Steptoe

Episode 250: We give you Weaver

Matthew Heiman: [00:00:08] I don't think Russia's having to work really hard to hack our electrical grid if this is what we've got in front of them.

Stewart Baker: [00:00:13] So I thought I would scare you more. It's not so much what violations they found as what they thought it took to get a violation. You know those password rules? I can't believe these are still the rules. But this is what they said: "Each password used by an electrical utility shall be a minimum of six characters long." That'll show 'em! Right? How long, Nick, would it take to run a rainbow table on six characters' worth of passwords?

Nick Weaver: [00:00:45] [Laughter] Done.

Stewart Baker: [00:00:49] Yeah, exactly! Yeah. In less time than it takes Nick to jeeringly laugh at the proposal.

Matthew Heiman: [00:00:55] If I remember right, the password "password" is eight characters, so that would survive that criteria.

Stewart Baker: [00:01:01] [Music] Welcome to a milestone Episode 250 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. And I should say that any resemblance between the views expressed here and the views of our clients, partners, and institutions is purely coincidental. Joining me on the News Roundup: Matthew Heiman, Visiting Scholar at the National Security Institute, previously with the National Security Division and Justice; David Kris, co-founder of Culper Partners and former Assistant Attorney General in charge of the National Security Division at Justice; and Nick Weaver, Senior Researcher at the International

Computer Science Institute at UC Berkeley. I'm Stewart Baker, formerly with NSA and DHS, the host and provocateur for today's program. Let's jump in with a story that I think should send chills down your back if your bank still sends you SMS messages as a second factor authentication when you log in to your accounts. David, the Justice Department caught a couple of people engaged in utterly defeating that kind of system.

David Kris: [00:02:27] Right. So they arrested a couple of guys in late January for a SIM swapping scheme to steal cryptocurrency. It has a certain alliterative ring to it. What happens in a SIM swapping scheme is the bad guys call up the cell phone companies, the providers of service to their victims, and they persuade them to port the phone number from the victim's SIM card to the bad guys' SIM card. And I'm sure Nick can explain this way better than I can, but you know a SIM card is that little thing about the size of your fingernail that goes into the side or back of your phone and tells the phone companies sort of what your number is. So it's an identifier for your phone. And they got the cell phone companies to switch the numbers over, which then allowed them, as you pointed out, they can interfere with two-factor authentication because now these text messages and calls would go to them rather than to the victims. And they hacked their way into the victim's digital lives. They stole various things from them, including cryptocurrency, and they also extorted them. The result was a bunch of charges under the Computer Fraud and Abuse Act and various extortion and fraud statutes. So yeah, this is concerning if you're using SMS for two-factor authentication. It would be better to use an authenticator app or something even a little tougher.

Stewart Baker: [00:04:00] Nick, anything to add on the technique of SIM swapping schemes?

Nick Weaver: [00:04:05] That it often depends on corrupt phone company insiders or social engineering at the phone company. So in some cases, these SIM swappers would basically trick the phone company. In other cases, they would actually just literally bribe a phone employee to do the swap. And the problem is the phone network has to support such swaps because what happens when you lose your phone? You get a new phone. You get a new SIM card. You have to be able to tell the phone company, "Hey,

route all phone calls to this new device." And so the bad guys are just taking advantage of that error recovery mechanism.

Stewart Baker: [00:04:53] My favorite social engineering device was a woman who did this kind of thing, and she had a tape recording of a crying baby – really, really upset crying baby – which at about two minutes into the call she started playing over and over again, saying, "Oh, God, I'm just so harried! I've got to fix this right away! Oh, my God, there's a baby!" And you know if she got any kind of empathy out of the person doing the swap for her at the phone company, she got it in you know two and a half minutes. But that's actually only one of the vulnerabilities that we're talking about today. There's also an indication that there are new ways to exploit vulnerabilities in the signaling system so that without even stealing somebody's SIM card – reassigning their SIM card – you can get all of their text messages and their location data. Nick, what's this all about, and how worried should we be?

