start filing comments. While we were gone, there were some APT10 indictments. APT10 is a Chinese attack group. And the indictment goes after just two members of the group, but it describes some exploits and some targets that are pretty troubling. David, your National Security Division was responsible for bringing a lot of these indictments and has brought a lot since you left. What's new about this one?

David Kris: [00:08:45] Well, it's actually more of the same, I think, in main band. They have definitely stepped up their actions at DOJ against China. There's an official China initiative that Attorney General Sessions announced before his departure. John Demers, who is currently running the National Security Division, has been very vocal both in congressional testimony and in public statements about the threat posed by China. The FBI, including the FBI director I think, has said pretty explicitly now that they are trying to replace us as the world's superpower. So they are sounding the alarm, summoning all hands on deck to deal with China. The debate here is really part of the larger debate about exactly what the proper role of law enforcement is in counterintelligence. And it's similar to a debate we've had and in some ways we continue to have about the role of law enforcement in counterterrorism. There are legitimate points of view on both sides of that, but that's what this has sparked, this increased law enforcement activity against China.

Stewart Baker: [00:09:48] So [Professor] Jack Goldsmith has a piece in Lawfare saying this is just a failure. The idea of indicting our way out of a cyberespionage problem is played out. It's not going to work. And he and Robert Williams muster some pretty good arguments about the fact that we've seen a modest decrease for a moment in time under the late Obama Administration and then a revival of commercial espionage by the Chinese despite much more frequent use of indictments. Do you think that's a fair criticism?

David Kris: [00:10:34] Not totally. No. I mean Jack is definitely the smartest and one of the most vocal critics of the use of law enforcement in this counterintelligence context. I mean everybody agrees that you prosecute spies for espionage, but the larger question is about the broader role of it in the overall program. And I think that the point that I disagree most with in Jack's views here is that it seems to me he sets the bar too high and then accuses law enforcement of failing to meet that bar. That is, of course the indictment strategy – if that's what you want to call it – has not produced perfect results. Nor has anything else that we have done.

Stewart Baker: [00:11:15] Right.

David Kris: [00:11:15] And so on that basis, you might just say that everything – sanctions and diplomatic pressure and covert action and anything else we may or may not have done – have all failed, but that doesn't, to me at least, make the case that there isn't a role for law enforcement as part of a larger mosaic or constellation of US government activities. So if you just sort of lower your expectations a little, then I think it doesn't seem to be as much of a failure, and I think there are some things in some cases that a law enforcement strategy can contribute to the overall strategy. But they have to see it as such in the government. It's not clear to me that they really do have an overall strategy so much as just a series of individual actors pursuing opportunities where they see them. And that I think is part of a larger problem. There's not really any evidence of an overarching strategery here.

Stewart Baker: [00:12:10] That would be the interagency process in the Trump Administration, right? Everybody doing what they think they can and want to do?

David Kris: [00:12:20] Right. And that to me is the larger problem here. Law enforcement can be a small but non-trivial part of an overall strategy, but only if you actually have an overall strategy and put it into effect.

Stewart Baker: [00:12:31] So this is not sufficient. Obviously these indictments are not sufficient. They looked briefly as though they were having a pretty significant effect, and that seems to have been played out. And we'd like to solve this problem or at least dramatically reduce the incentives to carry out cyberespionage, especially for commercial purposes. What is it we should be doing that we haven't been doing? We've certainly been putting plenty of sanctions on. We certainly have been indicting plenty of people. I don't think Jack has a lot to suggest, and to a degree his counsel is usually, "Well, suck it up. It happens to other people, too," which I must say I find equally unsatisfying compared to the naming and shaming and failing that we're doing with indictments.

