Kate Kalmykov: Hi, everyone, and welcome to the Immigration Insights podcast presented to you by the Global Immigration and Compliance Group at Greenberg Traurig. My name is Kate Kalmykov and I am your host. I co-chair the Global Immigration Group here at Greenberg. And today, I am delighted to speak with you on a [00:00:30] very important topic: global mobility and global security. And I'm pleased to be joined today by Don Aviv, president of Interfor International. In this capacity, he oversees Interfor's day-to-day operations and investigations and security consulting. Don, can you introduce yourself, tell us a little bit about what Interfor does?

Don Aviv: Sure, absolutely. Kate, thanks for [00:01:00] having me. I'm looking forward to this session. As you mentioned, I run Interfor International. Interfor International is a 50-year-old business intelligence firm. We sit at the intersection of global security, investigations, and intelligence, helping multinational organizations manage risk as they expand and move their people around the world for a variety of business needs. As we know in today's environment, mobility is no longer just logistics and legal, [00:01:30] it's a lot about complex security and compliance challenges.

Kate Kalmykov: So let's delve right into that. And Don has a very unique perspective because he's also married to an immigration lawyer. So let's talk a little bit about the evolving global security landscape. Obviously, it seems that the world in different regions of the world is completely unstable. There's a lot of geopolitical tension and new regulations [00:02:00] are really shaping cross-border mobility from an immigration perspective. But while we're planning how to move people according to the laws of different countries, whether they're employees or they're C-suites or very important dignitaries, you're looking at it from a completely different perspective. Can you tell us a little bit about that?

Don Aviv: Absolutely. Everyone who's listening probably [00:02:30] acknowledges and recognizes that the world has entered an era of permanent volatility. Geopolitical risk is constant, it's not cyclical anymore, so we're dealing it from all angles. And as a company, our role is to give companies the foresight to anticipate that geopolitical shifts, protect their data, safeguard their people, whether they're executives relocating abroad, employees on assignment, or entire teams navigating crises.

Traditional borders [00:03:00] are blurring, as you well know. Regulatory and political borders are becoming in flux. So we're looking at challenges and risks that are uncorrelated and different than we did in the past. It's now more about dealing with sanctions and trade restrictions, data sovereignty. And when we look at mobility plans, we have to assess and analyze not just today's risks, but what may be coming down the pike in the coming months or election cycles.

Kate Kalmykov: Don, [00:03:30] let's delve into that a little bit deeper. One of the biggest risks that we see these days is related to data and information security. Obviously, we have a lot of people moving. We are still a global economy, and depending

on the jurisdiction that you're in, your data may be compromised. Certain governments, including our own, have the ability to take and confiscate electronic devices upon entry into [00:04:00] the country. What does that mean for those that have sensitive data, whether it's financial, legal, government, regulatory, how do you protect that?

Don Aviv: It's a great question and there's no easy answer, but we have to first start off by acknowledging that during relocations and mobility, data moves as much as people do, and relocations expose sensitive, personal, and more importantly, corporate data. So we have to take that into account. Encryption, [00:04:30] endpoint protection, secure file sharing must all be embedded to any plans or considerations. It is acknowledged and universally acknowledged that some countries like to steal US corporate data to get the competitive advantage to help their domestic businesses succeed in the global market. So we have to acknowledge that when you move personnel around the world, there is a new [00:05:00] level of sensitivity and a security requirement when it comes to their data.

We teach, and others need to teach, executives and their dependents about phishing and digital self-defense and how to use safe Wi-Fis, and more importantly than not these days, how to practice self-constraint when it comes to social media. Social media is the new kind of battlefront. The US government [00:05:30] is now, as you well know, evaluating social media accounts for inbound individuals and executives coming here and visitors. And the same thing goes for other countries. So they're using social media to determine what are your political leanings, what trade shows are you going to, what kind of business are you doing? And they're using that to manipulate the business environment. So we have to be very, very careful about it and we have to acknowledge that data is the new kind of password and it needs to be treated [00:06:00] like one.

