Steptoe

Episode 239: The Ministry of Silly Talk

Stewart Baker: [00:00:04] Welcome to Episode 239 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking technology, security, privacy, and government. Today I'm joined for the News Roundup by Dr. Megan Reiss, senior national security fellow at the R Street Institute, senior editor at Lawfare, and a fellow at the National Security Institute. Megan, welcome.

Dr. Megan Reiss: [00:00:26] Thank you.

Stewart Baker: [00:00:27] And also on the phone, two graduates of the National Security Division at DOJ: David Kris, who used to run it, and Nate Jones, who worked there, then went to Microsoft, went to the National Security Council. And both of them now at Culper Partners. David, Nate, welcome.

David Kris: [00:00:51] Thank you.

Nate Jones: [00:00:51] Thank you, Stewart.

Stewart Baker: [00:00:52] And I'm Stewart Baker, your host for today, formerly with NSA and DHS and maybe still the only person who's had policy jobs at both those places. I once described myself as the child of a broken marriage. So why don't we start with a victory lap? We all – not everybody here, but David and I at least, maybe Nate – said last week we did not expect the Russians or anybody else to successfully hack the electoral process. It looks as though there may have been a lot of stuff that happened, but hacking does not appear to have been part of it. So David, congratulations.

David Kris: [00:01:40] Yeah. It looks that way, although as you say, we have enough complexity just on our own to make it interesting for an extended period of time.

Stewart Baker: [00:01:49] Yes, well, we'll be fighting about Florida at least for a long time. And that's deja vu all over again. And the Internet Research Agency is looking kind of sad trolling Americans saying, "See, you just can't trust your elections, can you?" As though they had done something. So history there is repeating itself as farce. So I want to start with a story that really is only the bits and pieces of it have emerged, and maybe there's no story here. But I am struck by the fact that the Justice Department has faced FISA challenges to evidence in the Chinese case involving heads of state in Africa, allegations of bribery, and then Bob Mueller has tossed the Concord Management Company into the trolling criminal case and Concord is clearly demonstrating an enthusiasm for litigating everything. They can keep showing up. They don't have to worry that they're going to go to jail automatically. And so there's been quite a bit of activity with respect to FISA, and I'm wondering whether FISA is going to have difficulty surviving the challenges that Bob Mueller and the National Security Division are inviting. David, am I wrong to think that there's a problem here?

David Kris: [00:03:32] Well, I don't think it's as severe a problem necessarily as you do. So the first case is one brought by NSD [National Security Division] and the Southern District of New York in which some Chinese officials or Chinese persons are charged with a scheme to bribe the president of Chad and the foreign minister of Uganda in order to secure contracts to drill for oil. This is a sort of a regular order of Foreign Corrupt Practices Act case in the continent of Africa with fake charities set up to funnel the bribes which is a fairly conventional tactic these days. And unsurprisingly perhaps, there is FISA coverage I guess on these foreign leaders and officials that comes into play. And Loretta Preska, the judge, has denied a suppression motion brought by the defendants following the unbroken tradition of doing so. And she's also refused to give them disclosure of the FISA applications. So that feels pretty routine. There was one case in which a district judge did order disclosure of FISA, and the Seventh Circuit promptly slapped that down in an opinion by Judge Posner as I recall. You know the funny thing today is whether that unbroken record will continue even after the shenanigans with the Carter Page FISA which obviously involved the first time that a FISA application or any part thereof ever saw the light of day. Apparently Judge Preska was not impressed by that as a sort of busting the dam and allowing for more exposure.

So she's hewed to the traditional line. In Concord Management it's a little less clear exactly what's going on. But I agree with you. Concord is going to pursue a standard aggressive sort of graymail style posture among other things that it can do. But I'm pretty sure that Bob Mueller and the Southern District of New York and NSD have gone through the usual equities process here to balance what can be used and what can't be used and what can be protected by SIPA or FISA or any of the other statutory mechanisms. I suspect it will ultimately shake out as business as usual.

Stewart Baker: [00:05:51] So he's handed it off to the Southern District, but that's after he actually announced the indictment. Is that right?

David Kris: [00:05:59] No, I think Concord Management is still being handled by him.

Stewart Baker: [00:06:06] Okay. It's the other case that's the Southern District. Okay. So I'm a little troubled because I've been on the other side of this issue from an intelligence equity point of view. And it's always been my perception that at the end of the day the Justice Department is restrained from bringing these cases even if they expose intelligence equities only by a sort of interagency process in which eventually you could get to the president. But of course if somebody doesn't think that Bob Mueller should be putting intelligence equities at risk, they don't get to go to the president. Doesn't the decision rest with Bob Mueller at the end of the day?

David Kris: [00:06:49] You know it is a very interesting question what would happen if it worked its way all the way up because of course my experience on the DOJ side of this was always that you know if the intelligence community really puts its foot down and throws a temper tantrum, the prosecutors back off and don't use the disputed take. But you're right. It does escalate up the chain. It would be you know ultimately through I guess Matt Whitaker now. That would be fun. I'm sure he's a real expert on FISA equities.

Stewart Baker: [00:07:25] And then on to John Bolton, right?

David Kris: [00:07:27] I think on to John Bolton. And frankly that is probably where it would come to rest because for either the traditional DOJ folks, who would be pushing this, or for the traditional Intelligence Community folks, who would be pushing the other direction, I'm not sure either one of them would want to try to escalate this to the president. It's certainly in Concord Management case just because probably the president, if he were rational, would say, "I should recuse myself and not weigh in on the equities in a case in which I am a subject of the investigation," but this president probably wouldn't do so. And I'm not sure that the traditionalists at either DOJ or an intelligence agency would ever want to have that possibility presented.

Stewart Baker: [00:08:15] [Laughter] So it's working.

David Kris: [00:08:18] You know the price of escalation is always high if you lose. But the price of escalation here would be exquisitely high and would I guess – to put it in the terms that Trump might put it – you know might threaten the long-term equities of the "Deep State." And so I suspect each side would probably live with whatever Bolton decided.

Stewart Baker: [00:08:39] Alright. Lots of China news this week. Megan, give us a feel for where all of the China stories are going.

Dr. Megan Reiss: [00:08:50] So apparently China surveils its citizens.

Stewart Baker: [00:08:53] Oh no!

Dr. Megan Reiss: [00:08:56] It's new, groundbreaking news. Yeah.

Stewart Baker: [00:08:59] It turns out that that's also an exportable industry.

Dr. Megan Reiss: [00:09:05] Yeah, from the US even. But exporting it in their particular surveillance goals to countries along the Belt Road.

Stewart Baker: [00:09:16] It's not really a surprise.

Dr. Megan Reiss: [00:09:20] Not a surprise at all.

Stewart Baker: [00:09:20] If you're a third-world dictator and you've got a choice of buying sort of a package of communications technology that comes with sort of freedom enabled and one that comes without, you're going to take the second, aren't you?

Dr. Megan Reiss: [00:09:35] Or more than that if you're considering a deal from the Americans who say, "We'll give you fairly cheap technology, but you have to reform some of your human rights practices," or you go to China and they say, "We'll give you even cheaper technology, but by the way here's a package that will help you surveil your citizens even better and potentially jail them," which are you going to choose?

Stewart Baker: [00:10:01] So this is no surprise, but we're starting to see stories that detail how that's happening and how enthusiastically people are responding.

Dr. Megan Reiss: [00:10:11] It's what people have been expecting, and it's been associated with all these contracts that we're seeing on the Belt Road that are helping these governments inch closer and closer to China as we kind of let this happen. So the particular story that you highlighted for us this week is that China is getting better and better at surveilling gaits. So people walking.

Stewart Baker: [00:10:34] How people walk?

Dr. Megan Reiss: [00:10:34] Yes. They're basically saying they have 94% accuracy now to be able to identify an individual with no facial recognition going on simply by how they walk. And not only is it how they walk, if they try to deliberately change their gait, if they try to limp for instance, they'd still be able to detect those individuals. And the US has tried to get in on this technology before in the early 2000s in order to catch terrorists. Didn't get as far.

