Episode 251: Executive Orders and alien abductions

Stewart Baker: [00:00:08] I feel as though this is more or less a cookie-cutter Executive Order. You could have the same Executive Order on alien abduction. Right? "We're gonna spend money. I'm not telling you how much, but the agencies will spend whatever they're spending. That'll be good. We're gonna do what we can, as long as it doesn't cost anything, to learn more about it. We're gonna talk to our international partners about alien abductions. We should encourage people to take up careers in alien abduction." There's no real new content here as far as I can see. I thought it was interesting that DoD has some very specific things they think AI is going to be really good for, and they aren't necessarily "killer robots." Stuff like that suggested they have actually spent a fair amount of time looking at AI as a tool for the institution.

Jessica "Zhanna" Malekos Smith: [00:01:04] I was doing my utmost to avoid the phrase "killer robots," but...

Stewart Baker: [00:01:11] [Laughter] Yeah, well, you know we're famous on this podcast for going there. So, yes, we went there right away.

Brian Egan: [00:01:18] [Laughter] We've already also gone to alien abduction, I will just note for the record on this topic.

Stewart Baker: [00:01:28] [Music] Welcome to Episode 251 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking technology, security, privacy, and government. And any resemblance between the statements made here and the views of our partners, our clients, our institutions is purely coincidental. Joining me for the News Roundup – and we're only gonna have a

News Roundup this time – is Brian Egan, who's a partner in our Washington office, formerly with the State Department and the National Security Council; Nate Jones, who's the co-founder of Culper Partners, formerly with the National Security Council's counterterrorism office, and along with David Kris, who's also a participant in our podcast, having been bitten by the podcast bug, he and David are producing a series – I think a limited series – of podcasts on how American government and the constitutional order work. Nate, can you give us the elevator pitch for your podcast?

Nate Jones: [00:02:39] Sure. Thanks for the opportunity to plug it, Stewart. So that's right. We're at a time when I think there's broad bipartisan concern about the rule of law and associated norms being trampled on or cast aside in some cases. We've wanted to pull together a group of experienced individuals from across the political spectrum and with different backgrounds in terms of experience in the private sector and across the public sector and hear from them about what the rule of law means to them, why it's important in the work that they did in government, in the private sector, and also to American security and prosperity more broadly. And so it will be a limited series, about 10 or 12 episodes at the end of the day. And, as I mentioned to you just before we kicked off, it's given me a newfound appreciation for the level of work you guys put into this, which is why it ended up being a limited series.

Stewart Baker: [00:03:42] [Laughter] No, if I had been smart enough to describe The Cyberlaw Podcast as a limited series, I would have spent another day in the Vermont mountains and probably would have broken something, because my advice to all of the listeners is when a nine-year-old who has a season pass to the mountain you're on says, "Follow me, Grandpa": don't. [Laughter] Okay. And our last participant is someone who – really I've never met somebody who had two completely different identities to assert. On the one hand, this could be Jennifer Smith that we're interviewing. And on the other hand, it could be the exotic Zhanna Malekos. So, Jennifer "Zhanna" Malekos Smith, what's the story behind your identity?

Jessica "Zhanna" Malekos Smith: [00:04:45] My goodness. Exotic? Thank you. It's a very humble origin actually. So going back to the history of Wellesley College's Russian

Department, which is founded by Vladimir Nabokov, Professor Thomas Hodge, who's the director there, he has a practice of assigning all students new Russian nicknames. So the Russian equivalent of my name, Jessica, would be Zhanna. So that's how I acquired that moniker. It's a fun Wellesley College Russian Department practice.

Stewart Baker: [00:05:17] Okay. Okay, I apologize. I think I called you Jennifer. So we are adding to the confusion of your secret identities. I like this. And Malekos Smith? I take it you sort of married into white bread?

Jessica "Zhanna" Malekos Smith: [00:05:32] Actually, Malekos is my mother's maiden name, and Smith's my father's. So combined.

