TORRES TRADE LAW
INTERNATIONAL TRADE & NATIONAL SECURITY

Podcast Episode 12

Olga Torres: Hello and thank you for joining us today to the Torres Talks Trade podcast. My name is Olga Torres and I'm the founder and managing member of Torres Trade Law, a national security and international trade law firm. Today we decided to divide our podcast into two series. We have two guest speakers, and we are all very chatty so I hope you enjoy the podcast. Stay tuned for more next week. Today we are going to be discussing ZTE, BIS enforcement priorities, and other interesting things with our guests. Thank you for tuning in.

Today we're joined by Don Pearce and Jim Fuller, both of them, former OEE agents with the Office of Export Enforcement. Hello gentlemen, thank you for joining us.

Don Pearce: Thanks for having me back.

Jim Fuller: Hello Olga.

Olga Torres: Today is going to be a little bit different because we have introduced you to Don before. So, we'll skip the intro for Don, if you are not familiar or if this is the first time you join our podcast feel free to go back to our very first podcast with Don, where he gave you his entire career background and a lot of really good information. But we'll get started with very good and timely discussions regarding recent OEE changes or BIS, Bureau of Industry and Security, changes to enforcement priorities. We've seen BIS released a memorandum outlining some of these changes and we'll talk about practically speaking, what that means, what to expect. And, in terms of past experience by both of them, I know Jim for example, was very involved in the ZTE case, which is we discussed last week, actually. So, he'll give you more of the on the ground, boots on the ground-type perspective, as an investigator. I'm sure, Jim, maybe you cannot share everything with us, but whatever you can share I'm sure is going to be very interesting, especially given the fact that we're seeing some new developments on that case as well. Like it's been so long and they're still coming up with things on that case, right? Like two monitorships wasn't enough and now we're seeing some of the recent changes or announcements that were made. I think it was last week or a couple of weeks ago regarding one of their suppliers that was acting as an in-between. But anyway, we'll talk about that as well.

So, I guess, Jim, if you can just give us a quick intro, your background, how long were you with OEE? My understanding is that you've been in Dallas or North Texas for a while, can you give us just your background.

Jim Fuller: Sure. Thank you very much. Thank you for having me too. I really appreciate it. I started with OEE in 2006, and I left in early 2019, so 13 years almost to the day. I started out in the New York field office and did five years there. That's where I met Don Pearce and an old friend of ours who's, both bosses, actually are friends of ours, John Carson, who's the special agent in charge and Bob Dugin, ho's the assistant special agent in charge. We all worked together. It was a great place.

That's where Don and I met and we did, PPG together and China Huaxing Nuclear Corp together. And we worked with, who was then the AUSA, G. Michael Harvey, who's now the honorable G. Michael Harvey, he's a magistrate judge in the District of Columbia. One of the most brilliant men, one of the most brilliant attorneys in the nation. They keep asking him to take other court, excuse me, other judgeships and he just laughs at them. He's just happy where he is.

But anyway, and then I moved to Dallas in 2011. I was on my way to work, and the ASAC [Assistant Special Agent in Charge] called, Tracy Martin, who ended up being a Special Agent in Charge. And he goes, “Hey, could you do me a favor and serve this subpoena?” And that's how ZTE started. It was actually started from Washington, the Deputy Director at the time, John Sandman saw intel as well as public reporting and he thought it would be an interesting follow up and his instincts were right.

Olga Torres: And has that been the case that you've worked the longest in, or are there other cases that have lasted longer?

Jim Fuller: That is you're correct. That's the longest case. It is a multinational corporation. It's, the second largest telecom in China, the fourth largest telecom in the world. It does have quite an international reach. I mean, we looked at a ton of countries and subsidiaries that they possess, they reach to the farthest corners of the world.

Olga Torres: And what we were discussing last week. We all know the violations were so extreme in terms of the concealment efforts, right. I have questions as an investigator, and Don feel free to chime in, but part of what we were discussing last week was, well, they lied to their lawyers, they lied to the auditors. How does, how does OEE or the government in general, but

specifically for you at OEE, how do you uncover these falsehoods basically? I mean, if the lawyers are thinking something, if the auditors are providing you certain information, what's done in the background by OEE to discover that it's not true?