Stewart Baker: [00:11:08] No, that was the TIA, the Total Information Awareness program, and Congress killed it. And I remember this one because I was following it pretty closely, and the ACLU and the EFF and folks like that went to Congress and they made fun of gait recognition, calling it, "This must be the Ministry of Silly Walks from Monty Python" –

Dr. Megan Reiss: [00:11:34] [Laughter]

Stewart Baker: [00:11:36] And managed to kill US research on that and guarantee the market for the Chinese.

Dr. Megan Reiss: [00:11:45] Yeah, well apparently when the US was doing it, they were hoping that they'd be able to detect – or they actually developed the ability to detect – someone who is holding an explosive under their jacket, for instance. Well, the Chinese are already saying they want to use it to catch jaywalkers, and I'm sure contribute to the Social Credit Score and all the uncomfortable technology that is popping up recently.

Stewart Baker: [00:12:08] The one other story that I thought was really interesting is the Australians. The Australian Strategic Policy Institute had a report out on how the PLA [People's Liberation Army] is getting access to all this technology. David, did you look at that?

David Kris: [00:12:22] I did. It's another news flash: The People's Liberation Army are going abroad to study at Five Eyes universities, heavily focused on Australia which is obviously geographically very close. The Chinese call it "picking flowers abroad to make honey in China." That is a very colorful description.

Dr. Megan Reiss: [00:12:45] [Laughter]

David Kris: [00:12:46] And you know apparently it happens a lot. And the trend is increasing. There have been about 2,500 PLA officers sent abroad over the last

decade. This report says most of them have come openly but some have been more clandestine, trying to hide their affiliation. You know obviously the Chinese are very explicit in undertaking this effort, and they also try to steal technology other ways. The report basically says that universities in Australia need to get into a better partnership with the Australian government to deal with the counterintelligence concerns that are created by these PLA officers doing joint research with Australian scientists. You know in the US of course, you can't get approval to have foreign military officers participate in classified research that gets conducted at university level, but I think the question here is you know are the borders there a little fuzzier than we might like and are the scientists who may be working in part on classified research and in part on unclassified research potentially targets of recruitment if they are you know bumping up against Chinese military or intelligence officers. And I think that to some degree is a legitimate concern. I'm not terribly optimistic that Australian or American universities are going to welcome a much more intimate partnership with governments to deal with these counterintelligence concerns. But the report is interesting in just documenting some of the trends here anyway.

Stewart Baker: [00:14:23] No, I think the universities of course are going to be upset at anything that looks like it might constrain their revenue flow from tuition and grants, and then they'll invoke academic freedom as part of their effort to keep that flowing.

Dr. Megan Reiss: [00:14:44] This just reminds me so much of the AQ Khan story from back in Pakistan, that he learned how to start the nuclear program while working abroad in laboratories. Just learn from history on this.

Stewart Baker: [00:14:58] Yeah, my guess is not going to happen.

Dr. Megan Reiss: [00:15:03] I agree.

Stewart Baker: [00:15:03] But I have to say it's really interesting that the Australians are having the debate that we really haven't had. This is the most important political debate or just about in Australia: The question of what's their relationship with China;

what are they going to allow the Chinese to do; what kind of equipment are they going to buy from China. There is nothing we are debating that they have not debated at higher volume and with more detail.

Dr. Megan Reiss: [00:15:29] Sounds like a good podcast, I think.

Stewart Baker: [00:15:32] Yes! Alright. We'll bring the Aussies up and ask them what we should be doing. And I'm sure they'll have plenty of advice. I've never met an Aussie who wasn't pretty free with his advice. Okay. Chapter 212 in the story of Silicon Valley versus conservatives. Facebook and broadcast media actually just said, "You know that ad that Donald Trump wants to run? We will not run it." The implication is they think it's racist or shocking or abusive. I listened to it. It's got an illegal immigrant saying about a couple of police he killed, "Well my only mistake was not killing more of the (unprintable) folks." And then the Trump campaign saying Democrats will be complicit in all the murders committed by illegal immigrants. You know that sounds like hard-nosed political rhetoric. I'm not sure I quite understand why that's being taken down by either social media or kind of remarkably even by Fox TV. Nate, you got any thoughts on that? Am I just misreading this? Having seen Willie Horton ads in my lifetime, am I just inured to improper campaigning?

Nate Jones: [00:17:00] Maybe. I'll take the opposite position. I mean I think it was a pretty... I guess two things: One is it was pretty clearly, by bringing up the caravan, a manufactured issue at the last minute to try to tip the election in the Republicans' favor. And it did say it, at least in my opinion, in a pretty inflammatory and arguably racist way. And I think you know these social media outlets have developed community standards. Those things do admittedly evolve over time as new challenges or new issues crop up, but they need to enforce them evenhandedly. And you know I think it's hard to tell if this was an issue of sort of like comfort in numbers where they all sort of decided to move at once. It seemed not. I mean there were some holdouts. I think NBC and Fox were the last ones to pull it off of television and refused to broadcast it, but I think the broad support for taking this thing down is also a pretty good indication I think when you

include Fox that this was not a politically motivated step on the part of these media companies.

Stewart Baker: [00:18:14] Alright. Well I'm not sure that arguably racist, given that pretty much the entire Republican Party is arguably racist in the view of at least 10% of the country, is the right standard. But I must acknowledge that if even Fox is taking it down, it obviously hit a nerve that evidently has been surgically removed from my body. Gab is back. What's interesting here is we're starting to see Gab as the service that essentially substitutes for Twitter for people on the right who are afraid they'll be de-platformed by Twitter and which had the anti-Semitic postings of the guy who killed those people at the synagogue in Pittsburgh. And in a frenzy of revulsion at that, companies started pulling any support that would allow Gab to stay on the air or on the Internet. But a couple of institutions have stepped forward to allow them to stay up for now. Kind of skin of the teeth though, right?

Nate Jones: [00:19:29] Yeah. They don't have many friends left in the tech industry. And so a few more missteps on their part may be the straw that breaks the camel's back. But you know again I think to the extent that these companies have public and clear policies on what's permitted on their platforms and seek to enforce those things evenhandedly, there's no surprise that the people who are on the wrong end of that at the end of the day are going to be upset about it. And particularly high-profile conservatives with a platform to speak on this from you know the folks at Gab to the Trump campaign to Alex Jones are going to be vocal about their opposition and their claims of potential bias. And they have a lot of backers even in Congress. You saw this with the Zuckerberg hearings where you know a lot of the people on the right were asking him questions about political bias rather than election interference and Russia's use of social media.

Stewart Baker: [00:20:34] Well, I don't think there is any doubt there's bias in Silicon Valley on this stuff. And it's driven in part by fear of their own employees. You saw the Google walkout. The employees, the engineers are a scarce resource, and if they fall out of love with the company and 20% of them leave, that company loses its future. So

they are really afraid to do anything that gets out of line with the values of their employees, and their employees are remarkably enthusiastic about shutting down speech that they don't approve of, which is pretty much anything that Donald Trump might say is something that most of Silicon Valley thinks is arguably racist and should have been suppressed more effectively in the campaign. Yeah. And you can see that in this LinkedIn campaign. There's an article in which BuzzFeed goes after LinkedIn saying, "Oh, there's a lot of hate on LinkedIn, too. You know LinkedIn doesn't seem to be doing enough." Which is kind of targeting for social justice warrior mobbing of LinkedIn saying, "How come you aren't doing more to shut these guys up?"