Stewart Baker: [00:05:37] Okay, so she married into white bread. Alright. And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. So the issues I thought I'd start with are just what a beating Big Tech is taking from regulatory authorities around the country, around the world, and maybe give a very quick update on them. You may remember there was a Copyright Directive that the EU was pushing that was designed to ensure a much more aggressive enforcement of copyright law through upload filters so that people couldn't upload products that were violative of copyright and taxes on links so that if you did a new search and you got a one sentence description of a particular story in a European newspaper, Google would have to pay the newspaper to include that one sentence summary. Both of those were heavily contested. And, as in the way of European legislation, regulations, and directives, it was an endless process that seemed at one point to offer some restrictions on the dumbness of these policies. But nope. Given the choice between dumbness and sticking it to Big Tech, Europe has chosen dumbness. And so these provisions are going to survive the EU legislative gantlet. Similarly, the FTC is in negotiations and widely rumored to be proposing a multi-billion dollar fine on Facebook for violation of the previous consent decree that was entered into in 2011 or so. I find this really hard to understand because the consent decree enforcement law, the law there, is not that good. There've been some decisions in which the courts have said, "You're only in violation of the consent decree if the consent decree is written in a very airtight way, so we can say, 'Yeah, there is no doubt that this was a violation.'" I'm guessing that most of the things that Facebook did that were being charged as violations were close calls, arguable, and Facebook could probably spend years in court arguing over this rather than settling for multi-billion dollar claims. My guess is that Facebook just doesn't think they have any public support on any of this stuff. They have just been beaten up so badly that if they were to press this further, they'd only get more bad press. That is the only thing I can think of why they would be settling at that level of damage. And then finally, just to show that I don't always say the EU is wrong, the EU has come up with a set of rules that they are rolling out, competition rules, for platforms like Amazon selling third-party goods. All of the third-party good platforms are going to be regulated by the EU with a relatively light touch. They're going to say, "We want to see how you treat third-party sellers different from your own wares." This is a big issue with Amazon, which sells a lot of third-party stuff. And figuring out how to get that coveted top slot has produced, as we've talked about, some really aggressive tactics on the part of third-party sellers and a desperation to make Amazon happy with them. And having those rules spelled out a little more clearly probably does make sense. And I think the EU is going to come up with a few things that no one should do on a platform and from there let it play out, which is probably as good as you can get. Exploiting your platform-ness is something that Microsoft invented in the '90s, and it made them a very successful company. And all of Silicon Valley has been searching for the opportunity to be a platform where you can both get paid by people to provide services and watch the services they provide so that you can take over from them if they get too successful. And that remarkable position of being both a necessary service and a competitor is a license to print money, and the EU is probably right to get nervous about it. Okay. So that is the news from Europe, more or less. In the US, artificial intelligence is now so much of a buzzword that even DoD and even the White House have felt obliged to express views on it. Zhanna, I did not think we learned a lot from the White House Executive Order on artificial intelligence. Am I wrong?

Jessica "Zhanna" Malekos Smith: [00:11:37] Well, it's true that no financial amount was listed and how much the US government will now be funding AI research initiatives. However, in the *Hill* article, it reported that the current AI budget for the Pentagon for this fiscal year is about $90 million, and the Joint Artificial Intelligence Center director will be asking for an increase in the 2020 fiscal budget request. But putting the monetary considerations aside, I thought it interesting that this order has five principles, and in contrast the DoD 2018 Strategy Summary that was released the day after has four. But the Executive Order: (1) it mentions investing in artificial intelligence research and development; (2) it talks about transparency, providing certain federal data and models, making sure that they're more available to American research and development experts and AI researchers in this field; (3) it talks about setting governance standards, and specifically, it mentions the National Institute of Standards and Technology [NIST] pioneering the way here in leading the development of setting appropriate technical standards in this space; (4) discusses talent development, so cultivating that pool, building partnerships in academia, creating fellowships, training programs, really trying to grow that base and build a connection going forward. The fifth piece is engaging with international partners and protecting the American advantage in this sphere.