Nick Weaver: [00:06:00] This is actually something that we should have been worried about for a long time. So SS7, Signaling System 7, is how all the phone companies talk to each other, and thanks to cell phone roaming, basically random phone company has to be able to say, "Hey, Stewart Baker's cell phone is at my network. Route all calls to it." And so bad guys have used this for all sorts of things. They've used it for tracking people. They've probably used it for espionage. If I was a senator on the Intelligence Committee, I would ask the NSA personally, "Have you seen SS7 attacks on my phone numbers and those of my staffer?" Because the answer is probably yes. And the problem is we're on the trajectory that's so common in the computer world is yesterday's national security technique is today's common criminal. And so crooks in Europe have somehow compromised or bribed or somehow gotten connection with a phone company that can speak on SS7 and have been using this to intercept SMS-based two-factor and steal from the banks that way.

Stewart Baker: [00:07:21] Yeah, and that sort of takes SIM swapping schemes and commodifies them and industrializes them so you can just take them in large gulps. You

can just – once you know the number – you just tell the home registry, "I need to know who this person is, and since he's here, send his messages to me."

Nick Weaver: [00:07:47] Yep. And it wouldn't surprise me if these days there's probably one or more underground forums where you can actually just buy it as a service.

Stewart Baker: [00:07:57] Oh, of course!

Nick Weaver: [00:07:58] So that's the real revolution in cybercrime over the past decade has been specialization in services, and so I would bet $50 that there is at least one service where you can pay with WebMoney or possibly cryptocurrency – but probably WebMoney, which is basically Russian PayPal that kind of says, "Criminality? Who cares?" – and perform this attack by just providing money.

Stewart Baker: [00:08:29] So is HaaS a thing? Hacking as a Service? Because that's what it sounds like.

Nick Weaver: [00:08:35] Oh, yes!

Stewart Baker: [00:08:36] Yeah. Absolutely. Terrific.

Nick Weaver: [00:08:38] Yes. Hacking as a Service has actually been around for a while. So if you want to, say, build a botnet of 100,000 computers for other purposes, you actually pay a pay-per-install service that will hack a huge number of systems for you, and depending on where the systems are in the world, you might pay more or less.

Stewart Baker: [00:09:01] So that does raise the question: did the [*National*] *Enquirer* get all of [Jeff] Bezos's romantic – I guess they're romantic, and actually they were pretty romantic as these things go – messages to his girlfriend by hiring phone hackers, or is it Bezos's girlfriend's brother who provided the data? Actually, we don't know the answer to that, and I think the only question for us, since we can't ignore this story – or at least I can't, what can I say – is what are the legal issues here? Jeff Bezos framed

this – this was a brilliant step on his part – he framed the whole issue by saying, "I am being extorted by the *Enquirer*, which has threatened to publish below-the-belt selfies," (I thought that was a nice sort of bowdlerized version of the usual expression), "in order to get me to agree not to accuse them of writing stories about me that are politically motivated," in particular, this girlfriend-divorce story. And a lot of people have been saying, "Well, that was extortion straight up. They said, 'We have these pictures of you. We'd like to settle this case. All you have to do is agree with us that we are not engaged in a politically motivated campaign, and we will implicitly or explicitly not run with these additional bits of information we have about our story.'" So I'm a little skeptical about whether you can make an extortion case there out of two lawyers. I mean practically every settlement I've ever been involved with could have been repackaged as extortion because you're giving up or failing to do something that will be really painful in exchange for some action on the part of the other side. But I know, David, you're a little more inclined to believe this is extortion.