Jim Fuller: Well, there's a variety of tools, and this is where Don and I diverged in our careers. I stayed on the criminal side, always looking to prosecution, and Don went the other way on the intel side, all the secret side and all those tools within the federal government. But for us,

Don Pearce: No, I didn't.

Jim Fuller: Not all, no, I'm wrong. It's the wrong Don, I got the wrong Don. But I had several sources, both within the telecom community and inside of Iran. And so, we knew what they were getting, we knew what they were doing, and I worked closely— It wasn't just me, and Don worked on it too, but it wasn't just us. It was the FBI and HSI. Of course, the FBI is the 800-pound gorilla in the room, and they bring a tremendous amount of resources and they did all their stuff, both on the criminal prosecution and the high side. But it's one of those things you can conceal, you what's going in, you know the systems that they support, okay.

Olga Torres: Right.

Jim Fuller: And then what they're telling you doesn't match what's operating within the country and what their capabilities are. And we knew what Huawei was doing, we knew what ZTE was doing, and we had people in both organizations, initially, that were open about it. And companies have to realize this: when you have engineers that work for you and they're on LinkedIn and they're on professional forums and boards, and then they stop working for you and go to work for somebody else. But they list all the things that they do in their career. "Oh, I ran this section up until this date in Iran." So ZTE is telling us "Okay, we're we don't have anybody anymore in our field office, right, in that subsidiary." And yet you go on LinkedIn, you could find five engineers that say they worked on current projects. In 2015 they were saying, "Oh yeah, we just supported this project that they're standing up in Iran."

Olga Torres: That's really interesting. But do you think that in terms of government enforcement, do you think the U.S. has highly sophisticated enforcement capabilities? Because it sounds like you were using intelligence on the ground, right, within the country in Iran, social media, and a variety of other sources. Because you, when you read the case, right, at least the charges, I

mean, what they were doing, it almost sounds like they think they have a really good system and they're not going to get caught, right. Especially after they started being investigated. They were already under investigation and they continue lying. So, I wonder if there's a little bit of a discrepancy between, sort of dealing with the U.S. government and sort of understanding the capabilities that the government has versus perhaps other jurisdictions. And maybe that's a very unfair statement. I just haven't dealt with other jurisdictions equivalent of you guys, but what are your thoughts on that?

Jim Fuller: Well, you really can't hide in today's day and age, right? There's such a stream of information and even when you go, for example, when you go to a trade show, okay? People know what's going on. They know what's needed. They know what other countries are asking for, because a lot of it, they were purchasing American equipment, U.S.-origin equipment. And so, the people on the other end know, right. And you put that equipment into Iran and that equipment will talk back to the U.S. manufacturer for warranty updates.

Olga Torres: Yeah.

Jim Fuller: For systems, for patches. And so, then when we go to the U.S. suppliers and we say, "Hey, can you tell us about this X, Y, and Z?" And they're like, "You know, we got a call from the Iranians. We didn't answer them, but they wanted this stuff that they purchased from ZTE." So, with the speed of business today. And there is no school of criminality. People think, "I'm smart enough, I have this covered." And they never do. They never do.

Olga Torres: Yeah, it reminds me, like in a little bit different because it's more about the money, but in customs cases we always receive documents, right. And I'm like, I need proof of payment for everything because that's really, that's when we get to the bottom of it. Like proof of payment, because everything else you could be false for all I know, but once I see who's getting paid what, then I can come back with. So, there's always a way to. Don, you were going to say something.

Don Pearce: Yeah, keep in mind that the U.S. export control system is unique in its application, extrajudicially. You don't see that with a lot of export control systems. In fact, many export control investigations in countries with solid programs kind of end at the border. And we're unique in that we have export control officers posted overseas in embassies doing end use verifications, which are administrative actions of the Bureau of Industry and Security. That also allows for, I think, a better understanding of how to get that information that you might need to make an international case. I think the European Union is

examining end use checks. I know Germany is starting to do end use verifications for munitions exports. Other countries are looking at the end use end user verification programs in their own ways. And I think it's like anything else. Anything is better than nothing.