Nate Jones: [00:22:00] Yeah, I mean LinkedIn is you know a platform where this kind of activity really hasn't been seen before. My guess is they were caught a little bit by surprise and are now seemingly trying to catch up to where the rest of the industry has been. I guess I would take issue a little bit with the claim that there's bias in the industry. I think they clearly, as you said, have been significantly influenced by their employees. Their employees admittedly do tend to trend left. But I think the big question that's important is how it manifests itself. And it has driven some companies, as we've talked about before in the context of Project Maven, away from Defense Department contracts. It's created fissures between them and governments over the issue of surveillance. But despite all of the conservative complaining – and this is again not new. They've been complaining about mainstream media bias against conservatives for a long time. And this to me is a standard conservative play where you try to set up your own platforms that will carry your message and you attack everybody else for being biased against you. And the thing that we've seen is there's actually no evidence to date that there is actually bias or controlling free speech, and you know the efforts by the Valley to protect free speech, even views that are quite unpopular in the case of terrorism for example where they held out for a long time and received quite a bit of pressure largely from Republicans to restrict that type of speech on their platforms. And there's actually very little evidence of bias. But what we've seen at the same time is the absence of evidence doesn't really matter. There was a poll out this summer that showed I think 72% of Americans believe that there is bias in social media.

Stewart Baker: [00:24:00] That might be evidence. [Laughter] And look, Louis Farrakhan is a notorious hater of Jews. He still has that coveted blue check, whereas the Proud Boys of Oregon have all been defenestrated by Twitter apparently because they got into a fight with some Antifa people. And Twitter apparently knows better than anybody that the fight was started by Proud Boys rather than Antifa. I'm not quite as confident of that. And I'm not sure that getting in a fight offline means that you have to be kicked off of Twitter, especially since Louis Farrakhan is still on there you know peddling his hate.

Nate Jones: [00:24:47] Blue check. I think the Farrakhan example is a good point. I agree with you on that. It's unclear to me though that that's clear evidence of bias, and this sort of takes us to our final story about Alex Jones being kicked off and still yet finding a way to propagate his videos on the platform. And I think some of these things are evidence of just how difficult it is to enforce these rules even when you establish them, you make them clear, and you put an effort into being evenhanded and unbiased in your enforcement. There's a bit of a game of Whack-a-Mole, particularly where people have a large following and have supporters on the platform willing to share their stuff. It becomes really hard to manage and actually kick people off.

Stewart Baker: [00:25:37] So a censor's life is a hard one. Okay. So Iran is kind of in the news in a couple of ways that make me think that we are taking our eye off the ball, the most likely next attack. They've been complaining that they've had a serious cyberattack, and they're blaming Israel. And there's also evidence that the US banks are getting ready to defend against an attack from Iran. Megan, how seriously should we take these accusations?

Dr. Megan Reiss: [00:26:18] Well, the accusations are really interesting. So Iran is claiming that Israel has been attacking its telecommunications infrastructure through a Stuxnet-like attack, and they're giving almost no evidence. They're not really explaining what they're claiming it was. It doesn't really [comport] with what Israel's been doing as far as why would they choose this as compared to a defense system, something that was more obvious. And so there's just a lot up in the air, and they didn't do a very good

job of making the case for attribution or even that this was happening to begin with. And so it just makes you wonder. I'm not saying it didn't happen. I'm not saying there's not something there, but it makes you wonder what the bigger moves here really is.

Stewart Baker: [00:27:11] So one possibility is they're getting ready for an attack, and they want to have a justification for it.

Dr. Megan Reiss: [00:27:14] It's possible.

Stewart Baker: [00:27:15] And US banks apparently are afraid and must have some intelligence to suggest there's an attack coming there too.

Dr. Megan Reiss: [00:27:21] Or broader just undermine Israel at every point.

Stewart Baker: [00:27:24] Yes. Well, they could be coming after us too. They have in the past.

Dr. Megan Reiss: [00:27:28] Oh, yes. Oh, we should definitely expect them to continue doing that as well.

Stewart Baker: [00:27:32] Okay. The Dutch police have broken IronChat, which is another one of these really expensive, you-have-to-be-a-drug-dealer-to-afford-it communications security apps. And they advertised on their website that they were endorsed by Edward Snowden. Nate, how is that working out for them?

Nate Jones: [00:27:56] Something we agree on, Stewart. We finally found it. Not too well. It's not working out too well for IronChat, and it's not working out too well for Mr. Edward Snowden. A couple things I think are interesting here. One is you know the underlying fact that the Dutch police have managed to break into these IronChat messages somehow is the flip side of the encryption debate a little bit. You know people have been advocating for strong encryption have largely been saying you know let the governments find their own way. And you know we've seen both in the San Bernardino

case with the FBI and now with IronChat that governments do have some ability to get into these things when they really work at it. They'll argue it's inefficient and ultimately ineffective, but it lends a little bit of credence to that side of the debate. Now as far as Mr. Snowden, you've tweeted about him and I'll let you talk about that if you'd like. But I think the thing that he continues to show is how easily manipulated he is. He's sort of Trumpian in both his overestimation of his knowledge and his underestimation of his lack of experience and context for some of these things. And you know he went out and apparently endorsed this thing. And you know apparently it's not just the Russians but private companies that can dupe him into doing their bidding.

Stewart Baker: [00:29:32] Well, to be fair... I did tweet at him. I said, "How much did they pay you for that endorsement?" And he did not respond to me, even though I know he reads my stuff because he occasionally when he finds something he thinks will be embarrassing, he retweets it from my Twitter feed. But in this case, he had his lawyer from the ACLU, Ben Wizner, say that Mr. Snowden has no connection to IronChat, not familiar with them, and did not endorse their product. Though it would have been fun if he had. It would have been a delicious irony. He is now saying that he didn't do it. But either way if you buy a product based on Edward Snowden's endorsement, probably means either that somebody is lying or that Edward Snowden doesn't know what he's talking about. In either case, you're probably not well served by spending extra money for that kind of security.

Nate Jones: [00:30:38] Trust but verify.

Stewart Baker: [00:30:38] Yeah, exactly. Or maybe just don't even trust. The Pakistanis, they're in the last stages. I think after bargaining comes surrender. They've just announced that all of their banks or practically all of their banks have been hacked. That is pretty scary. It indicates we've got a long way to go on cybersecurity, and as bad as it is here, it's even worse in Pakistan. David?

David Kris: [00:31:10] No, I was just going to say I mean they first said almost all of the banks, then they said most of the banks. A lot of money has been stolen. They're

looking at more than 100 cases. And apparently the data of 8,000 account holders is for sale on the Internet black market. So this is not a good thing. I don't give investment advice, but I would recommend putting your money in a Swiss bank rather than a Pakistani bank right now if you want to keep a hold of it.

Stewart Baker: [00:31:39] Yeah, and the Pakistanis probably... One suspects that they're selling nuclear technology to the North Koreans and the North Koreans are repaying the favor by stealing the money that they're paying for it from Pakistani banks.

David Kris: [00:31:55] [Laughter]

Stewart Baker: [00:31:55] That would at least be a certain form of justice. Okay. Thanks to all of you. We're going to turn to our interview now. It's a panel discussion. It's long. So you've got another hour and 15 minutes if you're listening to this, so you know this is the time to bail if you're going to bail. It's a discussion at the ABA's Standing Committee on Law and National Security in which we managed to persuade Tom Feddo, who's the current deputy assistant secretary in charge of CFIUS [Committee on Foreign Investment in the United States], Aimen Mir, who's the former deputy assistant secretary in charge of CFIUS, Sanchi Jayaram, who is head of the CFIUS and Team Telecom unit at the Justice Department's National Security Division, and David Fagan, who's a longtime practitioner in CFIUS. Managed to persuade them all to come together and unpack what turns out to be a remarkably innovative new law on US investment policy. So without further ado I'm going to jump in and see if we can get a conversation going about this topic. Foreign investment's been an issue, Tom, for Americans really since the '70s. We go through periods when we're worried about foreign investment, usually different foreigners each time. And we've come up with a variety of ways of addressing the concerns that we have, and there's been a new law every time we've had a wave of these concerns. Can you give us a sense of the history of CFIUS and the requirements of the statute?