David Kris: [00:11:15] Yeah, I am. I mean I think if you look either at the Washington State statute, which is probably what would apply here – Bezos lives near where I live in Seattle – or the federal law, 18 USC § 875(d), I mean most of the elements of extortion are pretty clearly met. There's interstate commerce. There's a threat to injure reputation. There's a thing of value probably being exchanged here, which is the forbearance or the statement that AMI [parent company of the *Enquirer*] is not politically motivated in its reporting. I agree with you, Stewart, that sort of the key issue is whether there's sort of this claim of right to do what they wanted to do anyway because if you take the doctrine too far, you could repackage every settlement discussion as an extortion. But I think here there's enough distance between what they have a right to do and what they're demanding that Bezos do in order to get them not to publish. I think the case probably works legally and probably would have some jury appeal. Imagine that they had said, "Give us money, or we're going to publish these photos." That would be sort of a textbook case of extortion. Supreme Court's actually ruled on such a case under the auspices of the Travel Act way back in the 1960s in the *Nardello* decision. So I think this has got legal and potential jury appeal, and if I were AMI's lawyers, I would be very, very

scared right now, particularly because, of course, they're under a non-prosecution agreement that gives the government additional leverage.

Stewart Baker: [00:12:53] Right. In which they agreed they wouldn't commit any further crimes.

David Kris: [00:12:58] Right.

Matthew Heiman: [00:12:58] Right. And I think the other interesting thing about that is in connection with the non-prosecution agreement, where they promised for three years to keep their nose clean. It's not limited to federal crimes. So going back to David's point, whether you can articulate a claim under Washington State law or New York State law, which based on my very quick reading of the statute seems to be a little bit easier to prove up an extortion case than under federal law, I think the federal prosecutors in Manhattan have some interesting choices in terms of what they want to do with AMI, which could be as simple as not worrying about a jury trial involving prosecuting AMI for extortion but simply going back to the judge that officiated over the non-prosecution agreement and say, "Judge, we've got a violation, and you alone can decide whether it's true or not that's something's been violated."

Stewart Baker: [00:13:51] But they'd have to have a mini-trial.

Matthew Heiman: [00:13:53] They'd have a mini-trial, but it'd be a judge trial rather than a jury trial.

Stewart Baker: [00:13:57] Interesting. Okay. So David, you had said if they'd ask for money, it would have been an easier case. Now, that's for sure. I guess the question is whether there is something that Bezos could have sued them over if they had just published these pictures and be damned, right? If they have a full legal right to publish the pictures, it's a little hard to call it extortion when they say, "We're willing to give up that right if you'll give up the right to stop accusing us of something that isn't true."

David Kris: [00:14:28] Yeah. There's sort of two elements in that. One is the thing of value aspect of it, which is the difference between just cold, hard cash and some other action here. I think most courts would find that what they were asking for was a thing of value. I think you're right, though, that there is this question about the claim of right, which is – I think, though, the courts have understood that not to be as simple as what you just said, which is that if you could do the thing that you are saying you would otherwise do, you can't be guilty of extortion. The courts, I think – and they're sensitive to the First Amendment concerns and other concerns that lie here, and I frankly don't know since I don't know how they got the photos, whether they would indeed have a right to publish them – but they usually want a tighter fit between the action that the extorter is seeking and the right that the extorter allegedly has. And here they're not sort of saying something to Bezos about the photos, per se. They're actually telling him to stand down from an investigation and disclosing results of the investigation of them. So I think that's a little bit too far afield probably to fit within this claim of right defense. And I also think to the extent they start putting up some kind of news gathering defense here, of course, although they are sort of a news outfit, they're actually trying to stop the *Washington Post* and Bezos from reporting the news, not trying to report it themselves in the extortionate elements.

Stewart Baker: [00:16:05] Yes. I think you're right, although I have to say if you've been on the receiving end of a sophisticated reporting, you know that there's an element of extortion in every call because the call usually begins, "Here's the story I'm running with. Would you like to correct it, or should I just publish something that will ruin your reputation forever?"

David Kris: [00:16:30] Yeah. "Tell me your side of the story."

Stewart Baker: [00:16:32] Exactly. So I think if you're the media, you kind of don't know who to root for here.

David Kris: [00:16:42] Complicated with two media organizations involved.

Stewart Baker: [00:16:46] Last question. Well, let me ask you the last question, which is: is it conceivable that these text messages found their way to the *Enquirer*'s hands without a violation of the Computer Fraud and Abuse Act [CFAA]?