Olga Torres: Right.

Don Pearce: And just thinking that something, once it crosses your border is no longer your problem. I don't think that's a good strategy these days for export controls, especially seeing how many of them are now plurilateral controls where we're not using the multilateral control system anymore. But we are asking, other countries, like-minded countries, to kind of step in line and do the same things. I think that kind of homogenization is actually very good for international security, as well as for protecting legitimate companies from falling afoul of foreign export control issues.

Olga Torres: Yeah. That's a really interesting point. And that reminded me, recently we had, or fairly recently, I had a discussion with a foreign client, and we were talking about the U.S. government and some of the differences and in this particular government or where they were from. They don't have concepts as, for example, voluntary disclosures, right? So that the concept of even having to go to your own government and say, "Oops, we messed up and we are aware of it and we're going to fix it." Still within our own government, we have such a good relationship, or better than other countries anyway, between government and really private industry where the government realizes, "Hey we will give incentives to companies for themselves, they can manage their own operations, they know their operations better. And if they find out that they did something, then they, we will let 'em come to us." It goes back to we have really strong enforcement capabilities but we also, in addition to what you're saying, Don, and the differences with some of the other countries, even like-minded countries. We also have this system of voluntary self-disclosures and that creates that relationship with the government. I feel like that you don't see sometimes with some of those foreign companies where they think: one, "We can hide it enough where they're not going to find out." Which we know now that it's not going to be the case. At least not when the government is already looking at you. Right? I mean, there is something to be said, but every government has limited resources. But if a government is already looking into your activities, especially for example, we're talking about ZTE, don't continue doing it. Just clean it up. Don't do it. You will get caught. And voluntary self-disclosure is, going back to it, this trust that we have in the government or maybe not trust, but we we're going to get mitigation if we assist, we get

cooperation credit in this concept with enforcement. Don, were you going to say something?

Don Pearce: Yeah, I was just going to say, it's the rule of a hole and if you find yourself in a hole stop digging.

Olga Torres: Yeah. It's a simple enough concept, like do not keep digging. Yes, it seems like a simple concept that is not being necessarily grasped by everybody. Okay, we diverted a little bit. I want to go back to some of the changes that were announced. One of them was the charging letter now being published as soon as it comes out. I know Don, you had a quote somewhere, I forgot, the Export Compliance Daily, what was the name?

Don Pearce: Yeah, Export Compliance Daily. Yeah, basically was that now we're going to tell the world that we caught you with your hand in the cookie jar before we even realized if it's actually, if it's there or not.

Olga Torres: Because they are allegations, right. So, what do you think is going to be the effect of that? And also, and I know this is going to be, well, this is what I think they're thinking, but why do you think BIS is doing that? Like, what's the purpose?

Jim Fuller: Is that directed at me?

Olga Torres: Either, or whoever wants to take it.

Don Pearce: I'll jump on this one. One of the things that I think is interesting about this is it's equivalent to the old school New York city police department, perp walk. When you have the big high-profile case and you're going to go out and you're going to make the arrest. And it just happens that every newspaper in New York has a photographer or a stringer at the back door of the precinct waiting for the dude or do dudette to come through in handcuffs. And sometimes that's great. It's not great for the accused, right? And to just to keep reminding myself, as well as others, that in this country, you are considered innocent until proven guilty. And I feel like this might have a chilling effect, right on companies coming forward, where much like in countries, where there is no voluntary self-disclosure, here you have the opportunity for voluntary self-disclosure, and there's supposed to be great weight mitigation. But now you've got this threat of well, "If they don't think we are a hundred percent on this that we've fallen on our sword appropriately. They're going to charge us and they're going to put this letter out and our stockholders are going to see it and they're going to bail."