Kate Kalmykov: So when we're counseling clients that are coming into the US, we're often telling them what their rights are at the border in terms of electronic devices. Of course, once they gain entry to the US, unless there's some kind of dark web or bad actors at play, there's no government interference, generally, in their devices without a warrant unless they're under investigation, correct? But that's not the case [00:06:30] overseas.

And many times when we're dealing with global mobility professionals, they are traveling to countries where, as you well noted, the country itself may be accessing their devices. So what are you telling clients that are traveling that have sensitive data in terms of do you recommend they travel with clean devices? Do you recommend they use, for example, Citrix to access their data rather than joining a Wi-Fi [00:07:00] network? What are concrete steps in a data protection plan that you recommend?

Don Aviv: First and foremost, every trip to a foreign country needs to be predicated with a risk assessment. We always advocate for conducting a comprehensive risk assessment into all moves. And this is important for a number of reasons. Primarily, you need to know the risks and concerns and vulnerabilities [00:07:30] that you face personally, physically, and from a security standpoint, when it comes to conducting business abroad or even coming here to the United States, for that matter. With that, you should identify what kind of risks your data faces when you travel abroad. There are countries that are aggressive in obtaining US data and US corporate secrets and vice versa. With that, there's a tiered approach. You have to understand [00:08:00] the layered protection.

So you decide what countries you would bring clean devices. And clean devices could be one-time use devices such as laptops and phones that you only use, and when you return, you hand them over to IT and have them wipe them or you embed protections on your actual hardware that could be used. It's a tiered approach. There are maybe two, three, or four countries that we would advocate using just one-time devices. And there are a number of countries that we would advocate using [00:08:30] enhanced protections on your devices that you can then embed and bring back into your corporate environments. But everything's predicated on a risk assessment, and with that, you should be empowered to decide what devices and what protections and proactive security layers you should employ for each trip.

Kate Kalmykov: So let's delve deeper into the risk assessment that you're preparing. Obviously, physical safety is also a concern in many jurisdictions, and as we have seen in the US, [00:09:00] even here for certain executives that become targets for certain movements. So how do you advise companies, their executives and personnel to protect themselves? And what kind of things are you doing? Do they differ by location? Do they differ by industry? Are there certain industries that are obviously more targeted than others?

Don Aviv: Absolutely. First and foremost, anything with cutting-edge technology, biotech, pharma. A lot of the [00:09:30] exciting advanced industries are more susceptible to data theft and IP theft, that goes without saying, but that doesn't not necessarily mean that they are more at risk. And you also have to take into account risk with your spouses and dependents as well if you are traveling with them. First of all, there's no off-the-shelf solutions. It's really catered to every specific movement where you're moving as a mobile [00:10:00] workforce and the risks embedded not just today, but you have to look down the pike as well in the future.

There are a number of different things that we would advocate for, creating policies and procedures from the corporate level, they should be adhered to. The biggest issues we have from an investigative standpoint is when someone travels to a country, there are policies and procedures that they should be following that their corporations embed them with, but they decide to cut corners, work around them. And with [00:10:30] that, that's typically when we

end up having issues. So the compliance framework, FCPA, AML, all these things, GDPR, come into play when it comes to what kind of policies and procedures you're embedding when you do travel. You're traveling with sensitive data. And then you're also at risk yourself physically.

We had to evacuate a number of people from Israel when the war started heating up. That's not something that most foreign companies planned to [00:11:00] have a concern about. They didn't think that Israel would be a country where you would have to evacuate from. That's just an example of the types of things that you need to think about wherever it is you're traveling.

Kate Kalmykov: And sometimes you may have to move employees because there's legal changes. About a month ago, there were significant changes introduced by the administration to the H-1B visa, making it significantly more expensive to sponsor employees in the United States for [00:11:30] the H-1B. And we're working with a number of employers who have global operations that are thinking about opening new hubs overseas to transfer employees that they previously would've sponsored for the H and had in the US to other hotspot locations like Dubai, Canada, London. So what do you recommend to employers who are embarking on a new program to mass-scale transfer employees to [00:12:00] a new hub?

Don Aviv: Visas are now being seen as geopolitical tools. Let's accept that reality. Visas are increasingly policy tools reflecting diplomatic relationships and national security policies. So when you have that backdrop, you need to understand that there are going to be new concerns, new risks, and new vulnerabilities facing your corporation wherever it is that you go. But there's also benefits, right? With changing policies comes new opportunity.