Tom Feddo: [00:33:51] I'll certainly try. Thank you very much for having me. I'm actually the new kid on the block, so others may have to fill in in some areas. CFIUS, as

many are aware, is chaired by the Secretary of the Treasury, and it's composed of 11 federal government departments and offices, nine of whom have a voting stake in CFIUS's process. And we can talk a little bit about that later on. And historically CFIUS has been directed at mergers, acquisitions, and takeovers in which a foreign person could gain control of a US business. And CFIUS's role obviously is to identify national security risks with those types of investments. Of course it's important to say the United States places a great deal of value on foreign investment. And just to set the context, I'll note that in 2016 it was valued at somewhere around $7.5 trillion in foreign investment in the United States. Foreign firms obviously offer new ideas and fresh technologies, and that investment is important both to the US economy and the global economy. But not all foreign investment, we know, is benign, and actually the history of dealing with non-benign foreign investment precedes the 1970s and goes back to World War I. In fact on the eve of our entry into World War I, Congress passed a law giving the president broad power to block investments in the United States related to wartime. In the 1950s and 1960s investment... There's also a really interesting story that you can look up about the Germans creating a front company in the United States to buy up ammunition and shells to distract the United States from producing its own ammunition, and the plans were discovered on a New York City subway. So there has been this issue of non-benign investment dating significantly back in the history of the United States. 1950s and 1960s: That foreign investment decreased. But in the 1970s with the oil crisis and OPEC, President Ford issued an executive order creating CFIUS to monitor and report on foreign investments, but there was no power to stop or block those threats. In 1988 there was the Exon-Florio amendment and the president could now block the foreign acquisition of a US company or order divestment where the transaction posed a threat to national security.

Stewart Baker: [00:36:50] So far we've got oil money as worry one. In '88 is Japanese money, worry number two. Go on.

Tom Feddo: [00:37:01] In 1992 Congress passed the Byrd amendment which required CFIUS to undertake an investigation where two criteria are met: Either the acquirer is controlled by or acting on behalf of a foreign government and the acquisition results in

control of a person engaged in interstate commerce. And then in 2007 we have FINSA (the Foreign Investment and National Security Act) which codified CFIUS's role in the national security construct.

Stewart Baker: [00:37:36] And if I can, practically everybody on this panel lived through that bitter experience. That was driven by sort of post-9/11 concerns about foreign terrorism in our ports.

Tom Feddo: [00:37:53] And then we have this past August the passage of the Foreign Investment Risk Review and Modernization Act which will be a substantial topic here today.

Stewart Baker: [00:38:04] Good. So let me ask Aimen about the experience of working through the FINSA and then FIRRMA. You saw both of those, if I remember right. What drove the adoption of FIRRMA, especially in a time when practically nothing gets through Congress?

Aimen Mir: [00:38:32] So just to give a broader, quick frame: If you think about the types of risks that we look at you're talking one about potential supply disruptions of critical goods and services, talking about technology transfer or the loss of technology that can be used against us or technology that's necessary for our national defense, and then you're talking about risks of espionage and sabotage. And those types of risks I think are a result of having an open economy and free market. A lot of those risks are mitigated in the ordinary course of business by export control laws, by US government contracts with companies and the provisions of those, and criminal and national security laws, and so on. But I think part of what CFIUS has historically been based on is this idea that ownership is different. Ownership actually gives the ability to change the calculus of a company and either violate their legal obligations and so on. And so I think over time you've seen different things challenge sort of the perception of whether or not that balance between allowing open and free trade and investment and the risk that companies may not do willingly or unwittingly abide by their obligations that different types of investment may challenge that. I think what you've seen in the past five years is

one a rise of investment from China which obviously has challenged – China's different than almost any other investors. You talked about the Japanese. You talked about the sovereign wealth funds from the Middle East. China is both a major economic competitor as well as a strategic challenge. And then you layer on top of that the rapid technological changes, increased globalization of supply chains, and you have changes over the past few years that result in types of investment and risk that we just hadn't seen in prior years. So I think that's what motivated this latest round of changes. There were a number of enhancements that we've been thinking about for a number of years, but because legislation is it an unpredictable thing you only open it when you really are at the point where you have a critical need. And I think we've found that it was increasingly clear that companies were particularly in relative risk of technical loss of technical capabilities and transfer of technical capabilities and technology that those weren't being adequately addressed under the existing control framework where CFIUS could only look at transactions that resulted in foreign control of a US business. It's pretty clear that there were instances of non-controlling investment that where the investors weren't passive even if they were not controlling that would allow them certain levers of influence to facilitate technology transfer.

Stewart Baker: [00:41:36] So wasn't this driven in part by a very influential report that was written for the Secretary of Defense at the end of the Obama Administration that came out of the DIUX effort? When they went out to Silicon Valley they discovered all kinds of reasons to be concerned about US technological edge and what it meant for our military technology in the future?

Aimen Mir: [00:42:03] Yes, absolutely. I think that report was influential in a lot of circles. I think the risks were already being seen even before that. And I think that sort of crystallized the concerns and I think resulted in two things. One is this increase... We were seeing at the same time this concern about minority investment and we were seeing concerns about other transaction forms such as joint ventures which also served as a means that didn't result in control of a US business or transactions didn't result in control of a US business but were opportunities for foreign companies or foreign countries to essentially acquire capabilities in the United States that you couldn't

develop frankly through theft. You couldn't just steal. It's not just a question of stealing a technology. You actually needed to get the capabilities that the companies had in the United States. And you had to buy it or you enter into a very close relationship – and that relationship can be in the form of a joint venture, it can be a form of close investment relationships where you have extended contact over a period of time.

Stewart Baker: [00:43:15] So David, let me ask you: You've watched CFIUS for a really long time. Were you surprised that this bill got through as quickly and with as little fuss as it did? There was fuss, but it was remarkably contained.

David Fagan: [00:43:36] That's a great question. I was going to start by saying for those of you who didn't know, Stewart, in 2006, he had a full head of hair before Dubai Ports, so he knows firsthand. So Tom that's what you have to look forward to.

Stewart Baker: [00:43:48] I was six feet tall too!

David Fagan: [00:43:50] The legislation [FIRRMA] actually started in 2016 and then picked up steam in 2017. So it was not necessarily a push by the way from this administration. It started in Congress before that. It reflected some of the concerns that were being picked up in DIUX. Even other transactions that were not identified in the DIUX report had raised some concerns I think within the executive branch and Congress. Anyone who was in Washington the last couple of years, I think if you asked them at the outset, "Does a particular piece of legislation stand a good chance of being passed in a bipartisan fashion by Congress with full support from the administration," you would have to start by saying, "Probably not." That being said, if you looked at the issues that were being examined, they were legitimate issues. It was fair for policymakers and for legislators to take a look in 2017, 2016, ten years after FINSA and say, "Well, the foreign investment composition has changed. The global economy has changed. There are more interconnections between the US economy and China. There is more activity, and it is in areas where both economies need to grow. That growth in turn is in technology sectors that may be relevant for defense and national security purposes." So it was a perfectly fair question to be examined. And when you start

looking at it that way – and you know nobody is going to stand up and say, "Oh well, we shouldn't be tougher on the Chinese," right? Across any political issue, there are not going to be people pounding the table that way. So when you frame it that way, which was how it was framed from a legislative standpoint, and it had I think fairly strong backing from this community, from the national security community, not necessarily in terms of the final substance but in recognition that there were legitimate issues that needed to be addressed. When you looked at it that way – and you know give credit to the people who steered it, they steered it in a politically sophisticated way as it went along. It got some real momentum so by the end it was not a surprise.

Sanchi Jayaram: [00:46:11] There is a thread of commonality still as a couple of people noted here. The five public prohibitions we've had in history are MAMCO, Ralls, Lattice, QC (Qualcomm), and Aixtron. Only been five prohibitions in history of 43 years there has been CFIUS around, and all of them do have a commonality that remains present today and was present at the time CFIUS was formed. So this is more of an add-on to what's already there. I wouldn't characterize it as a shift from what was in the past. We still care about everything, Stewart, so don't try and let people think that we don't care about something in the past now.