Olga Torres: I think for people that may not be as familiar, basically a charging letter and I'm reading it, it's merely the means by which administrative enforcement proceedings are initiated pursuant to the EAR. Basically, it's all the allegations of everything that you supposedly, or your company supposedly, did. But you haven't been proven, it hasn't been proven, right? So, what Don is referring to is if a charging letter comes out, there are repercussions to that. We can see companies stock plummeting the same day, or people getting fired, perhaps. Because what's going to be the repercussion if your company's charging letters out to the public before you've had a chance, for example, to do a VSD. But it sounded almost like Don, and correct me if I'm wrong, you're saying it could even have a chilling effect on actual VSDs for example, right?

Don Pearce: Yeah.

Olga Torres: I mean, I guess that's a question I have: could it be that a VSD will avoid that perhaps more so than if you don't do a VSD, if they find that on their own?

Don Pearce: I always say that you should err on the side of caution and contact OEE and initiate the process for a voluntary self-disclosure. In so many cases, good, trained compliance officers will read the law and read the regs and come to a conclusion that this item might have been a violation. And six months later, get a sternly worded warning letter telling them not to do it again. Because let's face it, we take this very seriously and we see every slip up as the crime of the century, which in most cases, it ain't even a crime.

Olga Torres: Right.

Don Pearce: And that's why there are erasers on the ends of pencils. People make mistakes, there are oversights. If you come forward in a timely manner, you're probably golden. I can't remember the exact statistic, but something like 8 out of 10 voluntary self-disclosures come back as warning letters.

Olga Torres: Right. That was one of the announcements that reminds me, for example, the announcement said, or the memo, we're going to have, the administrative VSDs, the voluntary self-disclosures that are more technical in nature. I don't know, I'm thinking of an example. Maybe if you have licenses and you haven't been managing your licenses, maybe you exceeded the value or maybe it expired or something more technical. Versus I'm assuming, you have Iran shipments and you have proscribed parties.

Don Pearce: I accidently confused Iran and Ireland and I shipped it all to Iran. That's probably not going to fly well.

Olga Torres: Yes, exactly. Okay, so, those cases, there's a distinction now going forward between the complex cases, let's call them, where we're going to get an OEE agent assigned and we're perhaps also an attorney assigned to the case. Which is going to be interesting, because now every time we submit a VSD, we're like, "Okay, we better not get anybody assigned because then that's like whoa, what's going on?"

I wonder, do you have any idea what's happening with VSDs that were under the previous system? Because we've had a couple where we're like, "
This is an administrative one," and we still have an OEE agent assigned and I'm assuming that's just because it was the previous way of handling things, and we shouldn't be worried. Should I be? I guess that's the question. Do we know, or is it still kind of in flux? What do you guys think?

Jim Fuller: Well, for me, I marveled when I read that enforcement memo because you have some amazing attorneys in OCC and you have a lot of great agents, but you darn sure don't have enough of them. I don't know where these people, unless they plan on a mass hiring event for both the agents and the attorney staff. Because OEE and OCC's role has grown even in the time that I've retired and Don has retired. They just keep finding applicable things, important things for them to do. They're like a utility knife, they're so good and stay so sharp we're just going to use them for everything, right.

Olga Torres: Yeah.

Don Pearce: The Office Chief Counsel is definitely a victim of its own success.

Jim Fuller: Absolutely. Absolutely.

Don Pearce: Because in addition to handling what they're supposed to be handling, which is the administrative enforcement, they're often called on as expert attorneys for the criminal prosecutions. And on top of that there're the outreach events and international programs and that mission creep can start to build.

Olga Torres: Yeah. That's interesting. So, you are worried that maybe they're not going to have, I mean, the announcement is the announcement, but in terms of actual manpower, the manpower may not necessarily be there?

Jim Fuller: Correct. You could infer this from the Far East Cable charging letter. Okay. Because the, the violations took place six years ago. What we don't see on the backside is any of the negotiations or any of the communications that may have taken place between governments and between the Department of Commerce and Far East cable, right?

