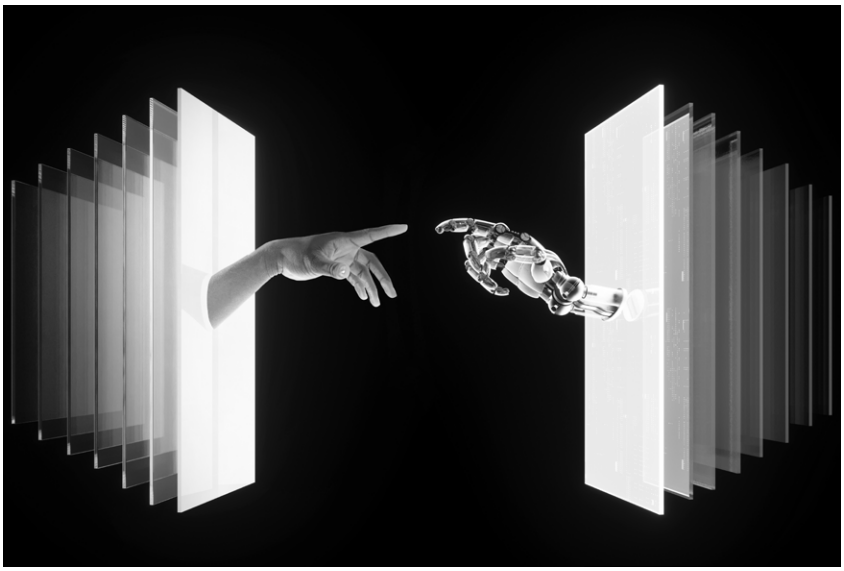

A&O SHEARMAN

THE TRUMP SESSIONS

Data, AI and cybersecurity – *what global businesses need to know about U.S. policy developments*

Welcome to the Trump sessions from A&O Shearman, where we explore the impact of U.S. policy developments on global business.

Our latest episode looks at data, artificial intelligence and cybersecurity.

Here, our partners explain how U.S. AI regulation is evolving, what multinationals are doing in response to the DOJ's new data transfer rule, how the President's executive orders are impacting the cyber risk landscape, and what tariffs mean for the development of U.S. data centers.

This podcast is a recording of a live webinar which took place on June 4, 2025.

FFION FLOCKHART

Hello everyone and welcome to today's briefing. My name is Ffion Flockhart, and I'll be your host for this, the fourth of our Trump Sessions, a regular series of conversations designed to help you navigate the new U.S. administration.

So, by way of introduction I'm global co-head of our cybersecurity practice, and I specialize in cyber risk management and cyber incident response.

Today we're going to be looking at the shifting policy landscape around data, AI and cybersecurity, and what opportunities and risks this dynamic environment raises for you.

I'm delighted to be joined today by three of the leading authorities in the U.S. market who are going to help me explore the latest developments.

So first we have Daren Orzechowski, one of the co-heads of our global technology practice based in Silicon Valley. Daren advises leading global tech companies on their strategic IP-, data- and technology-focused transactions and licensing agreements, and has handled matters relating to everything from cloud computing to drones, autonomous vehicles, semiconductors, and AI.

I'm also pleased to welcome Andrew Tannenbaum, my global co-head of our cybersecurity group. Andrew is based in New York and worked for more than two decades in financial services, technology, and also government, including the Department of Justice and the National Security Agency before joining a A&O Shearman at the beginning of this year.

Last but not least we have Dorina Yessios, who is the U.S. co-head of our energy, natural resources and infrastructure practice. Dorina has particular expertise in data centers, and she's been active in the sector for about a decade, advising sponsors and lenders on a variety of financing structures.

Right. Without further ado, Daren, Andrew, Dorina, welcome.

First, I'm going to come to you for your take on the key policy developments that our guests on this call need to be aware of, and then we can drill down into the detail.