Stewart Baker: [00:46:48] Fair enough. So China's the commonality in all of those. Let me ask you: National Security Division at Justice has now a long history of indicting Chinese espionage actors and also has a lot of concerns about Chinese investment from a CFIUS point of view. How do you view Chinese investments strategically for the future?

Sanchi Jayaram: [00:47:21] Well, again we care about everything. With China in particular, I think Aimen already talked a little bit about just the change in statistics over the years. But as Treasury officials have already publicly said, acquisitions by Chinese companies accounted for the largest number of notices of any country filed with CFIUS in 2013 and 2014. And in those years, they replaced the UK and Canada as the largest source of CFIUS transactions. That trend continued in 2015, which I believe is the latest year for which the official CFIUS stats are available by Treasury. And I mean the

composition of CFIUS transactions tends to be generally consistent overall with the trends in general FDI [foreign direct investment] in the United States. So even if there isn't a one-for-one correlation, China has been obviously a rapidly expanding investor. The Rhodium Group also reported that the number of mergers and acquisitions from China increased nearly threefold from 2012 to 2015. So it shouldn't surprise anybody here that we've seen a spike in the number of CFIUS matters where the acquirer is a Chinese company, most of which have been the result of voluntary filings. And as the process requires, we individually look at each transaction, but as a general matter our volume has increased as well. In 2016 that was a banner year for CFIUS, and the number of filings we reviewed was 172. Last year was even busier with close to 240, and this year does not show any indication of slowing. Quite the opposite, actually. So I would say that we are still interested in everything. We are still looking at everything individually, but we don't dictate the composition of the folks who are coming before us and what we're looking at.

Tom Feddo: [00:49:13] I'll just emphasize Sanchi's point. The CFIUS process is largely voluntary and has been. We're exclusively focused on the national security risks of the particular transaction at hand, so we're very rigorous in our analysis on the facts and circumstances of the particular case. And so it makes sense that if Chinese investment or other investment in the United States from another country is increasing that a larger proportion of the cases we look at will include investments from those countries.

Stewart Baker: [00:49:51] About whether we treat China just like everybody else. It's no surprise. And let me ask David, as a private sector participant in this, do you think China gets special scrutiny?

David Fagan: [00:50:05] So as the one person on the panel who actually has not been on CFIUS and just had the pleasure of living through it for 17 years and therefore maybe I can be a little more subjective – I'll put it that way – yeah, China gets special scrutiny. And the remarkable thing about FIRRMA was that it passed without China actually being mentioned in the statute notwithstanding the motivation of it. And everybody in the deal community, whether you're on the buy or the sell side or China or

not, recognizes that there are a special set of circumstances and legitimately so. There's not – and I think this has been drawn out in this panel – there is not a historical precedent for the two largest economies in the world including ours being so intermingled and at the same time the other economy, our counterpart being perhaps the longest term and most significant national security threat to the US. And when you have that and you have a globalized economy and the like, you have to be able – if you're going to run a real foreign investment process that allows in the foreign investment that you want but carefully scrutinizes others to ensure it's not harming national security – you have to be able to identify and differentiate among the threat actors. And so right now you know that certainly is China. And I can totally understand and respect why everybody on the panel who has recently been in government or is in government has to be very careful about what they say, and that's appropriate. But the reality is that we can't in the private sector look at a transaction that could go through CFIUS, even if it does not involve a Chinese acquirer, and not analyze it from the perspective of what will it mean for China versus the US.

Stewart Baker: [00:52:05] So Aimen, you are free at last to speak your mind, but you're remarkably cautious in doing so. Let me ask the question: Do you think China gets special scrutiny?

Aimen Mir: [00:52:15] To some extent it's a matter of semantics, right?

Stewart Baker: [00:52:18] I told you so.

Aimen Mir: [00:52:21] In the following sense: Any given transaction is a combination of looking at the threat vulnerability and the consequences. Right? I guess I would differ slightly from what David said in the sense that we're not looking to allow investment that we want. We're looking to keep out investment that we think causes a problem. And so if it comes to Chinese investment and you're looking at the particular transaction and it doesn't raise a red flag because you know there's either no threat or there's no vulnerability or the consequences don't raise security issues, then even as the time that I left which was just a few months ago we were approving those transactions. So you

take it as it's presented. And I think everybody knows the nature of the risks that we face. And I think everybody expects that the committee will scrutinize those that red flags any one of those factors. And I think that's what you see in practice.

Stewart Baker: [00:53:22] So I'll come back to David. My sense is that the Chinese have taken the hint, and it helps to have a fairly centrally planned economy. You can turn off your investment in the United States pretty quickly, and I wonder if that isn't happening already.

David Fagan: [00:53:42] So let me start by saying I think your question which was on the scrutiny as opposed to whether we're open or not open was an important way to frame it because I completely agree with Aimen, and we're seeing evidence of that. There are Chinese deals that are still getting approved. It's not that there's an absolute block. And that was an important decision I think that was made earlier this year which was to examine things on the facts and not actually have an absolute bar. So I totally concur with that point. There's been a slowdown of Chinese M&A activity and investment. Certainly the big deals that you saw happening 2015 and 2016 largely are not happening. If they are happening, they're outside the US with a smaller US tail, so a China-Europe transaction. The Chinese, for their own reasons, have instituted capital controls to more carefully examine how money is flowing out of the country and allowing it in certain areas and more carefully controlling it in other areas. The areas that they tend to allow it actually happen to overlap with where the US has more concerns. So I don't think they've totally turned off the spigot. What we're seeing is that one, as I said, the big deals aren't happening. That's not just because of China. It's also because if you're doing a deal, you want to have regulatory certainty. Timing matters. All of the things that go into an M&A process. And if there is regulatory uncertainty or if the timelines look too long and you're on the sell side, you're going to discount other bidders. And so there's a natural market reaction that's part of this as well. It's not just because of Chinese policy. With that being said, I think where we're seeing the most activity is outside of the SOE sectors. The SOEs seem to be...

Stewart Baker: [00:55:36] That's the state-owned enterprises?

David Fagan: [00:55:40] Yes, the Chinese state-owned enterprises seem to be – and this is anecdotal, I don't have the actual empirical evidence, but we have pretty good visibility into the deal flow activity – the Chinese SOEs seem to be more constrained. I think it's reasonable to infer that that has something to do with government policy also. Where we're not seeing the slowdown is with non-SOEs who in particular are in the technology sector and have their own investment funds and have a very active deal team and deal flow, and those are still being examined. Less so transactions that would confer control to them, more transactions that would be non-controlling, and I suspect now with the pilot program that we will get to, more transactions that not only will be non-controlling but also not have the indicia of the other investment criteria in the pilot program.

Stewart Baker: [00:56:44] Okay. Tom, can you give us some sense from your perch at Treasury what the change in investment trends is, not necessarily as a result of CFIUS but just are you seeing the same kind of trends in who's investing and from where and in what that David's talking about?

Tom Feddo: [00:57:07] So I don't think I'm in a good position to comment on trends that I'm seeing from my current position, but you know I would emphasize again a point that Sanchi made. In the history of CFIUS, only a handful of transactions have been blocked. So a couple of things to keep in mind as well: CFIUS is a national security authority of last resort in some respects. When we look at a transaction and we do that threat vulnerability and consequences analysis that Aimen alluded to, we're asking whether there are other authorities that adequately mitigate the risk. And if not and CFIUS acts, then we look to can we mitigate the risk, is there a way to enforce a mitigation agreement, and mitigation principles that deal with that risk. And so the bulk of transactions are not being blocked, have not been blocked or prohibited. And so you know an investment is looked at with the particular facts and circumstances in mind.