Olga Torres: That's a really good one. And for people that may not know, Far East Cable was acting as the in-between ZTE and Iran's government. They were buying things from ZTE, but, *wink*, *wink* "Were going to buy them and then we sell them to Iran." So, I thought it was actually eight years. We were wondering when it came out, that's interesting that you mentioned that we don't know how long this has been happening in the background. Because I thought, "Hey, what's going on with the statute of limitations there?" Right? Like I thought it was eight years, but anyway, beyond the five-year statute of limitations, so one of my questions was, What happened? Did they, I'm assuming, they tolled the statute of limitations?

Jim Fuller: That's correct. They would've gone OCC's never going to go past that without a tolling agreement. And so, the tolling agreement, they would basically say, "Hey, look, we're entering in discussions for resolution with you, it's going to go past this date. If you don't agree to it, we only have the last tool in our toolbox is the hammer, right. So, let's just talk through this." It's going to be painful, how painful it's going to be is up to the subject company.

Olga Torres: Right, so they volunteered to waive it.

Don Pearce: Probably.

Jim Fuller: Yeah, most companies, I mean, I think I can only remember one company that said, "No, go pound sand," and that didn't turn out well.

Olga Torres: Yeah, I can see that.

Don Pearce: Yeah. I mean, even if, even if the statute of limitations has tolled they can still do the denied parties list. Well, I mean, there's precedent for that as well. And I'll tell you what, there isn't a CEO in this country that thinks they're going to go to jail because of an export control violation. But if any of them know anything about export controls, the thing that would keep them up at night would be a temporary denial order. So, for 180 days, you're on the denied party's list. That could be a death sentence depending on the company.

Olga Torres: Right? Yeah. I can see that.

Jim Fuller: I'm sorry. But, although it might have changed right, since I was handling the case, one of the first things that we found out about Far East Cable was, at the time, that they were supplying Tesla with their wiring harnesses. Now that this goes back to 2015, I don't know if they're doing that any longer or what reach into U.S. markets that they have. However, I would assume that if they don't have a reach in the U.S. market that they would like to have that reach and get as many customers as they could that as they can. Adverse actions by the Department of Commerce, doesn't bode, isn't the kind of publicity that they want.

Olga Torres: Yeah, no, that's right. That's interesting. It also makes me wonder whether in the next few months or years, we're going to continue seeing other parties like them, that were "assisting" ZTE in whatever they were doing and that they could for all I know be under investigation and we just haven't heard.

Jim Fuller: Well, there are, parties that have already been sanctioned, mostly on the entity list, that ZTE was not mentioned, but it was a factor. But their actions were so egregious, that it wasn't even bothered to be mentioned. But ZTE was forthcoming in what it had done, but they did not disclose. And Don and I talked about this. They said, "Look, we're going to disclose what we did, what we're responsible for. However, we're not going to disparage other companies, particularly Chinese companies, but other companies, we're only taking responsibility for ourselves." So, they provided the information on the, when they could because they destroyed a lot of records, but they provided the information on the pertinent violations and the transactions. But they were not forthcoming. They had a lot more information, but they also had a professional reputation. The Department of Justice and the Office Chief Counsel, they understood that. It wasn't a scorched earth policy by any means. We understood that they were cooperating and there was, despite, everybody goes, "Okay, there were two monitorships." Those monitorships came out of different circumstances.

Olga Torres: Yeah. So why did we have two monitorships? I mean, one was coming in from the BIS side and one from the DOJ and we discussed the DOJ last week. Is it, is this the only case that has had two monitorships? I can't remember.

Jim Fuller: Yes, yes. The reason for that, the first monitorship was the Department of Justice monitorship. But actually you could rightfully categorize it as the honorable Ed Kinkeade's monitorship. He was the federal judge in charge of it. And he's an old school, he's a really good judge. I've been in his courtroom many times. He's a really good judge but he is an America-first judge

in the truest sense, not politically at all, because he is quite nonpartisan. But he said, “What you did was so egregious, we're going to trust, but verify.” But the Commerce monitorship, was Wilbur Ross's idea and that's because ZTE had not followed through on what they said. And they had left people, key people, still in place. And that did not sit well with them. So, they said, “Okay, we don't have control over the DOJ monitorship, the judge’s monitorship. So, we're going to institute our own.” And they've done a phenomenal job.