So, Daren, perhaps I could come to you first How has U.S. policy changed under the Trump administration in relation to data, AI and cybersecurity, and what are the principal drivers of these shifts?

DAREN ORZECHOWSKI

Thanks Ffi, and thank you everyone for being here. We could probably fill way more than an hour talking about this topic, but we'll do our best to keep it tight and stay on schedule.

At a high level, when we look at what's going on with the federal government with respect to AI, and that's really where I focus – IP [and] AI transactions, and then we have synergies with our cyber and the data practice, which Andrew will touch on and is more expert in – we don't really have at the federal level an overarching AI law at this time. The federal government over the course of the last couple of years has taken a conservative approach in that they haven't passed AI-specific laws.

Instead, what they've done is, they've relied on existing laws, executive orders, and agency rulemaking. And this is not without precedent. I think for those of you that practice in the privacy area, we saw this where the federal government in the U.S. didn't really step in and then the states kind of stepped up. And that's happening again now – states like where I sit here in California passed a lot of legislation, and there's talk about addressing specific concerns with AI at the state level.

Now, the Biden administration didn't ignore [AI rulemaking]. What they did was they took us down a path with industry. Some of you may recall that in the summer of 2023 there was a big announcement – a lot of stakeholders from companies like Anthropic and Meta, Microsoft, [and] OpenAI got together with the administration and tried to develop principles for how we use AI, how we develop it, and they focused on safety, security, and trust. There was a lot of work that was being done to advance these objectives, which in all honesty were taking the U.S. on a path towards maybe adopting some of the principles that we see in legislation in other jurisdictions, like the EU AI Act.

Then the election happened, the Trump administration came in and [the President] very quickly issued an executive order entitled "Removing Barriers to American Leadership in AI", which undid a lot of the Biden administration's policies, and very specifically is trying to clear a path for AI to be developed and for it to be advanced without a lot of regulation.

And I think this trend is going to continue. I'll give you an example.

Fair use in the IP area is a very hot button issue. Can you take a set of data, can you then use that to train an AI tool, and is that a fair use or is it a copyright infringement?

This is being litigated in a lot of our courts, including in the northern District of California. And the U.S. Copyright Office did a report on AI and IP, specifically copyright, and the last instalment of that report came out in May. The Register of Copyrights at the Copyright Office said it is not clear that using data for training is a fair use.

This obviously is a threat to the AI companies and the people developing foundational models, and within a few days, the [Register of Copyrights, who is the] director of the Copyright Office, was fired by the Trump administration. So this is consistent with other actions showing that the administration is going clear a path for this technology.

FFION FLOCKHART

Thanks. Andrew, what's your view?

ANDREW TANNENBAUM

Thanks Ffi. So for cyber it's a little different. You can trace some similarities across administrations, even going back to the Bush administration.

So you look at the policies and you see similarities: improve the cybersecurity of critical infrastructure and federal government systems; protect against threats from foreign adversaries; promote information sharing; secure the supply chain.

Those have largely stayed the same. The regulatory approach shifted a little bit – it was largely sector driven, and for many years based on flexible frameworks like the NIST framework. The Biden administration proposed at least to pivot toward greater regulation, especially with software companies, proposing that they'd be liable for their vulnerabilities. But that never came to pass.

With Trump, we definitely expect less of a regulatory approach. One of the most watched, and perhaps more controversial, regulators in the last few years in cyber has been the SEC. It issued a cybersecurity disclosure rule in 2023, requiring more robust public disclosures from public companies, including within four days of determining that a cyber incident is material.

There was a lot of pushback from industry on that rule at the time, just in terms of having to publicly disclose that quickly when you're in the middle of responding to an incident. And some banking trade groups recently submitted a letter to the SEC asking to revisit that rule and raising some of those same arguments, so we'll see.

In terms of enforcement by the SEC, they've had their case against SolarWinds, which is a very closely watched case pursuing some novel theories, including for the first time against a Chief Information Security Officer for securities fraud related to their disclosures in the wake of a major attack.