Stewart Baker: [00:13:29] So here's – and I'm going to ask Brian Egan to weigh in on this – I feel as though this is more or less a cookie-cutter Executive Order. You could have the same Executive Order on alien abduction. Right? "We're gonna spend money. I'm not telling you how much, but the agencies will spend whatever they're spending. That'll be good. We're gonna do what we can, as long as it doesn't cost anything, to learn more about it. We're gonna talk to our international partners about alien abductions. We should encourage people to take up careers in alien abduction." There's no real new content here as far as I can see. But, Brian, Zhanna, you think I'm wrong?

Brian Egan: [00:14:26] Well, I think this seems like part of a kind of a normal presidential playbook in how to address a big national security problem is, among other things, you would issue a presidential directive, which tries to organize your government in a way that would address the problem.

Stewart Baker: [00:14:42] Yeah, it sort of clears out the lanes. It says, "Oh, yeah. Oh, NIST, they've got that great document on alien abduction. We should [not?] name check that."

Brian Egan: [00:14:52] And in some cases, this document could be the Executive Order that's forever cited by the agencies who want to argue we should be doing more on AI. In other cases, it will be forgotten in a couple of months. It really depends on how much the folks in the interagency with the juice on this issue are behind this policy.

Stewart Baker: [00:15:08] So that's why I think that the DoD strategy is kind of more interesting because they've actually thought about how they would use AI. So, Zhanna, do you think there's more to this White House thing, or should we just jump right to DoD?

Jessica "Zhanna" Malekos Smith: [00:15:24] I agree with what Brian has said that this is a promising first step. You're laying that first brick in constructing a home. But I agree with you that there is much more to unpack in the DoD piece, so if you'd like to transition there, happy to.

Stewart Baker: [00:15:40] Yeah. So I thought it was interesting that DoD has some very specific things they think AI is going to be really good for, and they aren't necessarily "killer robots." They're things like, "We need to manage our logistics. We need to make sure that our planes are flying and are maintained in ways that prevent us from being surprised by maintenance failures that aren't ordinarily part of our checklist." Stuff like that suggested they have actually spent a fair amount of time looking at AI as a tool for the institution.

Jessica "Zhanna" Malekos Smith: [00:16:29] I agree. I'll begin first by saying I was doing my utmost to avoid the phrase "killer robots," but...

Stewart Baker: [00:16:39] [Laughter] Yeah, well, we're famous on this podcast for going there. So, yes, we went there right away.

Brian Egan: [00:16:47] [Laughter] We've already also gone to alien abduction, I will just note for the record on this topic.

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

Jessica "Zhanna" Malekos Smith: [00:16:52] But you're correct that the focus was not on autonomous weapons systems but talking about preventative maintenance applications for AI, possible humanitarian assistance and disaster relief, which was surprising to hear about how that could be applied in this sphere, but a very promising first step in highlighting that there is more to just the stereotype of, "Oh, it's DoD and AI. It must be 'killer robots.'" No. There are many more applications when it comes to the military relationship with this technology. In terms of the strategic focus areas, the Executive Order listed five. This one has four. There are some similarities, but some differences. And the chief difference I noticed was the last one discussing America leading the way in military ethics and AI safety.

Stewart Baker: [00:17:50] Yeah. So I always worry when DoD sort of says, "Oh, we're gonna out-lawyer everybody." It's not hard to out-lawyer people who don't care what the law is, and that's been our experience in fighting wars in the last 50 years. But a big chunk of what they're talking about here is a little more granular and a little less airy-fairy. Things like: how do we make sure that our autonomous weapons don't do things we didn't expect and start a war or dramatically change the nature of it without anybody having thought that was a good idea? And that is an interesting sub-problem and one that you don't have to express in legal terms. You can just say, "Let's not do something stupid."