Stewart Baker: [00:58:20] I'd like to jump now into what changes FIRRMA has made in the review process and give people in the audience a sense of what transactions are

going to be handled in a different way and if you're advising private clients or thinking about the impact on your agency to know what FIRRMA changes. And Tom, you had said CFIUS is largely voluntary, but the real innovation in FIRRMA – or one of them – is that a lot of these transactions are not going to be voluntary. Can you give us a feel for what FIRRMA says? "We don't care whether you want certainty or not. You're going tell us about this transaction, and we'll decide whether to review it."

Tom Feddo: [00:59:12] So that's a bit of a broad brush. I think post-FIRRMA it will remain largely a voluntary process. I have to be a little bit careful here because I'm actually on a panel during an open comment period on the pilot program. So the pilot program allows... So to back up, FIRRMA allows pilot programs to be initiated during the pendency of the promulgation of regulations fully implementing the statute. So it gives the government the power to take parts of FIRRMA and implement it before final regulations are promulgated. And so there is a pilot program right now that will be effective on the 10th of November. And that in fact does use some mandatory authority with respect to what is a new concept in the CFIUS process, and that is a declaration which is intended to be a short form filing of roughly five pages that provides an opportunity for the government to look at certain types of transactions in a certain part of the jurisdiction of the committee. And so yeah, there is a mandatory element to that, but that's with respect to the pilot program.

Stewart Baker: [01:00:50] Only with respect to the pilot program. Let me ask Aimen because I think Aimen, while he may or may not want to take credit for being the architect of all the changes in FIRRMA, certainly was present as they were developed. And there are a lot of them. The pilot program kind of pulls all of them together, at least for certain transactions. If you were painting with a broad brush, Aimen, what would you say the biggest changes are in FIRRMA? One, the move from voluntary to mandatory for certain transactions, and maybe you can tell us what those transactions are or what the statute says about things that must be disclosed to Treasury?

Aimen Mir: [01:01:40] Sure. With respect to the mandatory filings I think at least the intent in including the statute was to address this particular challenge you have with

technology transfer. Once the technology is gone, a post hoc review is not necessarily going to be an effective remedy. So what I think the intent certainly was to maintain a system that is largely based upon voluntary filings and recognize that there are going to be those transactions where you need to have the ability to look at them before the transaction is actually consummated. I think there's a tension there. The broader the scope of the mandatory requirement, the greater the obligation on the government to provide certainty on a timely basis. And I think for CFIUS going forward, they're going to have to think about that. If you're requiring so many things to be filed and you can't give people within 30 days the degree of certainty and just leave them flapping in the wind, then I think that's going to cause a lot of unanticipated turmoil. But in terms of some major changes, I would say that the core change in FIRRMA was the expansion of CFIUS authority to cover non-controlling but non-passive investment. That type of thing highlighted in the DIUX report in investment, in venture, in startup companies in Silicon Valley or elsewhere where you get a board seat or you get some access to information that you may not be able to get from the outside. And it allows you either to access technology or create relationships and so on that would facilitate technology transfer.

Stewart Baker: [01:03:20] So I think of this as moving from a CFIUS concern about control of the corporation to being concerned about insight, understanding of the technology, understanding of the industry trends without regard to whether you can make the company do what you want.

Aimen Mir: [01:03:38] Insight and opportunity to exert influence. The statute expands only with respect to critical technologies and critical infrastructure, and then it's very late in the process sensitive personal data was added. But I think the first two are the main risks there. Another thing that sort of came up during the conversation, as I mentioned, was this joint venture point. That got spun out into export control reform. And although it's not part of the CFIUS statute, per se, I think it's something that's very important to watch because it is out of this whole discussion in another area of risk that we just as a government had not adequately covered. And that was the subject of a lot of concern over whether or not our existing framework was sufficient to address really a new type of security technology-related risk that we hadn't faced in the past.

Stewart Baker: [01:04:43] So David, I thought that the one conflict that was pretty sharp over FIRRMA was this question of export controls and joint ventures where the Defense Department had become concerned that companies, US companies, were transferring large amounts of technology to JVs and to partners abroad who then stood up on their own two feet and wandered off in the direction of the PLA. And they wanted to get better control of that. They originally proposed that that be governed by CFIUS, and that's the one change that I think was significant in the progress of FIRRMA from idea to actual enactment. Can you give us a little bit of color about that and how the final resolution addressed it?

David Fagan: [01:05:45] Sure. So I think, Stewart, you nicely framed the issue. I think there was an additional piece of it which is that the export control laws which govern the transfer of that technology to China or other jurisdictions. It's a cumbersome process to identify controls and typically multilateral, and there was concern that as technology sped up, the export control laws had not and classification system had not kept pace with it. So it was not only that it was being transferred – it was being transferred lawfully – but that perhaps the control system needed to be updated and there was concerns about that. And frankly I think there was concerns about the export control rulemaking process being able to move fast enough, and that was one of the things that led the original proposals to include this within the CFIUS remit. There was a very strong allergic reaction to that among the US business community. And while one of the interesting aspects of FIRRMA is typically you have a law that comes along that that does fairly radically change something that relates to business, you have very strong engagement, typically some pushback from the business community. There was not a ton of pushback among the business community on the idea of FIRRMA, reflecting that among a lot of US companies there was real concern about China. So it sort of there was this conflict within the community that I think led them to not really push back on FIRRMA except on the one piece which was the outbound technology transfer, and if you look at it, CFIUS historically and remains an authority that acts where other authorities of the US government are insufficient to address the US national security concern. And we do have export control laws and trade control laws. And so the

pushback was not that the concerns weren't legitimate. It was not that there shouldn't be an examination of the outbound technology transfers. It was rather that CFIUS was not the appropriate authority. There are existing authorities: Commerce control lists administered under the EAR [Export Administration Regulations] by the Department of Commerce. You obviously have the ITAR [International Traffic in Arms Regulations] already. And that that was the right place to deal with this set of issues.

Stewart Baker: [01:08:17] So let me call BS on that. [Laughter] Because we had spent at least 20 years with a complete logjam over whether there was even going to be Commerce Department export controls authorized by Congress. In fact, Congress hadn't authorized them, and administration after administration had to gin up a pretend economic emergency so that they could use the International Economic Emergency Powers Act to keep the export controls in place. And then Commerce and the Defense Department were constantly fighting over what would be on that list, and so the list didn't get updated much. And what's remarkable about the achievement of Senator Cornyn and others in this is that they said, "Not only are we going to pass this bipartisan bill on CFIUS reform, by the way will clear out this logjam of the Export Control Act, and adopt a new one and encourage the Commerce Department and the Defense Department to come up with a list of technologies they're are actually worried about this year instead of in 1994."

David Fagan: [01:09:25] So, Stewart, is your point that it actually was the responsibility of the people who had been in government and legislators to have addressed this before? [Laughter]

Stewart Baker: [01:09:34] Yeah, if they'd only listened to me then! [Laughter] So Aimen, That took us to the idea of figuring out what technologies we're really worried about. And that gets us into the intricacies of what is going to be mandatory in the pilot program because the pilot program is very definitely aimed at a certain set of technologies used in particular industries. Can you break that down for the audience?

Aimen Mir: [01:10:04] Sure. The pilot program I think is a step towards addressing sort of the immediate need of transfers that investments are already occurring. I think it's the way the pilot program is structured is it's keyed off of the export control list as they exist today, and then it refers to companies that are producing those technologies or developing those technologies and are either themselves in a listed industry or are producing them or developing them for a listed industry. I think there is like 20-some industries listed by NAICS [North American Industry Classification System] code, and I think the real impact of this will ultimately be felt when Commerce is able to put out a rule that adds in the emerging and foundational technologies that are not currently controlled under the list. If you think about something like artificial intelligence, it's not clearly covered under any current export control provision but clearly an area of great concern from a national security point of view in terms of what capabilities are being developed, what technologies are being developed in the United States and of foreign countries may have an interest in. So I think that's when you'll see a lot more of the impact. I think we'll have to see what the impact is. David's probably talking to a lot of his clients currently and probably can give us a sense – and used to it as well – of what you're seeing in terms of the likely impact of sort of the list as it occurs today.