Although that case is still going on, the new administration has not indicated it's going settle or drop the case [and] it's gone to summary judgment at this point. But that's the kind of case that the SEC is signaling it might not bring in the future.

They've reorganized their crypto and cyber unit, they've downsized it a little bit from about 50 to 30 staff. They've rebranded it "Cyber and emerging Technologies", and they've talked about some of the priorities that they're going to focus on: weeding out bad actors across emerging tech, and things that would affect the market for promoting innovation, like the theft of material non-public information through a cyber attack or brokerage account takeovers that lead to fraud.

They've said they're not looking to second-guess good faith reasonable decisions, like perhaps you could argue is at issue in SolarWinds, but more material misrepresentations or omissions. So we'll see, but it's a signal that they've sent out.

And last point, one other clear difference in relation to the Trump administration is how cyber is organized within the government.

You look particularly at the role of CISA, the Department of Homeland Security entity charged with protecting critical infrastructure and cyber. There's clearly been a reduction in the role of CISA, largely stemming from the Trump administration's views that the work they did around election security in 2020 and combating misinformation was politically driven.

That's certainly not how CISA sees it, but they've been a target for massive staff and budget cuts, which I think it's fair to say will limit to some extent how the government coordinates with the private sector, and potentially drive more responsibility to the states and the private sector.

FFION FLOCKHART

Looking ahead, where do you see some of the other biggest tensions, maybe taking the lead from you, Daren?

DAREN ORZECHOWSKI

There's no tension here, Ffi! I don't know what you're referring to. Everything's smooth.

In all seriousness, I think there are two areas where as legal advisors and counsellors, we see a lot of the tension and potential conflict and stress that's being caused. And the first is [in relation to the] trade wars and tariffs. I think technology, while there's a couple of countries that are at the forefront, it is definitely an industry that is spread out across nations, with everybody contributing and adding different pieces to the puzzle.

And then the other thing that's really hard, particularly for multinationals, is dealing with the patchwork of regulation relating to AI, whether it's with respect to AI tools and safety, data privacy, [or] things relating to the technology [itself].

It becomes very hard in the transactions we do, and in the way that we advise clients to bring products to market. I think different nations will use that as leverage in trade negotiations, and it's going to continue, I think for the time being, to get more confusing. Even here in the U.S. we had, in 2024, 45 states and territories introduce AI bills, with a number of them being passed.

And that's just continuing the patchwork. Now, one thing I will say that is interesting for folks outside the U.S. [is that] you probably heard that the Trump administration put forth a bill, the One Big Beautiful Bill, and there's a number of tax issues and other things that are covered in there.

But one thing that's particularly interesting for this discussion, is that [the administration] put in a passage that is seeking to preempt any state legislation that's focused on AI, again back to what I was saying before, to clear a path. So it's interesting to see what's going to happen – that could cause some clarity, but also create some further tension as it removes regulation.

This is an issue that the Senate's going to pick up now. It's passed in the House, so it's over to the Senate. And the Senate is supposedly going to look at this issue a little more closely.

FFION FLOCKHART

And maybe Dorina bringing you in on this as well, where do you see the biggest tensions?

DORINA YESSIOS

So looking at some of the tensions from more of an infrastructure perspective, particularly digital infrastructure, it's similar threads [in terms] of geopolitics and tariffs and the like. We have the administration in many respects encouraging investment into the U.S. – for example, we've had the United States Investment Accelerator program announced, supporting investments into the U.S. of a billion dollars minimum. At the same time, many are feeling that the cost of investing in the U.S. is getting higher, particularly when we have capex needs for investments.

A big focus of the tariff discussion has been around China, has been around the auto industry, but it is very much affecting a big part of my day-to-day, which is investments into data centers.