David Kris: [00:17:00] You know that's – right. I mean there's lots of strange ways. I suppose the brother, who is apparently an ardent Trump supporter, the brother of the girlfriend, might have taken a photo of the girlfriend's phone. Maybe that wouldn't be a violation. I don't know. I think one of the representatives of AMI said on TV that they were using a longtime source here. If that source was hacking, then there would be a huge problem. If it was something more like a betrayal of trust from the brother, then maybe not. I just don't know.

Stewart Baker: [00:17:33] Just putting in her passcode would be enough to violate the Computer Fraud and Abuse Act. So unless she gave him the passcode –

Nick Weaver: [00:17:42] Not necessarily.

Stewart Baker: [00:17:42] Okay.

Nick Weaver: [00:17:43] If she gave him the passcode, it would be authorized access. And there's been cases going up and down with different answers to the question of basically: if somebody has the passcode but kind of exceeds what he or she is supposed to do, is that CFAA? And this has so many civil libertarian types worried because there hasn't been a clean answer one way or the other. But one other thing that's important to remember is on modern email, it's actually a lot harder to forge than it used to be because the mail servers will sign things cryptographically. So there'll be a nice paper trail for saying that the emails that Jeff Bezos published were as sent by the *Enquirer*'s lawyers who decided to violate Stringer Bell's Maxim.

Stewart Baker: [00:18:39] Which is you never take notes on your conspiracy?

Nick Weaver: [00:18:44] Yep.

David Kris: [00:18:44] Stewart, can I just ask? I mean I've settled a number of cases on behalf of clients, as have you and I'm sure Matthew too, and in the way that the *Enquirer*'s content folks and lawyers papered this, particularly the one email from the content director, I thought was pretty stark. I mean I would not have counseled my clients to phrase things that way in an email, even if they were pursuing this kind of a scheme.

Stewart Baker: [00:19:12] Yeah. I think, though, that you can't pass the New York bar without knowing how to write these letters just this way. It's sort of, "You sleazeball. You're going to jail forever. And by the way, how are the kids?"

David Kris: [00:19:30] [Laughter]

Stewart Baker: [00:19:30] So I think this may just be lawyers who think that this is how hardball is played. I agree with you. It was a little dumb and a little stark, but we didn't get all of the correspondence. We got the correspondence that Jeff Bezos wanted to put forward, and so he may have deliberately plucked from it the one exchange that had been sort of triggered by some behavior on the side of his lawyers that would make this more understandable. But we don't know that yet.

David Kris: [00:20:02] Well, I mean I acknowledge there's some tough issues in this, but I would not be feeling very comfortable if I were AMI right now. That is for sure.

Stewart Baker: [00:20:13] So I guess we should close this with this question: what kind of romance is it when you say, "Darling, I love you so much I'm leaving my wife, and I'm going to ensure a felony charge against your brother"?

David Kris: [00:20:31] [Laughter]

Matthew Heiman: [00:20:31] Well, or maybe put another way, Stewart, the practical takeaway for your vast swath of listeners is if you're dating one of the world's great tycoons, maybe don't lend your phone to your siblings.

Stewart Baker: [00:20:42] [Laughter] Yeah. It's sort of sad that when there's that much money involved and the stakes are that high and President Trump is tweeting about you – better use WhatsApp. Okay. Moving right along. I thought what was happening in Europe involving Facebook and social media generally deserved at least a little attention. The Irish data protection agency has 15 or 16 big cases, and half of them are against Facebook. They've issued warnings saying, "Don't you dare merge your databases about WhatsApp and Facebook and Instagram." And at the same time, there's a lot of antitrust competition law action. Both the Commissioner for Competition Vestager has said, "I think there's a big problem with data and dominant industries," and the German cartel office has said, "We think Facebook is the dominant player" in whatever market sector they identified – probably wasn't social media, which is what I'm sure Facebook was arguing – "and therefore the use of data is subject to special regulation." And they started to suggest that there were going to be new limitations that would prevent Facebook from again combining this data. I am not entirely persuaded that there is as big a privacy problem here. But I am interested in what the competition authorities are saying. Matthew, did you look at all these cases?