David Kris: [00:13:27] Yeah. You know the distinction here I think is between the economic espionage and other forms of espionage because when the Chinese hacked the Office of Personnel Management and stole all the security clearance forms for you and me and Nate and others you know many former members of the IC actually sort of tipped their hat and didn't exactly applaud it but did give it some respect. That's old-fashioned espionage. Both sides do it. Both sides try to stop it, but we sort of all agree that in some meta sense it's inbound. We're going to prosecute people if we can catch them. But state to state, high level, that's part of the game. We think and we have tried to get the Chinese to agree that stealing economic information for economic purposes as opposed to intelligence purposes is sort of a different type. We failed, it seems, so far to do that successfully. And I don't have a magic bullet. I don't think Jack does. I don't think anyone really does. I think this is one where you just have to keep pressing in a strategic way using the typical combination of carrots and sticks that are available to try to motivate other states to do things and see things the way you want them to do them

and see them. We haven't had a lot of success. There was a moment where maybe it looked like it was going to get better. It hasn't. But if we make it a priority and we keep pressing, you know maybe things will change over time. But that's the way I see it. I don't see a simple magic bullet that's available here.

Nate Jones: [00:14:59] Getting other states to care about it as much as we do or at least close to as much? I think this is one more area in which we're seeing that American influence isn't quite enough to get us over the hump and deter certain activity, and we frankly haven't been getting the kind of support from international partners on countering some of this stuff that we probably need to get to be more effective.

Stewart Baker: [00:15:24] But we got the G20 to sign on to a ban. We got the Germans to sign on to a deal with China that was meant to stop commercial cyberespionage. They have done some things, and we haven't asked them to do a lot more. I agree with you we ought to ask them for more. I am at work on a list of 25 truly shocking things that we could do in response to cyberattacks, things that really crossed lines for us. I have been calling it the Itheberg Project because we'll be thinking the unthinkable, and when you want to think the unthinkable, an itheberg comes in handy. And I think the answer there is to start looking for tools that are much more kinetic – but not necessarily fatal – that have deniability, that have reversibility, that have some of the advantages of cyberattacks but that play to our strengths in kinetic and power projection capabilities in ways we haven't in the past. So at some point I'll come out with a paper on that, and you can look forward to at least a set of amusing and occasionally pretty serious options that we should be deploying beyond indictments.

David Kris: [00:16:44] You know, Stewart, when it comes to thinking the unthinkable, there is literally no one like you. So I, for one, am definitely looking forward to your list. I mean it is certainly true that if you sort of really prioritize this and you decided that this was you know in your top five or 10 foreign policy initiatives – and I'm not sure frankly that it is, even for you – you could do a lot of stuff. I mean, hey, you could just cut off diplomatic relations with the Chinese if you really want to tell them that you're cranky about it. So the question though is you know will doing something like that have

collateral consequences that you don't like. So I do look forward to your unthinkable list. It will certainly be informative and educational at a minimum, and maybe it'll get you a job in the NSC [National Security Council].

Stewart Baker: [00:17:30] Oh, God! What's the second prize? Two jobs at the NSC? Alright. Hacks of the month, very quickly. We saw newspaper production interrupted and looked like maybe it was going to be states, and then it turns out it was probably ransomware. Merkel gets all of her personal phone data and the phone data of a lot of other German politicians doxxed, and everybody says, "Oh, this is too serious to have been done by kids," and then it turns out it's a kid. Right? And then the North Koreans break into a bunch of South Korean agency files to find refugees and asylum seekers from North Korea who have relocated to South Korea and who are obviously going to be the subject of harassment by North Koreans in the future. As I read it, a lot of pretty standard stuff. Nothing too surprising there. You guys see it differently?

David Kris: [00:18:35] No, it looks like just more and more and more and more of the same. Whether it's state-sponsored by the Russians or some other government, whether it is some 400 pound guy living in his parents' basement – or even someone not that heavy – there's just more and more of this kind of stuff going on. I think though you know as more and more institutions become victim of this – and I'm thinking particular that the US judicial and legislative branches are potentially vulnerable – we're going to see more and more ugly emails that were written in haste or written stupidly, and you know it sort of seems to me likely to lead to a further undermining of trust in our institutions, maybe deservedly. But I think in any event it will happen, and so we're going to have to learn to adjust to this new world as a society both by increasing our cybersecurity and then maybe also by sort of trying to see these kinds of disclosures in a broader context.