I mean, both monitorships were hampered because they weren't under the control of the government. They were asked to do monitoring functions, but without the law enforcement tools or without any of the other tools that could have been used if it was a government entity. So, both of them did a tremendous job with what they had and both of them required very strict accountability. The DOJ monitorship is over, and the Commerce monitorship still is functioning, I think, shoot 2018. So, they've got six more years left.

Olga Torres: Very interesting. And it basically sounds to me like if you are a company under investigation, the more you try to conceal or you're not cooperating, don't be surprised if you get not just one, but potentially even two monitors. We have the precedent for that now. Very interesting.

So, because I have both of you on, if companies get, let's talk about investigations separately from let's say visits or outreach visits by OEE. So, let's talk, one is if a company is dealing with an investigation, right? And let's say we have voluntary self-disclosures that lead to something else or a referral to DOJ. What are the tips that you have for companies to be able to navigate OEE in terms of not getting into situations where the agency distrusts the party? And also on the outreach side, same thing. How should companies deal with, for example, unannounced OEE visits that are outreach visits? Whoever wants to take it, Jim, Don.

Don Pearce: Let me start with my rule of three. If a single agent comes to your door on a Friday afternoon at about two o'clock, talks to you for 10 minutes, and hands you a flyer for red flags. You have nothing to worry about. That was what we used to refer to as a “drive by,” “drive by outreach.” Probably, not only are you not under suspicion, but that agent will probably never remember that he did the outreach. If two agents show up, you should certainly be a little bit more concerned. However, in many cases, when Jim and I would go on travel we wanted to stay overnight. We had to be able to show that we had more work than just the one meeting with the attorney or with some company or with a source. So, we would stack a couple of outreaches around it. In some cases, , maybe those ones that we had planned didn't really wash up or didn't take

enough time, and so we just decided to drop by that. That can happen too. And again, probably not going to worry about it unless you confess to the Lindbergh kidnapping. And then if two or more agencies show up, so you have BIS, an FBI agent. Yeah, you should probably be concerned. You should really be concerned if you get all three, because let's just say that is a major work of coordination and, , not the usual game plan and the fact that they just happen to be in the neighborhood all at the same time. You might want to call your lawyer.

Olga Torres: We've had situations, we recently have one OEE/FBI, right. But I have had situations in the past where it's OEE, but then within a week or so FBI shows up, right. And they appear to be unrelated.

Don Pearce: But are they though?

Olga Torres: That's the question?

Don Pearce: That's the question you have to ask the client.

Olga Torres: Yeah, yeah.

Don Pearce: But if it's a counterintelligence investigation, then more than likely, you're going to see someone from the FBI show up. They also have the prime role for counterterrorism. So, depending on the commodity and the location of the end use/end user, you might see someone from CT taking a an interest. In fact, I think my first, run in with the FBI was I was assigned to the Joint Terrorism Task Force as their export controls guy. So, that's not unusual. And in my final part of my career, I was for two years, the liaison to FBI headquarters, they had a counter proliferation center that was multi-agency had representatives from various agencies. We would basically just get together and guide FBI agents through how export controls actually work or provide information on cases of interest from the field in, so that, so that they could kind of have the situational awareness to be able to make good decisions as to whether cases were counter intelligence or had some kind of a nexus that they might be interested in. I know Jim and I had many phone calls from that, from that desk phone that I had there.

Olga Torres: Thank you so much. both of you. I think this is a very interesting, topic that I feel like we didn't even get to cover more than 30%. I think enforcement is such a hot topic and also just a top priority for all the agencies. Thank you very much for being here and thanks to our listeners for tuning in. We'll bring you more of the Torres Talks Trade podcast very soon. Thank you.

Jim Fuller: Thank you.

Don Pearce: Thanks.

1201 Main St. Suite 1350, Dallas, TX 75202 • Phone: 214.295.8473 • Fax: 214.396.1583
1050 Connecticut Avenue NW, Suite 500, Washington, DC 20036 • Phone: 202.851.8200