Matthew Heiman: [00:22:38] I did. I looked at a certain number of them, and I think it is the twin clubs of the Europeans: one club being GDPR and the new muscle they have to enforce and levy big fines, and then the other is the one you mentioned, which is the competition authority led by Vestager saying, "Well, there's anti-competitive effect of having all this data pooled and having companies control it." And I continue to think it's really interesting that the primary targets of all these happened to be the American Big Data platforms, and you know I anxiously look forward to seeing some GDPR enforcement against European players in this space.

Stewart Baker: [00:23:18] Or Chinese players! [Laughter]

Matthew Heiman: [00:23:20] Or Chinese players in this space. So you know this is what Europe's doing. I do think that Facebook made their hole a little deeper in connection with the one case you mentioned, Stewart, around integrating the three platforms – Facebook, Instagram, WhatsApp – because they had the then-WhatsApp leadership going into European commissioner offices, saying, "Oh, no, this will never be pooled. We're going to be independent." And it was a way to assuage all the concerns that are now being brought to the fore. And now all that seems to be by the by, and it's evidenced by the fact that the founders of Instagram and WhatsApp are now gone from the Facebook empire because they said, "We've lost our independence." So Facebook seems to do what it typically does, which is make promises that need to be made at the point in time they need to make them and then back away from them later and explain why they were mistaken before. So you know I can quibble with the merits of what the EU regulators are doing, but I don't think Facebook makes its case any better when it goes back on its word within four or five years.

Stewart Baker: [00:24:24] So I agree that massaging the regulators has never been their strong suit. I'm really interested in the – as you know, I think that basically Facebook is getting Twitter mobbed here. They're the company everybody loves to hate, so of course they're violating data protection law because everybody's violating data protection law. The question is: who do we pick on? And we pick on the people we hate, AKA Twitter mobbing. I'm more interested in the idea that maybe there is a data concentration problem here. But don't you think that the ultimate remedies fall into very different buckets? On the one hand, you say, "We're going to not allow you to share this data under data protection rules. You can't share it. You can't combine it." But if you're worried about concentration of power through the use of data, wouldn't you be looking for mandated sharing of data? Say, "You need to make this data available to six other competitors. Otherwise, you will maintain your concentration and your duopoly or dominant position forever."

Matthew Heiman: [00:25:44] Yeah, but that remedy, the latter one you articulated, the mandating of sharing it with six other competitors completely runs into the wall of: what does privacy mean? If I give my data to Instagram, and now the competition regulator

says, "Well, to make this fair in the marketplace, I need to share Matthew's data with these other six competitors," then I'm thinking, "What does privacy mean at this point? And why do we have the GDPR the first place?"

Stewart Baker: [00:26:10] We have the GDPR so that we can Twitter mob people we don't like! It's all about protecting privilege at the end of the day and signaling virtue. Alright. The PLA [People's Liberation Army] is out of the business of stealing commercial secrets because the Ministry of State Secrets [MSS] is in the business of stealing commercial secrets. David, what's the latest on MSS's activities in the US?

David Kris: [00:26:34] Yeah. So you know it should surprise no one that there may be some rivalry within the vast Chinese Intelligence Community, much as there is from time to time – or so I've read – within the US Intelligence Community, and for a while there, the People's Liberation Army had believed they were celebrated in various DOJ indictments. Then there was an agreement to stop doing that, and now the Ministry of State Security, in cooperation with something called APT10 – Advanced Persistent Threat Number 10, also known as various other things, including Stone Panda, Potassium, Red Apollo, and many other wonderful names – is engaged in a very major hacking scheme. And two folks were charged in December with trying to steal intellectual property and confidential information, and they seem to be pursuing efforts all across the globe, including in Norway and the United States and elsewhere, and the US government is hopping mad about it.