[00:12:30] So we know a number of clients who are taking what would be historically considered riskier moves to emerging markets or markets that are being opened up to their industries. So these are exciting times as well. But coordination early between immigration council and security must align early. This is the type of thing that we advocate for. It's no longer just talk to your immigration council, talk to your security council, and [00:13:00] just hope for the best. We're now seeing an integration between immigration council and intelligence services because that's really what's going to move the needle in increasing protections and security for your company.

Kate Kalmykov: And to sort of follow up on that, even when security perhaps is not an issue, getting a visa and getting into a country oftentimes could be. Before, you mentioned social media. The US absolutely checks social media when it's issuing visas, and there [00:13:30] have been a number of high-profile visa revocations initiated by the administration based on social media activity. We also may have clients who have been the subject of bad press or targeted campaigns, and now that impacts their ability to get visas, whether it's to the US or outside of the US

to other countries. Do you work with clients to clear up internet and social media history [00:14:00] to help remediate that?

Don Aviv: Absolutely. We have a PII removal program and a social media clearing program. We try our best. I would say there are a lot of services, platforms, and technologies out there that do this, and a lot of companies are very aggressive about it, but there are a couple of realities that we need to embrace. First and foremost, the internet never forgets. And I think we should all embrace that reality. If you write something, post something, tag something on your part of a discussion or a listserv [00:14:30] or some sort of blog post or whatever it is, just acknowledge and accept that there is or may be a record of that somewhere. So yes, I think it's very important to sanitize your platform. But from the US side, we live in a, quote-unquote, free society, so it's very hard for corporations to advocate or demand that their employees avoid political commentary or clean their social media histories, but it's a reality of the day.

[00:15:00] Just as inbound immigration is impacted by it, so is outbound. So we are seeing companies ask their employees, or encourage their employees, to clear their social media histories. But there's an added caveat here, and the reality is it's oftentimes not just what you say, it's what your friends say and what your family members say. We are seeing well-documented situations in which a prominent executive goes to country X or comes here and they think [00:15:30] that they're fine. They've never posted anything negative, they've never disparaged the government or a government official, but it turns out upon arrival that their cousin is a very far-left or very far-right individual who's well outspoken about a lot of topics that are deemed to be unsavory. And in those situations, it has impacted the executive coming to the United States or the executive going somewhere else.

I think the most important thing to do, or the biggest takeaway, [00:16:00] is to envision and map out the entirety of your social media platforms and the extent to what data bleeds out there and realize who is saying what in your world, what your kids are saying, what your spouses are saying, what they're doing on social media because that will impact. So if you know that beforehand, then you may decide not to go to a certain country or you may decide to delay a trip. But those are the types of things that need to be decided before you get on a plane. [00:16:30] And I think that's the critical takeaway. But yes, there is a lot that can be done to clear a lot of this out, but it's not an easy one and done, these are usually monthly engagements that take time.

Kate Kalmykov: And it sounds like something that in-house council and human resources obviously also need to be involved in, and where you have high-net-worth foreign nationals, whoever's managing their travel and their business interests as well. Sometimes we have clients [00:17:00] that also get caught up by relation, as you talked about, not so much for social media activity, but I'm thinking about recent sanctions that were issued initially under the Biden administration. A lot of family members may have had somebody who was

designated as a specially designated national and then that impacted their ability to travel to certain places, whether it was the US or Europe. Do you have any suggestions in that case on what they [00:17:30] can do?

Don Aviv: Well, work very, very closely with immigration council, work very, very closely with your HR departments and your attorneys, and also you're investigative and security consulting professionals because you need to know these things before you take the trip. You need to know where the sanctions have moved. You have to know where the problems may be, where the minefields are. There's not much you can do about a lot of these designations and about the PEP lists and all these different things that may impact you where and when you go [00:18:00] places, but knowing so beforehand gives you the power to decide what to avoid and where the potential pitfalls may be as you travel. And also, remember that more often than not, you may be traveling with dependents and spouses and then that creates a whole other dynamic. So consider their situations as well as you make these plans.