Nate Jones: [00:19:32] Being more thoughtful about what we write down. [Laughter]

Stewart Baker: [00:19:37] Yes. In theory that works. When you're thinking about it, it works, but it's very tempting not to think about it. Okay. So I want to ask you guys about

the Hal Martin case because again it's a national security case. He's the guy who is accused of hoarding a whole bunch of [NSA] exploits at home. He was busted. And there was some thought that he might have been the source of some of the materials that were actually released online. That's looking more complicated, isn't it?

David Kris: [00:20:15] Yeah. There was a recent decision by the district court that denied two and granted one of his motions, in particular his motion to suppress statements that he made when the FBI came in a large group with SWAT operators to his house, handcuffed him, put him on the ground, and so forth and so on. The whole mosaic of the case is a little bit hard to figure out right now, but there's clearly a lot of activity going on on Twitter and in chat rooms and bulletin boards. The core of the judicial ruling that just came out was basically that although Martin, when he was arrested – well, when the agents came to his house, handcuffed him, and put him on his couch, set off a flashbang grenade, and started searching through the house pursuant to a search warrant – they told him that he was not under arrest and he was free to leave. But the judge basically said you know you have all these agents standing around you with their guns pointed at you and you've been handcuffed and put on the ground and then you're seated on the couch while the agents run through your house, you don't really feel free to leave. So he should have been Mirandized. He wasn't, so his statements were suppressed.

Stewart Baker: [00:21:24] So that struck me as a perfectly reasonable interpretation of the situation. He couldn't talk to his long-time domestic partner. It was extraordinarily coercive environment. And my question for you is obviously the Justice Department has something to say about how the FBI conducts these raids. Did they just decide let's let the FBI do it and if he confesses we'll fight over whether it was coercive or not? Or do you think the FBI went beyond what the Justice Department wanted them to do when they conducted this interview?

David Kris: [00:22:04] You know I frankly doubt that the Justice Department lawyers got into dictating to the agents whether and to what extent they would Mirandize him in this. I mean the Bureau has its MIOG [Manual of Investigative Operations and

Guidelines], which is extremely detailed manual of how it proceeds, and some of that inevitably gets left to the discretion of the agents on the ground. So it's certainly possible that the prosecutors discussed with the agents an arrest scenario and the use of Miranda in particular. But I think it's also possible that the agents just sort of thought they were following their standard procedure. I have to say though reading the judge's opinion, I do think like you that you know the judge's decision is not wrong given everything that happened. When you have all these SWAT operators there with their body armor and so forth and they set off flashbang grenades to do a little overpressure check in case there's a booby trap or something, you know it's not just a walk in the park for the recipient of that kind of thing. So I don't know why this happened, and I'm not at all sure that the prosecutors made an informed decision to roll the dice on getting him to talk. It's certainly possible. But it might also be that they just didn't get into that kind of micromanagement and planning ahead of time.

Stewart Baker: [00:23:24] So I've got a theory, and the theory is that these are counterintelligence FBI agents and they do a moderate number of arrests and almost no trials so that they don't pay the price if they screw up in this way usually. But in this case they are prosecuting him, and they did screw up and they will pay a price.

David Kris: [00:23:48] Yeah.

Stewart Baker: [00:23:49] So let me jump – first, very quickly. There's a nice article from *MIT [Technology] Review* saying that quantum technology is going to be an arms race issue between the United States and China, and they talk about some applications of quantum technology. Kind of remarkably no real discussion of quantum computing. Instead it's all about the uses of entangled photons for intelligence purposes, for encryption, which I think is a you know highly over-hyped technology in terms of its ability to change the course of warfare, and the kind of more interesting idea that you can entangle a couple of photons and send one of them out to find an enemy plane that is using stealth technology. You can tell when photons that are entangled were set out and come back, and that allows you to identify enemy planes in ways that you can't if you're just looking at a bunch of incoming signals. So that sounded kind of interesting.