A lot of components for data centers are manufactured in the U.S., but there are quite a few that are manufactured outside the U.S. as well. And a lot of that is also not just standalone pieces – again, another similar issue to the auto industry – [but things that are] embedded in other products. A lot of [those products] are coming from China, and even though the government did announce a pause on the tariffs for semiconductors – one, it's a pause, and two, it's not taking into account all of these various other embedded pieces.

The challenge that further creates, is a distinction in who has deeper pockets in order to withstand some of these challenges as compared to some of the newer developers, smaller developers. The likes of Alphabet, Microsoft, Meta, Amazon, Oracle – they alone are expected to invest nearly a trillion in capex from 2023 to 2026.

FFION FLOCKHART

Thanks, Dorina. Maybe coming back to you, Andrew. One thing I know we are talking about to clients quite a lot at the moment in our practice is the DOJ's new data transfer rule. Looking at that from a U.S. perspective, but also an Asia perspective, could you give us an overview of the rule itself and then maybe explain what you are advising clients to do in response?

ANDREW TANNENBAUM

Yeah, absolutely. So, and this is, as Ffi says, really top of mind for a lot of clients.

It's a rule that was issued at the end of the Biden administration and I think a lot of people were assuming it would not be taken forward by the Trump administration.

Lots of rules were paused or rescinded, but in April, the Department of Justice came out and said they were enforcing this rule, it is in effect.

And it's really a national security rule – it sounds like data privacy, but it's driven from a national security perspective, and it regulates and prohibits certain data transactions between U.S. entities and entities or people in countries of concern.

And those countries of concern are China – including Hong Kong and Macau – Cuba, Iran, North Korea, Russia, and Venezuela. It's focused on sensitive personal data in bulk thresholds – whether it's financial data, health data, precise location data – and there are different thresholds for each of those, depending on their sensitivity, as to when they get covered by the regulation. Some U.S. government data is also covered.

And what [the rule] does is it prohibits a U.S. entity from engaging in a data brokerage transaction – basically licensing or selling the data – to an entity in a country of concern.

There are also certain transactions that [companies] have with vendors, employees, and/or investors in those countries of concern, that are prohibited unless they implement certain CISA-approved cybersecurity requirements to limit access to individuals in those countries.

There are a number of exemptions that apply, and a lot of the clients we talk to have a lot of activity that falls within those exemptions. There's exemptions for financial services, for example, and that's pretty broad and includes anything that's part of, or incident to, a financial service, as well as certain transactions within a corporate group like HR, payroll benefits, etc.

So the question is going to be: where are you using data potentially across borders into these countries that falls outside of what would be reasonably considered part of a financial service, for example? There's also an important requirement that any U.S. entity sharing this data with any non-U.S. entity has to have in its contracts a provision restricting the onward transfer of that data to the countries of concern.

So that's a pretty complex set of requirements, because it requires you to really map out where you think you might have some of these transactions. And what we're advising clients to do is to look at who their covered persons are, [and] try to really focus in on where those non-exempt activities might be. Data scientists, for example, research and development, ways that you're mining data or using data that's outside of traditional financial transactions. Look at the security controls for those transactions, and then review your contracts for those onward transfer restrictions.

By October you also have to have a compliance program in place: you have to have written policies and programs and attestations and training and audits and such. We're helping a lot of clients with that now because there's a lot packed in there.

FFION FLOCKHART

And it's that last piece, right, that's potentially very broad. Any data [that] goes to a service provider outside the U.S., you have to contractually provide that they don't pass it on. If I could stay with you, Andrew, and move on to maybe what impact U.S. policy developments and geopolitical tensions are having on the cyber risk landscape at the moment, because we've seen as a group a huge uptick in cyber incidents against clients.

ANDREW TANNENBAUM

I'd say the environment is unpredictable right now. Take ransomware as one of the major cyber threats. That has ebbed and flowed, and when LockBit, the major [ransomware] group was taken down last year, there was a bit of an ebb as that group was scattered.