Jessica "Zhanna" Malekos Smith: [00:18:44] True. And in the Congressional Research Service's new report on US ground forces, robotics, and autonomous systems, it had mentioned that Congress was just beginning to evaluate the issue of whether the Department of Defense should develop fully autonomous weapons systems for ground forces. I've been thinking, in my research at Duke Law School, before we can really address that question, shouldn't we also first discuss what the core operating principles are for the war fighter? By understanding the law of war – that's the legal lodestar here. But what about developing a warrior ethos specific to artificial intelligence that the human war fighter can take going forward? And the DoD summary report, it mentions that humans are essentially the center of this technology. So in playing with that idea and looking at what other reports that the different military branches have put out there concerning robotics and autonomous systems and the US Army's warrior ethos, I actually developed a[n] intelligent autonomy warrior ethos, some core principles to help the war fighter in this sphere because a warrior ethos is more than a code of conduct in war fighting. Broadly put, it's a way of life that applies to the soldier's personal and professional life as well. If you'd like, I'm happy to demo it for you. It's four lines.

Stewart Baker: [00:20:22] Okay.

Jessica "Zhanna" Malekos Smith: [00:20:22] It reads like a poem in a way. The US Army, for example, they have a warrior ethos that's about five lines. So if you have any military members in the audience, which I'm sure you do, they might recognize the parallels with this. So here goes: "I am the warrior in the design. Every decision to employ force begins with human judgment. I verify the autonomous weapons system's target selection before authorizing engagement, escalating to fully autonomous capabilities when necessary as a final resort. I will never forget my duty to responsibly operate these systems for the safety of my comrades and to uphold the law of war. For I am the warrior in the design."

Stewart Baker: [00:21:11] Alright. So whenever you tell me about the law of war in unusual circumstances, I think it's overdone. But because we have no idea what it means in many of these contexts and to the extent that we make it really clear and reduce it to a whole bunch of rules, they are rules that no one else will recognize, and I don't think the Chinese warrior ethos is going to have any reference to the law of war, although they may well recognize the idea that you shouldn't let these things get out of control, that you ought to know what targets you're attacking or setting these things loose at. But let me ask this: how is it that you can actually know what these things are doing when we've already seen artificial intelligence that is able to come up with actions, often clever and effective actions, that no one could have explained? No one knows how the machine developed those capabilities. It just ran enough simulations that it said, "Well, this seems to work every time, so I'll try that." And this is how IBM's Watson has managed to win Go against all the champions, as well as chess and Jeopardy. So how is it the warriors who are designing these things can actually take responsibility for what artificial intelligence is going to do?

Jessica "Zhanna" Malekos Smith: [00:22:46] So there are different categories of interface between the human and the machine. You may have heard it described as human-in-the-loop weapons, human-on-the-loop weapons, and human-out-of-the-loop. And the type that I was referring to would be – the warrior ethos concept is talking about human-out-of-the-loop weapons. So that's the fully autonomous weapons systems, in theory, would not depend on the human input to function. However, the Department of Defense's Autonomy Directive states that we will use AI in a human-centered manner. So there is still, even though this technology theoretically would be capable of operating without human input, once activated there is still a human operator at the core overseeing this. And there was another article in Verge that had said military commanders are leery of relinquishing control to a technology to make that decision to employ lethal force. And thus far, we've seen that DoD policies clearly reflect that there will always be a human in the equation and making the decision to employ lethal force.

Stewart Baker: [00:24:06] So that sounds like the sort of thing that the peacetime bureaucrats in the Pentagon say, and we don't know whether that's how it will work out until we're actually in a war and we see what's working and what's not – and, most of all, what is working against us. But we'll have to see.

Jessica "Zhanna" Malekos Smith: [00:24:24] The UN Group of Government[al] Experts meeting on this technology, the chair released a summary of the discussions, and this is on point to what you had said, Stewart, that disconnect. Surprisingly, the chair's comments had said, "Well, the law as it stands now is fine. We don't need to adjust it, but we should keep developing this technology." And it was strange to see in a way a green light saying go forward and then encouraging a type of lethargy in exploring how international law maps out onto this technology, both in a time of peace but also in times of conflict. So it's a[n] undeveloped area for sure, but it was interesting to see the UN Group of Government[al] Experts take that position.