I'm not sure how transformative that is, but it's a pretty big deal if you're relying on stealth. Let's talk quickly about litigation involving privacy. Los Angeles has sued the Weather Company for collecting location data – which of course we all know they collect location data, but apparently they've been collecting very detailed stuff. And Los Angeles almost certainly at the insistence of some plaintiff's law firm has decided that that's a violation of California's commercial reasonableness rule. Anything going on there that we ought to focus on?

David Kris: [00:25:45] I guess two things struck me about it. First is you know through litigation, maybe through legislation, social activism, and other ways, we are going to be having sort of a more focused national conversation about exactly what consent means because there is in the Weather App a general consent and statement and warning that you know we get information and we share it with partners. But how much information, how frequently, how granular, with which partners, for what purposes? All of that is obviously not included. And it may be that we're going to have to refine what we expect by way of notice and consent in these kinds of cases.

Stewart Baker: [00:26:29] Yeah, but this is a classic case of you're damned if you do and you're damned if you don't. They can only squeeze so much onto the screening or phone before you just say, "How many of these screens do I have to scroll through before I click 'I accept'?" So the idea that they should have talked more about what you were consenting to just raises the question of if you talk more, aren't you likely to be confusing people and beating them into submission by page after page of a privacy policy.

David Kris: [00:27:03] Yeah. I think that that's right, and that'll be part of the conversation that I think this lawsuit represents, which is exactly – how much is just right, between too little and too much, in the way this is disclosed? And I think the other aspect of this is just the tremendous economic value of Big Data aggregation of location information, including micro-weather information, and the uses that can be made of it. So this is likely to continue. I think there's big money to be made here if you do it at scale. And the question is you know what do consumers need to be told and what do

they have to agree to in order to allow that to happen. This thing is about $2,500 per violation, so if this lawsuit has legs, you know because this thing is happening at scale, it could become quite expensive for IBM, who owns the Weather Channel.

Stewart Baker: [00:27:57] Well, and this is California unfair business practices law, so it's very vague. And the courts have been so far kind of reluctant to just say, "Oh, yeah, everybody gets $2,500," for things that are not obviously scams and frauds. But you're right. We're going to see lots of litigation over this. Have you followed the litigation over the Illinois biometrics act? I sort of view that as a revolt of the judges. They're just not willing to impose liability so far at least.

David Kris: [00:28:41] In one federal court case, court basically found no standing in some people who used Google Photos and whose facial geometry was captured and stored by Google. But there was nothing else. There was no commercial use of that you know in the sense of selling it to other parties, nor was there a data breach, nor was there really anything other than the mere collection of it. And a federal court said that is not enough. It's true that you know state legislative findings that there is an injury in fact are relevant to standing, but based on the record the court saw in the Illinois legislature, it didn't find that there was enough. It sort of invited the legislature to make some additional findings, and that might change the balance going forward. But that was the result there.

Stewart Baker: [00:29:29] Well, standing is a federal doctrine. It says, "Well, we, the federal courts, aren't going to address this because we don't think there's enough at stake. It feels like people are asking us for an advisory opinion." But the state courts don't have that out. They're gonna have to address this. And I guess the [*Rosenbach v.*] *Six Flags* case is where they're going to address it.

David Kris: [00:29:54] Yeah. Because in that case the plaintiff's son had his fingerprint collected – biometric information collected – when he went to the amusement park. There was no breach. Again I don't think there was any use. The statutory question seems to be whether he was really "aggrieved" and therefore entitled to sue under the

Illinois Biometric [Information Privacy] Act. And we will I guess find out what the state courts think when that ruling comes out.