We've seen now, I think, a lot of new groups come back, some of whom are unknown in terms of what their reputation is. If you're going end up paying a criminal for a decryption key or for suppressing data, you want to do a lot of things like work with law enforcement, but you [also] want know how reliable they are.

That's been scrambled a little bit and there are higher ransom demands, there are harassment techniques that are being used, there's the use of AI by threat actors.

We've seen that not just in social engineering and deepfakes and such, but even in their ability to look across large data sets that they've compromised and be able to summarize what they have, almost like in bulleted format like it comes from ChatGPT.

AI is enabling them to be faster and more aggressive. So you add on that the geopolitics, or the budget cuts... The most recent cuts from CISA, for example, USD500 million is the proposal, including USD144m that the Trump administration is proposing moving to increasing capacity at immigration detention facilities.

So that's a clear shift in priorities. And you put that along with high-profile firings at the NSA and Cyber Command and the National Security Council, [and it] certainly raises the possibility of new opportunities for threat actors.

FFION FLOCKHART

We've seen the similar thing with the FBI as well in terms of not being able necessarily to give the same proactive attention to companies and incidents as before.

Shifting a little bit to AI regulation, maybe Daren if you can give us your thoughts on how the Trump administration is approaching that and what we can expect from the president's AI Action Plan. How might that reshape the development and deployment of AI technologies?

DAREN ORZECHOWSKI

It's a good question Ffi. Back to what I was saying before, I think we're going to continue to see this trend of clearing a path for the technology to develop.

As far as investment is concerned, I think because this is such a rapidly developing area, there's a little bit of an element where we're flying the plane and building it at the same time.

It's just moving that quickly so it becomes a bit of a challenge. The AI Action Plan was something that was referenced in the initial executive order when the administration came into power. And then they put some thoughts out for public comment.

That public comment period ended at the end of April. They received more than 10,000 comments and all kinds of input was shared.

Picking up on some of the policies of the first Trump administration, where I think they were going look at – in terms of developing American AI capability – research investment, using federal AI computing power and other resources, setting AI technical standards, and then building out our workforce.

I think there's been a lot of talk about bringing stuff back to America, [but] whether we've up-skilled [the number of people we need] to do it is another discussion. And then an interesting piece that's relevant to this discussion is engaging with international allies and maybe some harmonization around AI.

So all these things are in the mix, these comments are now in, we'll see over the summer some follow up on that in terms of how we should steer this.

And one of the things that's really cool about working at a platform like A&O Shearman is that we can touch on many geographies. Even on this call we all have different practices but they're all interconnected.

As AI becomes more of a service model, the premium on things like what Dorina does with data centers, and then the things that the rest of us do with the technology and the data that's in that, become so important.

I think we're going to see a lot of focus on data centers. And this was kicked off earlier in the year when the President got up with leaders from SoftBank and OpenAI and Oracle and said, "We're going to get investment of about USD500 billion into AI infrastructure." And that's why I think it's going to start with data centers.

FFION FLOCKHART

That's the perfect time to bring you in Dorina. Obviously, the Trump administration wants to improve U.S. data center infrastructure, and we've seen some headline announcements in that space over the last few months. What are you hearing from your clients? And how are tariffs and shifts in energy policy affecting decisions around U.S. market entry or expansion?

DORINA YESSIOS

It's interesting. This investment has been going on for a while, and it's been an area that government policy hasn't focused on as much, directly.

The regulatory environment has been more [focused] around semiconductors and making sure that we keep the technology here in the U.S.

The boom of AI actually breathed new life into data center development in the U.S. There was a feeling that the market was getting saturated, and with COVID, we all of a sudden saw this huge resurgence in the need for power. And that's where, again, we're finding some challenges with the policies of the [Trump] administration because we need power.