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

Stewart Baker: [00:25:19] Yeah. The Russians, who are a big part of that discussion, have finally gotten around to something they've been talking about for a while. They're actually going to implement an Internet kill switch. They're going to cut themselves off from the global Internet and do all the routing inside Russia using their own technology. I thought that was an interesting experiment because it implies that they think that that's going to give them a military advantage. They'll be able to filter attacks and at the same time take advantage of the global Internet's architectural weaknesses to destroy their adversaries' (i.e., our) capabilities. And it does strike me that if nothing else, this experiment on the Russian part ought to ask us what would we do if they actually did disconnect and then attack our DNS system and the remainder of the global architecture for Internet communications. I don't think we've got an answer. Alright. Speaking of answers. Israel has apparently got an answer to a question they hadn't been planning to ask until DoD and the US government started leaning on them, which is: are you going to keep taking Chinese money for some of your military and AI capabilities? And the Israeli government is now looking at developing its own CFIUS [Committee on Foreign Investment in the United States] process, proving that CFIUS really is contagious. Brian, what do you think this actually is going to amount to?

Brian Egan: [00:27:10] Well, that's the thousand dollar question because, as you said, Stewart, Israel has been under a lot of pressure from the US government, including several high-profile visitors who publicly called them out for not doing more to screen foreign investments. So there was a [*Wall Street*] *Journal* article last week indicating that the prime minister's office is developing some sort of mechanism. Remains to be seen whether this will be Israel's equivalent of the AI Executive Order you talked about a few minutes ago or whether this will look more like a real interagency process with real authority to screen and potentially stop transactions that are problematic from a national security perspective.

Stewart Baker: [00:27:48] So FIRRMA [Foreign Investment Risk Review Modernization Act], the new US law, does have provision for more coordination with foreign governments that have similar processes. Does this open opportunities for Israel to get more information and to do more coordination?

Brian Egan: [00:28:07] Yeah, it does. So there are two advantages under FIRRMA, the CFIUS reform law, for countries that cooperate with the United States in forming their own foreign investment reviews. One is sharing of information, as you said, between the US and foreign governments becomes easier. Second is it's possible for companies from those foreign countries to take advantage of additional flexibility in the US CFIUS rules if they can show that their own government has a CFIUS process on the backend. FIRRMA writes in some additional exceptions that the US government could use to apply to those countries that have their own CFIUS processes.

Stewart Baker: [00:28:46] So my guess is then if you're the Israeli government, you want to develop a process that looks enough like CFIUS that CFIUS is comfortable using those authorities.

Brian Egan: [00:28:59] Yes, but you're balancing that against what has been a real surge in investments from China, in particular, and trying to figure out if you can kind of have your cake and eat it too, in a way, in this in this area.

Stewart Baker: [00:29:12] And that's always been DoD's worry with Israel is that they're closer to China than the US is in a big way on things like drones. And so it's possible this marks the beginning of forced choice between Chinese money and markets and US money and markets.

Brian Egan: [00:29:36] Yep, that's true.

Stewart Baker: [00:29:37] Okay. Alright. So speaking of forced choices and China, the Chinese government is offering a new service. The Ministry of Public Security is now going to pentest [penetration test] businesses in China, including, as far as I can tell, anybody connected to the Internet. Any Western companies can be pentested, which – and apparently without much by way of notice and consent, which is indistinguishable from hacking them to see whether they're hackable, and maybe to improve their security but also to see if they're up to things that are violations of Chinese law. It's a remarkable step beyond what the Japanese did. The Japanese were saying, "Maybe we'll try out a few default passwords on peoples' Internet of Things to see whether they're part of a denial of service attack," and the Chinese have said, "Why don't we just see if we can get into the systems and see whether they're doing anything that we don't like from a security or otherwise purpose point of view?" And this is a new authority, relatively new. There's a report out by Recorded Future that talks about it. But I think if I had to say what's the lesson here, it's that the idea of governments getting more intrusive in the private sector is certainly one that China has picked up with enthusiasm, and it may be a worry for people – the Western companies who are still doing business in China. The Iranians are – their tradecraft is always surprising. They actually managed to convert a former military officer to provide targets for a bunch of hacks, people who are still in the US government and still working on classified programs. And the US government has kind of come down on that whole operation in a pretty serious way. Brian, what's the story here?