Stewart Baker: [00:27:36] Yeah. And, if I'm right – and, Nick, maybe you can weigh in on this – one of the things that MSS specializes in – one, I guess my sense is their tradecraft is a little better than the PLA's was, and two, they've been breaking into intermediate service providers so that they can compromise their customers, which strikes me as pretty chilling because you know you can't necessarily know whether you're at risk because it's your outsourced provider of IT services that's been compromised.

Nick Weaver: [00:28:12] That is, from what I understand, something that they've been doing, and it's an effective strategy. So if you outsource stuff to some cloud hosting provider, somebody takes over your cloud hosting provider, they can take over the instances. If you connect to those instances, you might be able to connect back, therefore getting you a foothold into the target institution. There's all those things. Plus, overall it looks like the Chinese have been doing a lot of what I think should be called "DATAINT" [data intelligence]: collect huge reams of data, no matter the source. So the Marriott hack –

Stewart Baker: [00:28:52] The Anthem hack.

Nick Weaver: [00:28:56] Scrape stuff. The Anthem hack. Et cetera. So that whenever you want to target an individual or generally an institution, you can find the individuals, find the individuals' weaknesses, and then go from there. And it looks like that is the new part that they're really practicing by hacking all these huge data sets.

Stewart Baker: [00:29:20] Yeah. Or maybe they think they can eventually. I don't know that there's a lot of evidence that they're actually doing that. Maybe they are, but I haven't heard the FBI say that they think that happened, and they certainly find people who are compromised all the time. And I'm sure the Chinese run compromise ops against people who don't get compromised fairly often. You would think that if they had specialized information, they'd end up using it in ham-handed ways that told us they were using it. I just haven't gotten any sense that that's happening yet.

David Kris: [00:29:56] You know one thing that might be going on here is the Chinese are obviously very interested in collecting huge amounts of data in order to help train their AI algorithms. And they have a lot of data, unlimited basically data, on their own people, but Westerners may have different habits or behavior patterns, and if they can get enough data from Marriott or other sources like, they may be able to use it generally to help train their models, which would be a benefit to them. So even if they're not doing any particular kind of compromise operation, it still may be beneficial.

Stewart Baker: [00:30:33] Oh, I love that because they've got the OPM [Office of Personnel Management] stuff that tells them all about a whole bunch of government officials, some of them intelligence operatives, and they could dump all the Anthem data and the hotel data into a machine learning algorithm and say, "Can you find the people who are engaged in work for the US government that we should be interested in?" And since they know the answer, they can actually evaluate how good a job their AI is doing.

David Kris: [00:31:02] Right.

Stewart Baker: [00:31:04] Okay. Alright. Speaking of foreign government attacks on the United States, there's a $10 million fine floating around aimed at an electrical utility. The name was redacted when the order imposing the fine was released, but reporters have said it's Duke Energy. Matthew, did you look closely at this?

Matthew Heiman: [00:31:31] Yes. I think it is a scary story because Duke is considered by and large to be one of the Class A utility providers in terms of resourcing, funding, profitability. It's supposed to be a really well-run large utility, and some of the things that NERC, which is the North American Electrical Reliability Corporation, which is a quasi-governmental entity that kind of polices this stuff, referred to FERC, which is the Federal Energy Regulatory Commission – my two favorite acronyms, NERC and FERC, working together – found some really gaping holes in cybersecurity practices at Duke Energy. Things like technicians sharing passwords with other employees, not updating cybersecurity such that Duke's own engineers are blind to hacking attempts for six months at a time, just really kind of sloppy practices. And the scary thing about that, of course, is with all the stories about Russia in our electrical grid, if this is what a best-in-class company looks like, we can only expect the same or worse from the rest of that industry. And so just points out that you know I don't think Russia's having to work really hard to hack our electrical grid if this is what we've got in front of them.

Stewart Baker: [00:32:44] So I thought I would scare you more. It's not so much what violations they found as what they thought it took to get a violation. You know those password rules? I can't believe these are still the rules. But this is what they said, this is

the rule that they require: they require that "each password used by an electrical utility shall be a minimum of six characters long." That'll show 'em! Right? How long, Nick, would it take to run a rainbow table on six characters' worth of passwords?