Then, the question is, where is that power source going to come from? In many respects, renewables are falling in disfavor. The Big Beautiful Bill very clearly [attacks] some of the Inflation Reduction Act features that have made U.S. renewable investment very attractive, not only to U.S. investors, but also a lot of foreign investors.

And that's one of the key focuses as well: why should anybody who's not a U.S.-owned company be benefiting from some of the tax credits and the like?

Nonetheless, I do expect that we will see continued investment in renewables. It's too important to the policies of some of the hyperscalers and the cloud providers.

They require so much power source for their businesses, including their data centers, and it's a key feature of their proposition. So I do expect, notwithstanding those hurdles, that we will continue to see development of renewable power, maybe recasting some of the models and how it's being funded from [an] equity and debt [perspective].

The other interesting feature when you listen to the current administration is that nuclear is going to be key to powering data centers. This comes after several decades of no real investment in nuclear [in the U.S.], and in fact we've seen U.S. companies finding more success in investing in nuclear outside the U.S.

So there does seem a real push to bring that back. But again, many hurdles through government policies, and even some of the state policies. Just yesterday Meta announced – and the details are very light – an arrangement with Constellation Energy to benefit from Constellation Energy's nuclear power plant in Illinois. It's supposed to be a 20-year deal, and that is to service Meta's businesses, and particularly its data centers.

And all of the major hyperscale cloud providers have announced one form or another of nuclear arrangements, whether they're making equity investments in developers or PPA [power purchase agreements] type arrangements. So it's definitely here to stay.

The regulatory environment will need to start changing to support it, particularly as small modular reactors are considered the key way to fuel data centers.

And then finally Ffi to close it out, gas. Gas was a bad word for a while. We're certainly seeing a lot more building of new power plants, and also refurbishing existing power plants and really seeing that as a source.

Texas has become the third largest state for data center development, for obvious reasons given their gas supply, and so I expect that that will continue to be important.

ANDREW TANNENBAUM

Can I just draw a connection there? If nuclear power is the answer to the AI data center power need, and we're going greatly expand nuclear power, talk about critical infrastructure that needs protecting from cyber attacks, right? So it just shows how all these issues are interrelated and create potential vulnerabilities as well.

DAREN ORZECHOWSKI

Andrew, your point's a great one because I think from a technology innovator perspective, as you scale these things up and you build it, you want to create a bottleneck because that's your opportunity for where you can monetize and take advantage.

But with that centralization, for a lot of what you and Ffi look at, Andrew, that creates more risk.

If we're using the AI for automated decisioning, that presents a whole new layer of risks that really weren't exactly present in earlier types of this technology.

Ffl's question I think is really a good one, too, as we deal with policy shifts and tariffs and stuff like that.

A lot of what Dorina was saying about how we bring these things together, and what I was saying about the fact that technology is so interconnected around the world, I don't think it's easy to take an isolationist view.

Semiconductors is a great example. We need chips to basically power this. Even as you move towards an AI-as-a-service type model, what's the cost going to be for a device [in a world of higher tariffs]? What's the cost going to be for a server rack that is going to sit in these very large data centers that Dorina is helping to finance and build?

You have to think of these things as you bring all the pieces of the puzzle together. It's very complicated, and it's only going to get more complicated.

FFION FLOCKHART

I know we're very close to time, but there's one question that would be great to cover off, but very briefly. Daren, how is what we've discussed impacting the M&A landscape?

DAREN ORZECHOWSKI

Every technology has its own set of diligence questions and things that you have to dig in on. Dorina was talking about power before, and 10 years ago you weren't really pulling all the strings to trace back [to] where are you going to get the power from?

Now, that's really important in terms of making the engine go, whether we're doing M&A deals or we're doing joint ventures.

I think whether you're doing M&A or VC [venture capital] or growth equity, there's a lot more scrutiny on where the money is coming from, too. So we have a lot of foreign direct investment, a lot of CFIUS issues, that are coming into play. Who's getting access to the technology? So that's going to continue to be an issue.