Brian Egan: [00:31:49] So last week Treasury and the Justice Department jointly announced sanctions and an indictment that relate to a woman named Monica Witt, who was with the Air Force counterintelligence office, who publicly attended a conference – this has been in the press before – organized by a group called New Horizons – Hollywoodism – which has been derided by the Anti-Defamation League and others as just antisemitic. She converted. She defected from the United States. She moved to Iran, and she's now accused by the Justice Department of espionage. She's accused by *The Daily Beast* of being "Iran's dumbest spy" because her tradecraft was so obvious and well-known to the US government, they've been tracking this for years. This culminated in an indictment of Ms. Witt and a couple of Iranians last week and sanctions by OFAC [Office of Foreign Assets Control] against this New Horizons organization and several individuals associated with that effort.

Stewart Baker: [00:32:50] So Iranian tradecraft continues to surprise, but maybe not in a good way.

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

Brian Egan: [00:32:56] [Laughter] I mean in a way the accusations are pretty serious that she disclosed a compartmentalized DoD intelligence program. She turned over the identities of some of her former colleagues, who were then subject of attacks from Iran. But in the other, it's not clear how effective any of this actually was when the Iranians got the information.

Stewart Baker: [00:33:17] Okay. So it also reflects the relatively coordinated indictments, sanctions from Treasury, attacks on espionage, cyberespionage, and other forms of espionage that we don't like. But of course, it was easy to go after Iran because we're going after Iran on everything else anyway.

Brian Egan: [00:33:35] That's right.

Stewart Baker: [00:33:37] Okay. Nate, the EU is using sanctions – or threatening to use sanctions, as well – in a slightly different context. What's going on there?

Nate Jones: [00:33:45] Yeah, so the EU is in the process of developing a plan to utilize, as you said, sanctions to try to deter malicious cyberattacks on the EU. Some of the language is reportedly explicitly focused on election-related hacks. And I think, on the one hand, this is obviously somewhat encouraging as we see the EU steeling itself and getting ready to try to fight back against these types of attacks on its infrastructure and its elections. We still have this ever elusive question about what level of harm must be inflicted by the hacker before the deployment of these kinds of tools are appropriate. We've never really been able to get agreement on that important question internationally. It sounds like the Europeans may be coalescing around a single approach on that question. The reports are it's a pretty low bar. It would potentially include mere intrusions into IT systems or even attempts to intrude into IT systems. But the million dollar question ultimately is going to be when and how effectively do they actually deploy these things once this new system is in place and how well are they going to stick together and work with others to impose these kinds of consequences in an effort to change behavior. And that is the thousand dollar question, as Brian said, on this issue, I think.

Stewart Baker: [00:35:32] Yeah. So they're worried about the European Parliament elections. Probably most afraid that people won't notice that there are elections. But –

Nate Jones: [00:35:43] You always have to get a jab in at the EU.

Stewart Baker: [00:35:48] [Laughter] I can't help it. It's true. But it is also true that people in Europe tend to treat the elections to the European Parliament as an opportunity to protest whatever it is they're protesting. There has been relatively little consolidation of parties around European platforms that would actually make a difference. As witness, I think, the link tax and the Copyright Directive and the filtering, all of which are probably bad for consumers but which the European Parliament isn't going to do anything about after whining about it. So they've made a lot of noise and not much else. But it is an opportunity for Europe to say, "We're gonna get tough if somebody tries to interfere with these elections." And maybe they do have something to worry about as enthusiasm for the European project wanes even in the core countries. You could see a concerted effort on the part of parties that really dislike the EU to capture a majority and then take action against the kinds of things that the European Commission is trying to do. I'm skeptical, but that could happen. And obviously, if you're a European Commission grandee, you worry about that. Alright. I love this story. William Webster is 94 years old. He was the head of the FBI. He was the head of the CIA. He continues – I see him pretty regularly because he's chair of the Homeland Security Advisory Council. A remarkable man with a remarkable history, to which really he's added to the legend of this-is-not-a-guy-you-screw-with. Nate, tell us this story.