Stewart Baker: [00:30:23] Yeah. I have to say all of these standing and was-he-really-aggrieved points strike me as not getting to the heart of the problem, which is that the courts just don't see what the problem is with the collection of this data. There's no harm identified, but it surely is open to states to say, "We're not looking for harm. We think that the harm is implicit. The risk is real. And we're just going to tell people if you collect this data, you will pay and pay and pay." And you don't need to have standing for that, and I guess that's why these cases probably are going to end up in state court because the feds may not find standing, but the state courts don't have to.

David Kris: [00:31:11] Yeah.

Stewart Baker: [00:31:12] Okay. Very quickly. I like this story. I just can't resist this story. There's a kind of generative [adversarial] network form of AI in which you run exercises back and forth and each side tries to see if they can improve on what the other side did. And it's basically just two algorithms battling each other to see whether they've done a good job of making the decisions that had to be made. And this was a decision about how to translate maps into satellite photographs and satellite photographs into maps. And as the generative network algorithms moved back and forth, they started doing a remarkably good job of identifying map data from the satellite photographs. And it turned out the reason they were doing that is they were hiding all the relevant satellite data in the maps so that they could recoup it later, so it's really a form of steganography. Now you can say what the artificial intelligence had done was found a way to "cheat," or you can just say that the people who were running the algorithm, because they didn't understand how the results were being achieved, did not realize that the results were not being achieved in the way that they thought. But it certainly shows we're gonna have algorithms that seem to do magical things, and if we don't find ways to understand what they're actually doing to achieve those results, we're gonna have shocking miscarriages and surprises in the course of using it. But it was a

great story with the implication that maybe the artificial intelligence was just gaming us. I don't think that happened, but we won't know when it does.

David Kris: [00:33:26] We have a confession: Culper Partners is actually an AI.

Stewart Baker: [00:33:31] [Laughter] So Nate and David are actually sipping piña coladas somewhere in the South Pacific?

David Kris: [00:33:42] That's exactly right, and we programmed these avatars to interact with you in an extremely realistic way. I think we've definitely passed the Turing Test.

Stewart Baker: [00:33:50] Absolutely. Absolutely. Alright. Some actual law got actually passed by an actual Congress. Kind of amazing at a time when everybody says nothing works in Washington. The SECURE Tech Act got passed, and it did you know some small but useful things with respect to the Department of Homeland Security. Nate?

Nate Jones: [00:34:15] Yeah, it did I guess three primary things: It directed the secretary of DHS to develop a process for addressing security vulnerabilities that are discovered within DHS's network; it establishes a bug bounty pilot program; and I think the dark horse in this legislation is the establishment of a process to identify and address supply chain risks. Now setting up a process is nothing new and may have happened anyway, but, similar to I guess that the risks from AI and the other technologies we talked about earlier in the Commerce Advance Notice, we are hearing some grumblings that there are concerns about supply chain risks within the executive branch. And how they ultimately deal with them through this process I think will be very interesting.

Stewart Baker: [00:35:05] Yeah. So on the whole, especially I guess in cybersecurity, we do continue to see the vestiges of bipartisan concern, and we got a little bit of legislation. Whether that will help on the shutdown's not clear since about 45% of the DHS cybersecurity workforce has been furloughed as not essential. I kind of am puzzled

by that. Actually, here's a question for you, David. You probably dealt with shutdowns. It is my theory that what we're gonna see in what is almost certainly going to be a very prolonged shutdown, we're going to see a lot of strain on the question of who's essential. There are plenty of people who are not essential if you're going to be shut down for a weekend and who are essential if you're going to be shut down for a month. And I wouldn't be surprised to see the president calling more and more people back to work as essential as a way of responding to the stories about how terrible the shutdown is and why the president should back off his demands. Instead, I think he's going to make it less terrible, and I don't think there's really a lot of legal ability on the part of Congress to tinker with that.