Nick Weaver: [00:33:26] [Laughter] Done.

Stewart Baker: [00:33:26] Yeah, exactly. Yeah. In less time than it takes Nick to jeeringly laugh at the proposal.

Matthew Heiman: [00:33:32] If I remember right, the password "password" is eight characters, so that would survive that criteria.

Stewart Baker: [00:33:38] And this is what NERC and FERC are saying. These are the cybersecurity standards. And when you read the settlement – and it is a settlement, that's also significant, I think – it is endless little check-the-box, "I came through with my clipboard, and I found this violation. I found that violation, and there was rodent feces on the floor." At some point you say, "This is compliance over security." And yet, this is all we have that protects the cybersecurity of the grid.

Matthew Heiman: [00:34:16] Yeah. And it makes you wonder, too, if there couldn't be more creative ways by our regulators to incentivize cybersecurity best practices, whether it's long-term monitoring arrangements where they're trying to hack on a regular basis to really test are companies doing what they say they're doing.

Stewart Baker: [00:34:33] Yeah. Yeah. Okay. Last story. This strikes me as the least likely civil liberties scandal to get legs that we've seen in the last year. It was an effort in the *Washington Times* to say, "Oh, we should be really worried that the Justice Department is going after a North Korean botnet by going in and figuring out who's been compromised and getting them to respond to different instructions than the instructions that the North Koreans are sending them." It's the Joanap, I guess is the name of the botnet. And DOJ essentially got a court order saying, "Yes, you can go find those computers, and you can give them new instructions. Instead of listening to the North

Koreans, they can listen to the FBI, and the FBI will tell them to stop attacking people." And Julian Sanchez, who's been on this program, said, "Gee, those poor people. They were victimized by the North Koreans, and now they're being re-victimized by the FBI. It's just a shame." And the EFF [Electronic Frontier Foundation] flips out. I have trouble seeing any problem here. This is the result of the change in Rule 41 that the Obama Administration proposed, but it looks as though it's working exactly as we expected it to. David, did you look at this? Nick?

Nick Weaver: [00:36:07] Yes. And from my point of view, it's actually working too hard. So the FBI got permission to participate in the botnet, talk to the bots, and basically act like another node in the botnet and just collect basically passively information about how the botnet is structured. This is the kind of thing that researchers like us – and, in fact, colleagues have – done without making our lawyers blink twice. So this was a natural experiment done a few years back by some colleagues. They infiltrated one of these botnets, they participated in the peer-to-peer network, and then they rewrote the spam that was being sent so that it would have links to the researcher copy sites so that they could actually understand how well those spam bots actually work at getting people to respond. And this was work done with consultation with our lawyers, and our lawyers were good with it.

Stewart Baker: [00:37:14] Your IRB [Institutional Review Board] approved it, or did they not think that this was human subject research?

Nick Weaver: [00:37:20] Not human subjects.

Stewart Baker: [00:37:22] Okay.

Nick Weaver: [00:37:23] The FBI request didn't include what they could have justified. So just talking in the botnet doesn't actually touch the CFAA or anything else because you're actually just participating with the legit protocol. The bots are supposed to do that. The CFAA comes in if you want to, say, tell the botnet inject your own commands like, "Oh, shut down," and there was no request even to authorize that.

Stewart Baker: [00:37:58] Oh, I'm sorry. I thought they had done that. Oh, my God. This is so sad. Julian Sanchez is losing his sense of proportion here.

Nick Weaver: [00:38:06] Yes. This was literally the kind of thing researchers in computer security will do without causing our lawyers to blink twice. We'll still ask our lawyers, "Is this a good idea?" And they'll go, "Yes." And the other thing is just overall I don't think the civil libertarians appreciate just how much our civil liberties are protected by paperwork. If I had to do the paperwork for this, I'd just say, "Ah, screw it. Let the botnet go. Let the North Koreans have their fun." It's just a huge amount of pain for stuff that is just straightforward.