Nate Jones: [00:37:49] Yeah. So there are 31 different flavors of these kinds of fraud scams, either email or phone call-based scams, that are being directed at people around the world. And despite it being pretty commonly known, it is a still somewhat effective business for scamsters around the world. It's a fairly large industry by dollar amount, but it's a volume business. So you have to call a lot of people and to get a small handful to fork over some money. In this case, this Jamaican gentleman, who was out looking for money using a pretty common scam that's been used before – it's often referred to as an advance fees fraud scam – he made the mistake of calling, as you said, William Webster, the former FBI director and CIA director. And even at 94, he recognized the fraud, reported it. They had a number of conversations over a period of time, it sounds like. And if that wasn't a big enough mistake, the poor Jamaican gentleman made another mistake by traveling to the United States voluntarily after he'd been indicted.

Stewart Baker: [00:39:13] I'm sure he didn't know he'd been indicted. [Laughter]

Nate Jones: [00:39:17] No, that's true. I assume he did not know that, but it was a mistake nonetheless where he was promptly arrested and charged in relation with that attempted fraud. Pled guilty, and upon serving his time, he'll be promptly deported back to Jamaica.

Stewart Baker: [00:39:34] So here's my question – and I didn't see this in the story or maybe I didn't notice it, but – it occurs to me that at 94, Judge Webster may be in the generation that still answers their landline phone. Was this a scam where he was randomly calling people's landlines?

Nate Jones: [00:39:56] It sounds like it. Yeah.

Brian Egan: [00:40:01] [Laughter] That's what my kids say now. When the phone rings in our house, they say, "Don't answer it, Dad." [Laughter]

Stewart Baker: [00:40:05] [Laughter] Yeah. Exactly.

Brian Egan: [00:40:06] "Why do we have this thing? Just don't answer it, Dad!"

Stewart Baker: [00:40:13] [Laughter] Well, obviously we're all glad that Judge Webster did answer the phone and came down on this guy. It's very exciting. Alright. That wraps up our Episode 251. Thanks to Brian Egan. Thanks to Nate Jones. Thanks to Jessica "Zhanna" Malekos Smith. This has been Episode 251 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Remember: if you get a chance to check out Nate and David's Rule of Law podcast series, the first episode is now up on the Lawfare podcast. And in additional public service announcements, our friends at Third Way and the *Journal of National Security Law & Policy* are looking for proposals for their upcoming Cyber Enforcement Symposium. So if you've got ideas about things you'd like to write about in that area, this is a great opportunity to get published. If you send us an interview guest suggestion and we bring them on the show, we will send you our highly coveted Cyberlaw Podcast mug. I'm looking forward to getting more of those suggestions. Send them to CyberlawPodcast@steptoe.com. When I'm not trying to follow nine-year-olds down cliffs that I should not be on, I am tweeting the suggestions for the next podcast. So if you follow me on @StewartBaker, you'll probably see some of those suggestions, and you can comment if you think I should or shouldn't cover them. Please do rate our show, especially on Stitcher, where we only have one rating and it was grumpy and mean. So if you think it wasn't fair, please leave your own. Coming up, guests we're gonna have: Dmitri Alperovitch from CrowdStrike is gonna be talking about their new report; Gordon Crovitz and Steve Brill, an unlikely ideological pairing, have gotten together to create NewsGuard, which is an effort to rate the media sources that are getting online. We'll be talking to them. I'm a mild skeptic on this. Elsa Kania, who has been on before, from the Center for a New American Security, will come on and talk about her most recent research. Amy Zegart of Stanford's Hoover Institution will be coming on shortly. And Adam Segal of the Council on Foreign Relations. He knows a lot about what's happening in China. It'll be fun to talk to him. Our show credits: Laurie Paul and Christie Jorge are the producers; Doug Pickett's our audio engineer; Michael Beaver is the intern who has brought order to our program and is the only reason that Nate Jones thinks that we're better organized than he is; and I'm Stewart Baker, your host. Please join us again next time as we once again provide insights on the latest events in technology, security, privacy, and government.