Stewart Baker: [01:11:54] So let me ask David to jump in. What is the impact of the list approach and the pilot program itself?

David Fagan: [01:12:02] You mean other than funding my kid's college education?

Stewart Baker: [01:12:05] Nothing wrong with that!

David Fagan: [01:12:07] So the pilot program is, I would say, pretty radical in the sense that it changes things from an evaluation diligence analysis standpoint. To be determined how much impact that actually has on deal flows, what CFIUS sees, and the like. And just to recap what the pilot program does, FIRRMA requires CFIUS to implement mandatory declarations with certain types of transactions and these other investment categories when they involve a substantial interest of a foreign government. That is still to be implemented through rulemaking. FIRRMA also has a provision that

says CFIUS also can mandate declarations with respect to other investments, whether they include foreign government interest or not, into the critical technology area. And that's where the pilot program is. The pilot program applies to any equity or contingent equity investment made by a foreign person into a business that manufactures, fabricates, produces, develops, designs, or tests critical technology in one of 27 industry sectors or for use in that industry. So it's broad in a lot of respects. It is not limited to a particular country. It applies to any foreign person. For those of you who work in the CFIUS space, you know any foreign person is any person who themselves are controlled by any foreign government, foreign national, or foreign entity, and the control definition is very broad. So there are probably a number of US companies that don't realize that they are foreign persons who could potentially be captured by this. And then it mandates filings in those areas. So at this point what the immediate effect is you have to go through – if you're doing a deal that involves equity or contingent equity, and contingent equity is defined as anything that could ultimately convey or convert into an equity and voting interest, and you can have you know convertible note that has one share that can be converted downstream to equity or voting and then that's a contingent equity under the pilot program – when you're doing deals in any one of these 27 sectors or that may involve something that manufactures, produces, directs, develops, designs, tests a technology into those sectors, you have to evaluate upfront: Do we have a foreign person? Is this structuring something that might trigger this? Is critical technology potentially in scope in any of these ways? Which in turn relates to a number of lists. (The US government likes lists. The private sector is not so accustomed to dealing with as many lists.) The most salient one is the Commerce Control List and certain categories on there. And then you analyze whether you're in the 27 sectors. That last piece actually isn't that hard. Although for those of us who have not been in the government, it's not like we were walking around with NAICS codes on the tip of our tongue for the last 10 years or longer. But once you look them up, they're pretty broad and you can figure out whether a company is in that industry.

Stewart Baker: [01:15:37] They're mainly used for statistical purposes or have been up to now. Are you seeing any sign that people are lawyering their classification thinking, "Well, maybe I should restate what my customers, our business is"?

David Fagan: [01:15:53] No, we have not seen any sign of that. What we are seeing is a very careful analysis on the export control piece of it because if you have a select agent or toxin or you're dealing with nuclear material or you have ITAR, right, that's fairly clear. That doesn't require a ton of analysis. The Commerce Control List, as many will be familiar in the room, it's not like every company has gone to the Commerce Department and had a full classification of all the technologies that they may have. There's a lot of self-classification in that also, and maybe they have or maybe they haven't closely examined it. So what we're seeing is first a lot of questions on structuring, and second a lot of questions on whether you can have a critical technology. Now within that there's a fair amount of ambiguity. What does it mean to design or develop? Right? Testing seems to be more clear. Manufacturing, fabricating, or producing seems to be more clear. But developing or designing? There's a little bit more ambiguity in that. And that's where we're seeing the most questions. On the structuring side it becomes more complicated again if you've had a past foreign investment and you haven't gone through CFIUS or if you're in the fund world that's where we're seeing it.

Stewart Baker: [01:17:12] This decision to say, "We're not interested in control. We're interested in insight. And we're going to give you a list of stuff that you have to file." That strikes me as driven in part by the past success of the private bar in structuring transactions in ways that make the buyer happy and leave the government without recourse. And that has led to the decision to sweep a much broader group of transactions into at least potential review. Let me ask Aimen to address that because you were there for that discussion.

Aimen Mir: [01:17:56] Yes, certainly. We saw transactions structured to avoid CFIUS review, but I don't think that it was necessarily only lawyers' advice that got us to that point. I mean clearly there are efforts to acquire technology through a whole range of means. And as CFIUS has started to become more assertive or aggressive with respect to transactions with in the scope, it was only natural that there were going to be efforts to look for perhaps less effective but still other means to access the technology. And

frankly I think that will continue to be the case that the statute itself, while giving CFIUS significant authority, did leave some things on the table. And there are judgments in any legislation about how far you're going to go. Are you going deal with the instance where the foreign company is setting up an office right across the street from a major US company and hiring away its engineers? That's a different type of regime. So I think companies will be looking for ways to get their capital to the companies that are looking for the capital. But I think there's also something more at play in relation to concerted strategies to acquire technologies and using a whole array of means to actually effectuate that.

Sanchi Jayaram: [01:19:35] From DOJ's perspective, last year we co-led more cases than we had in the previous five and a half years combined. And there are some reasons for that. These stats are in part due to the high value of seemingly ordinary information, so thus far on this panel we've talked a lot about the pilot program and technology and China, but there are other things to consider too. And so while I can't talk about specific CFIUS cases, I can give you some examples of some of the other work that the National Security Division has done that kind of illustrates some of our concerns, and some of them have a regional nexus that have something else and not China related at all. So just to give one example, in a recent action we found that at the outset of its work for DOD, a government contractor committed that only US citizens with a security clearance would work on certain projects for the US military. We found that that very same code that was intended to run our military's computers, including the classified network some of you know SIPRNet [Secret Internet Protocol Router Network] was written and stored on computers in Russia that was transiting networks that Russian intelligence officers have the ability to access and collect from and do so without no notice pursuant to a Russian legal regime called SORM [System for Operative Investigative Activities]. We also found that there was no definition of the scope of the project and its requirements. So ultimately the Department of Justice settled the action with and reached a non-prosecution agreement with the firm, closing the criminal investigations without charges last December. But what that illustrates – and there are a number of other cases I could describe – legal regimes matter. We look at whether a foreign country has a system like ours where the government needs to

make at least some showing to an independent judge before it can compel a US party to provide information. Remote access matters. A company's network is only as safe as that of the least secure user or vendor that accesses it, and secure remote access requires vigilance. On the other hand, words on paper can matter less. So contract security agreements, security plans, and so forth will not protect a company or its assets unless the management actually ensures that they are followed. And then finally, data matters. Even personal information can be a matter of national security. Protecting that privacy of individuals is something that we care about, and there are several reasons for that.

Stewart Baker: [01:21:56] So my understanding is that sensitive personal data is singled out by FIRRMA as a reason for special scrutiny for investment review, and DOJ has been particularly attentive to that concern.

Sanchi Jayaram: [01:22:13] I think the whole US government and all agencies care about that. I mean there's a convergence of cybersecurity and information, and frankly that undergirds every industry we have, every NAICS code that we just discussed. So it isn't in and of itself its own issue. It's something that is connected to every other issue. And I mean people I'm sure realize 10 years ago this may not have been a concern, but in the last decade a few things have changed. First of all, the volume and variety of data has increased exponentially. Information that was previously not stored in a digital form now is and at the rate that those data are being created and the velocity of data growth that's increasing. So for an example, take cars. Not long ago a car was essentially a mechanical device or an engine with seats that moved you from point A to point B, and whatever limited electronic components it had were self-contained. But today's cars, by contrast, certain communication devices, sensors, GPS, navigation, other kinds of services, they're all computers with a variety of functions. They allow you to check your fuel levels and tire pressure on cell phones. You can track a stolen vehicle over the Internet or call for help in an emergency. And your kids can enjoy the same entertainment in your backseat as they are at home. So some of those things are good and useful for the driver and passengers, but obviously they can be useful to other nefarious actors as well. There are similar examples in the market for DNA testing. So

for example, according to one report from last year, DNA testing with respect to health, longevity, paternity, and ancestry that has become an $830 million industry. And one industry leader in that particular area has claimed to have information about more than six million people.