David Kris: [00:36:25] You know I'm not an expert on the legal background, but certainly I think you're right as a political matter. If the shutdown continues, there's going to be pressure across a whole variety of government agencies and functions to reclassify. And that'll have interesting effects on morale because I think employees – I've been through several of these as a career employee, as a political appointee, as well. On the one hand, you don't want to have to go and work for free, and it's kind of demoralizing. On the other hand, everybody likes to be thought of as essential. And so there can be some interesting effects on workplace morale. But I think you are probably right. You know with respect to getting tax refunds back and then with respect to airport security and with respect to even civil litigation at some point, you can certainly imagine a wide variety of retail-level classifications that allow more and more individual functions to occur. Whether that's coming from the president or whether that's coming from the Cabinet secretaries or below and bubbling up could be either way. But I think you're right.

Nate Jones: [00:37:28] And one of the great ironies here, of course, is that the first place they've suggested that they're going to call more people back to work is the IRS, so –

Stewart Baker: [00:37:37] Only to issue the refunds! [Laughter]

Nate Jones: [00:37:38] Exactly.

David Kris: [00:37:41] Not to collect taxes!

Stewart Baker: [00:37:43] Exactly. No, in the hands of a different president this could be a really sharp partisan knife to say, "Yeah, the government is shut down, but it turns out the only programs that are shut down are the ones that the Democrats care about." I don't think this president's likely to be able to pull that off, but you never know. Alright. Last item: I just want to make a recommendation to our listeners of an article that I just thought was fascinating and deeply weird in *The Verge* – a very long article – about Amazon Marketplace, which actually is a lot bigger – you don't notice it when you're on Amazon, but you're much more likely to be buying from somebody other than Amazon when you buy stuff. And the competition to be the third-party supplier who gets the coveted "Buy" button is extreme and full of dirty tricks because if you're number two and there's one guy ahead of you, if you can find a way to get Amazon to say, "Oh, that's not a product we want to be selling," you become number one and you suddenly get a boatload of money. And so my favorite is when a bunch of scooters started catching fire, Amazon got very serious about product safety, and so people who were number two, three, four, or five in line to sell their products would buy the product that was number one, set it on fire, and then send a video of the thing on fire to Amazon, saying, "I bought this, and it burned up," which immediately bumped them off. And in the usual charming Silicon Valley way, there was no way to find a human being to talk to. You had to fit their algorithm, and their algorithm was you had to confess that you had done it and that you had changed something. So there are like whole law firms devoted to telling people how to confess to Amazon and get their number one rating back by changing something, anything about the way they sold their product. It's a fascinating dive into a world I didn't even know existed.

Nate Jones: [00:40:15] It was a fascinating article. I particularly enjoyed the thin socks. [Laughter]

Stewart Baker: [00:40:20] [Laughter] Yes. We'll leave that for our listeners to try to figure out what that is. But as I said, it's in *The Verge*. It's a great article. Alright. Thanks, Nate. Thanks, David for joining us. This was terrific. This has been Episode 245 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Please send us guest interviewee suggestions, and we'll send you our highly coveted Cyberlaw Podcast mug. Send those to CyberlawPodcast@steptoe.com. If you want to follow me on Twitter, I will from time to time flag the articles that I think we'll cover in the podcast. But this week I didn't, so I apologize. Please rate the show. We got a couple of new ratings in. Go rate us on Spotify, especially, because we just got started there, because well we're just disorganized. I'm going to have a fun interview coming up with Jeff Jonas, who's the founder and CEO of Senzing, who's really the master of agglomerating data into undeniable identities and a host of applications from card counting rings in Las Vegas and terrorists in the Middle East and people who just want to make sure the voting rolls are accurate and up to date. Show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett's our audio engineer; Michael Beaver's our intern; I'm Stewart Baker, your host. Please join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.