Kate Kalmykov: Absolutely. So let's talk about when everything goes wrong. You can do all of the planning in the world, [00:18:30] you can come up with a policy, you can identify risks, you can, from a business standpoint, decide to take a risk and decide to travel to a country that is perhaps unsafe or perhaps a safe country, but you're a target and you do actually become a target.

What is the way to handle a crisis? Do you have a security protocol that you follow? Is it customized and different in every situation? I know you and I have talked [00:19:00] a lot about this topic and you've told me before, the goal of security is to protect and not to retaliate or anything like that. So can you elaborate a little bit on that?

Don Aviv: Absolutely. Crisis readiness defines resilience. So it comes down to the planning and the procedures that you put in place before you go anywhere or do anything in life. Just as you would protect your home, just as you would protect your business, you need to think long and hard about [00:19:30] preparedness. But the issue is crises today are multidimensional. They're both physical, they're digital, they're reputational, and then oftentimes, psychological. So you need to plan for all of those items and concerns. Have evacuation plans, communication plans, various triggers in place that will indicate what you do next. And these are critical things that if you spend a couple of hours before you take a trip or plan for a trip, you can actually move the needle and [00:20:00] be significantly more prepared. But communication is key. We found during recent crises, when telecom goes down or you don't have access to communication, email goes down, you can't access your corporate email.

This is very concerning for a lot of travelers who are used to just looking at their phone and shooting out a message. But plan for the lack of communication, plan for little access to communication, plan for little access to banking and to finance [00:20:30] and put all those plans in place. What would you do if you

couldn't make this phone call? What would you do if you couldn't email? What would you do if you couldn't pull out money from an ATM? Have simple granular plans and then move forward from there, and then you'll be prepared for most crises. But think about it, talk about it, talk to the professionals about it, and see what your companies are implementing and supporting and how they're supporting you abroad.

Kate Kalmykov: It also seems like it might [00:21:00] be worthwhile to just even do a dry run if you're truly going to a risky place to be able to enact a scenario where everything goes wrong just so that you don't panic in the moment, right? That's a very common human emotion, but it's something that can cost time, cost security, and it's something that key executives who are in risky places just cannot afford.

Don Aviv: Absolutely. Freezing up in a crisis, not knowing what to do, [00:21:30] having a panic attack, reacting poorly is probably the worst response in a crisis. Maintaining a level head, being confident in your abilities, being confident in your procedures and plans does make the difference. And we see in all types of crises, whether it's a weather emergency, whether it's a business emergency, whether it's a geopolitical situation where you're all of a sudden suddenly caught in a war zone or caught between conflicting armies, [00:22:00] these are the types of situations where maintaining a level head and knowing that you have the ability to get through it is critical. So we always advocate, first and foremost, being calm, collected, and having a plan to get yourself out of that situation.

Kate Kalmykov: Let's talk a little bit about the future. What is the outlook? What's going to be the role of technology, policies, and do we see a world in which things really stabilize?

Don Aviv: [00:22:30] Well, I think we've already established that we're in an age of volatility, how we should embrace that volatility because it's not going to get any better anytime soon. But I think the future of mobility is data-driven, right? We have to be secure by design. It's predictive. I think artificial intelligence, quite frankly, will forecast or will have the ability to forecast emerging risks, automate routes, or even handle visas to a certain extent. I think you will see, and I don't know if that's [00:23:00] a popular thing to say to an immigration attorney, but I think AI will help improve mobility in general from a variety levels, whether it's granular, whether it's yourself personally, whether you're using ChatGPT or Gemini to help make decisions as to where you go, what routes you take, how to communicate locally, translations, there's a lot of improvements that are available to us.

But with that, we're going to [00:23:30] see more of a hybrid mobility workforce. But we have to expect that with an increase in the digital workforce, there will be additional vulnerabilities. The corporate security and the corporate intelligence and cybersecurity infrastructure becomes more attenuated, a little

bit more vulnerable as you are a solo person traveling to a different country and you're not in the brick and mortar corporate field office, or you're [00:24:00] working alone or working from home office, a lot of these things make things a little bit less stable, and a lot is left to you as an individual to navigate. So it could be a scarier time for some, but with that also comes opportunity. So if you're able to handle this next-generation outlook, then you will be more valuable as an employee.