And really understanding the technology [is another key consideration]. A lot of our M&A deals get done using reps and warranties insurance. The insurers are still trying to figure out the risks around generative AI. So really pinning down a target, and understanding is what you're doing really generative AI or is it different machine learning strategies, or is it a souped-up search function, [is] really important. Because then it might impact you when you go to do the insurance.

And then, again, a healthy dose of privacy, cyber, intellectual property – really understanding all the elements of the product and the data that it's using is going to be key.

DORINA YESSIOS

Ffi, just to add that in addition to some of these due diligence "inside" questions, it also just creates valuation questions more generally, both because of the issues that Daren is identifying, but [also because] some of the uncertainty around the regulatory environment makes it hard to understand what the capex costs are going to be.

DAREN ORZECHOWSKI

It's a very good point that you raise. Valuations can swing a lot. Just like some of those due diligence results will inform your drafting – and we're already seeing bespoke and targeted reps and warranties – you're also seeing a lot more provisions that are coming into play around budgeting, adjustments for financials and purchase prices and things like that, based on these uncertainties.

DORINA YESSIOS

And you have a lot of different players looking at the assets as well, which is another interesting factor. The valuations can be different if you're a more traditional private equity firm or looking at things from more of a real estate perspective, and so something that's attractive to one may not be to the other. And that plays into how the market continues to evolve.

FFION FLOCKHART

We'll take a question we've got from the audience, and this is to Andrew. Can you talk a little bit more about the mandatory compliance programs you mentioned in relation to the DOJ rule that need to be in place by October, and is that requirement mandatory for all U.S. companies?

ANDREW TANNENBAUM

So briefly, it's not required for all U.S. companies. It's required for any U.S. companies engaging in any restricted transactions under the rule. Now, of course, the key thing there is to know whether you're engaging in any of those restricted transactions. Because what you don't want to happen is [to not] have a compliance program, and then you find out later that you were engaging in those transactions and you're in violation of the rule and you didn't have a program in place, or you didn't take reasonable steps to assess your compliance.

So that's why it's really important upfront to identify those transactions. And if you do have them, the elements of the program are annual risk assessments, written policies, procedures, controls, vendor management, training, annual certifications and audits, as well as record retention. So there's a fair number of elements to the program.

FFION FLOCKHART

So final thoughts to wrap up. Maybe if you can give us your sense in one or two sentences, what are the key things to take away in this area? Maybe I'll start with you, Dorina.

DORINA YESSIOS

It's a very dynamic space and again, I've historically always looked at it from the infrastructure side of things.

I do think that we will continue to see strong investment, and it'll be a question of how we manage these risks and work together with the clients to understand them. That's the key.

FFION FLOCKHART

Thank you. Daren?

DAREN ORZECHOWSKI

I think the only thing certain is uncertainty right now, and I think that's part of the stress, the fun and excitement of working in the technology sector Ffi.

We're presented with a lot of puzzles and challenges and we work through these hard issues with clients. The important thing is to analyze each situation, making sure you're bringing in a very broad team with technology support, legal support, accounting support, a lot of diverse inputs brought into it to get your projects done efficiently.

FFION FLOCKHART

Thank you. Andrew?

ANDREW TANNENBAUM

We're here talking from a U.S. policy perspective, but what's clear is these are all globally connected issues and bringing a global team and global expertise to that is really important.
And there are opportunities and risks and vulnerabilities, and that's what everybody is trying to find: the right balance in terms of how to use or rely on these technologies and not be vulnerable to the risk.
As Daren says, it is certainly not boring, that's for sure.

FFION FLOCKHART

Definitely. Well, thank you so much. Unfortunately, that's all we have time for today. A big thank you to Daren, Dorina and Andrew for your insights, and thank you all for joining. We hope you can make the next session, so look out for the invitation in your inboxes.