Stewart Baker: [01:24:07] Sanchi, let me ask you about this. You're right that sensitive personal data about us is everywhere now. It's like Pig-Pen, the Linus character where we just keep dropping it everywhere we go online. There is no federal regulation of sensitive personal data. It's export to anywhere, unlike the European Union. When the Justice Department or other parts of CFIUS reviews a transaction that involves sensitive personal data being transferred or insight being allowed, it has an ability to say no or to impose mitigation. When there is no transaction, there's no jurisdiction. You've made the case that it's something to worry about. But should we worry about it outside of the CFIUS context? Should there be a broader regulation of transfers of sensitive personal data?

Sanchi Jayaram: [01:25:11] Well, I mean I think we're seeing a trend in this area generally with GDPR that became effective earlier this year. There was recently an order the Australian government put out in August and its own TSSR [Telecommunications Sector Security Reforms] and security regime became effective September 18th of this year. In New Zealand we have TICSA [Telecommunications (Interception Capability and Security) Act] – or they have TICSA. We don't have TICSA. But the point is that everybody is thinking about this. A lot of people are thinking about this. And I think what many people have understood is that information that seems unimportant or purely personal or irrelevant can in fact be used to threaten national security, and that's the nexus that we care about. Is it a national security issue? And frankly in the aggregate the information that may otherwise seem irrelevant can actually provide commercial or cultural insights that might have a monetary or other use, and the information can also offer a pattern of life of a company CEO or a government official and could also be used to target that individual. Now some people might say, "Nobody cares about my data or what my kids are watching on TV in the backseat of my car." But the fact that most people in a data set might not be targets themselves actually provides

little comfort because anyone on social media has learned that we are more connected than it seems from our daily routines. Folks know in 2016 that Facebook reported that its American users were actually separated by fewer than three and a half degrees of separation on average. So extrapolating what that means offline, a private citizen's information can be useful for what it tells us about maybe that person's brother, the CISO at a major bank, or her aunt in the CIA. Our concerns are exacerbated by the fact that the traditional methods of de-identification of data such as anonymization or encryption of content may be defeated by, for example, sensor and geolocation data or by cross-referencing sanitized data against other data sets.

Stewart Baker: [01:27:11] So this is very broad. At the end of the day, since all of this information can be turned into pattern of life analysis and any of the individuals whose pattern of life could be extracted from this might be working for SOCOM [United States Special Operations Command] or the CIA, there is a national security element to this. But the implications of saying we're worried about that and we want to control it are that you need a regulation that addresses the handling of almost any personal data by almost any private sector entity. Right?

Sanchi Jayaram: [01:27:54] Well, I mean I think, as I noted earlier, there are correlative efforts underway in a number of different governments to address what this question is and what the scope of the question is. I can tell you that in certain circumstances we're certainly interested in it. It's reflected by the cases that the National Security Division undertakes. But it can also be reflected in surprising ways. In one of the cases that a lot of my colleagues and I have talked about is this example of a few years ago when a Midwestern consumer goods company was the victim of what appeared to be a run-of-the-mill intrusion. So in that matter an intruder had obtained unauthorized access to their customer database and had obtained personally identifiable information for their customers. The company's IT personnel worked diligently to eject the hacker, but he kept coming back. And eventually he threatened to expose the company's customer information unless he was paid a ransom. So I'm sure at this point everyone here heard 20 stories about that kind of thing if not more. Around that time is when the company contacted the FBI, and the FBI determined that Ardit Ferizi, who was a Kosovo citizen

studying Computer Science in Malaysia, was one of the hackers who had gained unauthorized access to the victims' PII. FBI determined that Ferizi had a financial motive in demanding the ransom from the company. The PII he stole was actually not destined for the black market, but the data was of interest because among the tens of thousands of customer names and emails he stole there were more than 1,000 addresses that ended in ".gov" or ".mil". So ultimately Ferizi had used that information to produce a kill list essentially of approximately 1,300 USG civilian employees and US military personnel, and provided that to the Syrian-based ISIS member named Junaid Hussain. So I mean what happened at the end of that is a few months earlier Hussain had posted that kill list and purported to include the names and addresses of hundreds of members of the US military, and in fact soon after he received the information from Ferizi, Hussain used Twitter to publish the PII of 1,300 government and military customers of that company. DOJ charged Ferizi with violations of the Computer Fraud and Abuse Act, with conspiring to provide material support to ISIS, and were successful in obtaining the extradition from Malaysia to the United States, and ultimately he pleaded guilty. But what that story illustrates though is the number of connections between what can seem relatively innocuous and only commercial in nature, and unfortunately there aren't a lot of these types of stories that we can talk about but this one is actually connected to counterterrorism.

Stewart Baker: [01:30:42] The other part of that story is it's a great triumph of attribution because not only did we attribute the hack and arrest the guy who did the hack, we found the guy who sent the Twitter message about his kill list and blew him to kingdom come, suggesting that at least if you're going to have to be on a kill list, being on ISIS's is maybe not as bad as being on ours. [Laughter] But you had another lesson you wanted to draw from that.

Sanchi Jayaram: [01:31:13] The point is that what may seem innocuous or irrelevant or mundane or unimportant can actually have an extraordinarily larger consequence, not just for your own commercial business but for the interests of the nation. And we see this obviously many times over in a way that folks who are not in our world, you know

they don't see it. So my only point is to say that the connections are real, and the reason we care about these things is exactly because of stories like that one.

Stewart Baker: [01:31:49] That is the last word. I want to ask the audience to join me in thanking a really excellent panel. [Applause] Alright. Thank you to Dr. Megan Reiss, David Kris, Nate Jones for joining me. This has been Episode 239 of The Cyberlaw Podcast. I promised I would read some of the more entertainingly abusive reviews that we've gotten on iTunes and elsewhere. This time I'm going to give you two to see if you can do better than this. They kind of come as a pair, as I see it. Here's one that says – quite critical and maybe not so entertaining – "Because California is taking a states-as-laboratories approach to Net Neutrality, the host made a comment along the lines of 'If South Carolina wants to take down their statues of John Calhoun, looks like California might want to put them up.' I get that the host did not mean that California is as bad as the Confederacy" – actually, Calhoun was dead by the time the Confederacy came along – "but this comparison went too far and was horribly offensive. I am really interested in cybersecurity law, but this was so out of line I may stop listening." So there we go. I think one star out of that one. And here's the one that comes right after it: "Millennials beware. Don't be fooled by the fact-based discussions in this podcast. Do not find yourself intrigued by listening to actual high-ranking government employees discussing cybersecurity. These people are all over 30 and are not to be trusted. Five stars." Yeah, and I'm not sure that Megan is over 30. But you know she is clearly not to be trusted and deserves all five stars. Okay. Please do see if you can do better than that. We're running out of entertainingly abusive reviews already, so I'd love to see some more. As I said, I'll take any abuse at all for five stars. If you got somebody to suggest as a guest interviewee, send us the suggestion at CyberlawPodcast@Steptoe.com. We'll send you a Cyberlaw Podcast mug – highly coveted – if they come on the show. If you're interested in finding out what we're going to talk about, you can follow my Twitter feed [@StewartBaker] where I sometimes list the stories that I think are worth talking about. And for upcoming shows we've got: Mieke Eoyang of the Third Way, who will be talking about her Cyber Enforcement Initiative, which is an interesting approach to improving cybersecurity; and Representative Jim Langevin of Rhode Island, who is the Democrat most

knowledgeable about cybersecurity, in my view, in Congress will be coming on now that it's clear he'll be in the majority. Show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett's our audio engineer; Michael Beaver's our intern; I'm your host, always trolling for abusive reviews that give me five stars. We hope you'll join us as we once again provide insights into the latest events in technology, security, privacy, and government.