Kate Kalmykov: And we know that governments are also [00:24:30] using AI. They're not only sharing data between agencies, but they're using AI to do backgrounds on people, to search for things of concern, to identify potential risks. And they're using it in law enforcement. And this is something that as immigration lawyers, we know it's being used by the government, it's being refined because it's probably in its infancy at this point. But we do believe that it is going to make [00:25:00] a huge impact, and different countries are using it already in different ways.

Don Aviv: Yeah, I would agree 100%. And I would add that I think we have to embrace the reality that you should not have an expectation of privacy. I know this is very hard for many coming from various Western countries where GDPR and all these privacy rights are so strong, even in the United States to a certain extent. But I think as long as you appreciate the reality that [00:25:30] privacy is not really where we want it to be to a certain extent, and that there is no real expectation of privacy at the borders which you are transiting, then you may be able to plan accordingly. As organizations continue to expand globally, security must evolve. You're going to have to ebb and flow with the winds of change when it comes to mobility. So I think that's something that if we embrace it as a global workforce, we'll do a lot better going forward.

Kate Kalmykov: [00:26:00] And in this age, unfortunately, we have seen a number of high-profile assassinations just over the course of the past year or two. And perhaps AI can also be used to really alert people in certain ways, whether it's not through official law enforcement, but if companies use it in a way where they can really profile people in their management that may be at risk, they can take certain proactive steps with companies [00:26:30] such as yours to protect themselves.

Don Aviv: Absolutely. We devote a significant amount of time, effort, and resources into developing these predictive risk platforms utilizing AI. So we're scraping the internet, the deep and dark web on a routine basis. We put our executives into a little bit of a protective digital bubble, and we're analyzing sentiment and anything negative about them that's being said, that's being discussed, [00:27:00] discussed about their companies into this little environment, and we're monitoring it 24 hours a day in a language-agnostic model.

I think AI is allowing us to do this in ways that we would never be able to do in the past. And it gives us almost a predictive concept or an early warning about threats coming down. And I think that can make the difference, right? When

you travel to a new environment and you're walking into a riskier environment, if you know that before you enter, [00:27:30] you'll do a lot better to either avoid it or to make plans that'll increase security. AI has been fantastic with that. It's not there yet, and it won't be for some time, but if it's used smartly, it can greatly help predict any of the emerging risks anywhere in the world.

Kate Kalmykov: And I think one of the takeaways from our discussion for me is that we, as immigration lawyers, as global mobility professionals, obviously, [00:28:00] we work all over the world. We do US immigration, but we also work with our network on outbound immigration everywhere. But it's not a one-dimensional type of practice. We have to necessarily work with security professionals, especially if we have people transferring to risky places like we just discussed. Getting policies in place is key.

Now we've been encountering a lot of raids in the US, a lot of investigations [00:28:30] of companies due to I-9 or employing unlawful immigrants and giving advice to companies that may be investigated. But if you take that idea and you apply it to global mobility, you should have a rapid response plan as we've been discussing, just like we do if a government agent shows up. Who are they? What agency are they from? What are they asking for? And it's the same thing related to immigration. Where are people going? [00:29:00] What are the risks? What are the ways to get them there? And once they get there, how do we keep them safe?

Don Aviv: Yeah, absolutely. It's all about planning. Spend your time and your effort planning and looking ahead and figuring out all the vulnerabilities, the risks as you put a mobile workforce out there, whether you're relocating a single executive or deploying entire teams abroad or inbound. It's all about preparation, transparency, adaptability is key in these [00:29:30] situations. And if you plan that before you step foot on a plane, I think you're going to do a lot better in the long run.

Kate Kalmykov: Thank you so much, Don, for joining us today. Your insights are really valuable. I really enjoyed chatting with you, and if there is a takeaway, I think preparation is key, as you said in this discussion, for planning and for protecting your workforce.

Don Aviv: Absolutely. Thank you so much for having me. It's been a pleasure, as always.

Kate Kalmykov: Thank you.