Stewart Baker: [00:38:47] Yeah. So the alternative would have been to go to every single federal district where there was a bot and get another court order aimed at the bots in that district. That's what the rules used to be before Rule 41 was changed.

Nick Weaver: [00:39:03] No, it's worse. The problem is you never could because this work was only really about finding out where the bots were. So if you need a warrant to talk in the botnet and find out where the bots were in every jurisdiction that may potentially have a bot, you couldn't do it all!

Stewart Baker: [00:39:25] You'll never be able to get there. Yeah, you can't get there from here. Alright. Well, thank you, EFF. Let's hope that your fundraising campaign on this issue completely fails. I want to say thanks to Matthew Heiman, David Kris, and especially to Nick Weaver for joining me on Episode 250 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson, because I'm going to read, as I promised I would, a recent review that was posted on Apple. And it was posted by HoyaSaxaSD, says: "I got a fever, and the only cure is more Weaver. Love the show. I’m a lawyer but not in tech or security law, but it’s still fascinating. My teenage sons also like most episodes, especially the Nick Weaver segments. And I concur. There needs to be Weaver in every episode, and more of him. In fact, an hour of Weaver and Baker debating/discussing

would be the perfect show." So as Peggy Lee once said, "Just give me Weaver / Give me Weaver."

Nick Weaver: [00:40:40] [Laughter]

Stewart Baker: [00:40:41] So, Nick, thank you. That's a great review. And thanks to HoyaSaxaSD. And let me say, I will read some of these others. We have a fair number of reviews on Apple, but if you are listening to this on an Android device through Google or Pocket Casts or Stitcher, there is only one review. It's about a year old, and it's sort of sad: "Baker has become a political pundit. Baker is becoming increasingly irrelevant as he works to defend every action that conspiracy pushers like Devin Nunes take. I thought *Skating on Stilts* was a good read" – thank you – "that provided an interesting perspective. But now he seems to have lost to partisanship." So if you agree with that, at least give me five stars –

David Kris: [00:41:31] [Laughter]

Stewart Baker: [00:41:33] But if you think that is not a representative criticism, and you're listening to this on Stitcher, now is the time. There's only that one review, so it would be nice to balance it out with another review that says you know that *Skating on Stilts* wasn't that good a read. So that's my pitch for the week. One more pitch: our friends at Third Way – you remember we've had Mieke Eoyang on here – and the *Journal of National Security Law & Policy* are looking for proposals for an upcoming Cyber Enforcement Symposium. If you've got a paper that you want to present and you are looking for a way to break into policy and pundit circles in Washington on cyber issues, this is a good place to start. So we'll put up a link to the CFP in the show notes so that you can send your proposals for appearing on the program to Mieke and her friends. Remember, if you send us a suggestion for an interview guest, we will send you one of our highly coveted Cyberlaw Podcast mugs. It's very selective. We don't always have a guest, as witnessed today, so you've got to meet our high standards. But I'm sure with our listening audience we can do that. Send 'em to CyberlawPodcast@Steptoe.com. I occasionally will give previews of what we're going to

discuss @StewartBaker on Twitter, so you can lobby for your favorite stories by liking those if you want to. We're gonna have some great guests coming up: Dmitri Alperovitch, who's always terrific, the CEO of CrowdStrike, will be coming on; Gordon Crovitz and Steve Brill, an unlikely pairing of liberals and conservatives from mainstream media, have started a company called NewsGuard, which is right in the middle of the Fake News fight, and while I'm both interested and skeptical about their proposal, it'll be fun to have a deep conversation about Fake News and protecting the *New York Times* from criticism; and Amy Zegart of Stanford's Hoover Institution will be coming on to talk about some of the cyberwar issues that she's been struggling with along with Herb Lin at the Stanford Hoover Institution. Our show credits go to Laurie Paul and Christie Jorge, our producers, Doug Pickett, our audio engineer, Michael Beaver, our intern. I'm Stewart Baker, host and provocateur. We hope you'll join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.