CYBER SIP™

Barclay Damon Live Presents *Cyber Sip™*
Season 4, Episode 5: "Essentials for AI-Ready Data Centers," With Michael Kurzer

Host: **Kevin Szczepanski,** Barclay Damon

[Kevin Szczepanski]: Hey, everyone. Welcome back. Driven by AI-ready cloud infrastructure, the market cap for global data center construction is already estimated at $250 billion—billion with a "B"—and it's set to double in less than 10 years, so it should reach a half $1 trillion by 2034. Here to talk to us about what may be a new topic to many of us, about the legal essentials for building and operating AI-ready data centers, is Michael Kurzer. Michael is a partner at Vinson & Elkins and leader of the firm's Technology, Transactions & Intellectual Property Group. Michael, welcome to *Cyber Sip*.

[Michael Kurzer]: Thank you. Kevin. It is a pleasure to be here on *Cyber Sip*. I watched probably most of your podcasts to date to get a sense of things, and great stuff. Happy to have a chance to join.

[Kevin]: Well, we are very happy to have you. Well, let's start, and let's assume that there are many of our listeners and viewers who haven't grappled with the concept of the data center. So what is a data center, and why is it important to have an AI-ready one?

[Michael]: Right. So a data center is, it could be a warehouse, a number of servers, computers, technology in one place. And that place is the data center. How do you define that? It could be cloud infrastructure. It could be a lease of space where you have computers shared with others. They call that, you know, either co-management, co-lease, co-location and then there are other, there's sort of everything in between. They're hybrid models where you're mixing your servers and other servers, but at a high-level a data center is a is a room with computers in it.

[Kevin]: So there are three options. You alluded to a couple of them there, Michael. You could build one. You could lease one. You can license one. Walk us through the pros and cons of each. And what trends are you seeing out there in the market today?

[Michael]: Sure. So, let's start with building. So building is ... can be quite an involved process. But it's not unlike the process for building a factory or refinery or a warehouse or large real estate or office project. It's... it involves the construction of a building and, with the added complication of acquiring all the equipment to be in the building and then maintaining the temperature and the power of the facilities in order to operate that, that equipment. So, construction just, you know, in general, that's something where typically there's, a contractor that's involved that's assisting with that construction process. It may take a year more or more. It may take a considerable amount of time in order to get your data center into operation when you're constructing. Let's talk about a lease here. A lease would be there's already a facility or a building at least in place somewhere. That place may already have servers that others are using, or it may be completely empty. Or it may not even be built yet. And you're signing a lease for something that somebody else is constructing. It includes the same terms that you might have in any lease of real estate, plus all of the technical considerations that come with the use or operation of the equipment in the space. So you may lease the servers, you may own the servers. So there's an in each point, you may own the HVAC equipment. You may lease HVAC equipment that would be used to heat or cool those servers. So there are again options all the way in between on the lease as to what component you're leasing and what component you are... that you that you own in are providing into the into the facility. And then the last option might be, we call renting or cloud infrastructure. And this is... this could be as simple as a log in. Somebody else out there has gone through all the effort of building and placing their servers into a building somewhere, or maybe in many places, and have set up through virtual software a platform that connects that... all of those facilities into one place where you might access and use them and on your end, you can make that look however you want. You could make it look as if you're looking at computers, servers, folders, or as simple as, you're logging in as if you're using, you know, a login on your desktop computer, and anywhere in between.

[Kevin]: So I want to give our listeners, our viewers, a sense of the complexity of this operation, Michael. So I imagine you've got... when you're dealing with AI-intensive, computing, there are a lot of demands for power, servers, software. Can you talk to us about some of the issues and challenges that a client might confront in dealing with those issues?

[Michael]: Yes. So data centers obviously been around for a long, a long time. You know, I say so... you know, not to date myself, but, definitely worked on those agreements for my entire career, more than 20 years. And AI has been around at least as long as that and earlier that, AI has been around in the '60s and the '70s. The two coming together really is, I would point to the developments with respect to Open AI, ChatGPT and those developments that use Nvidia's graphics processing units. These are processing units that gamers used to use in their...to improve the speed and performance of their video games. Those all sort of came together when, ChatGPT was released and people started to recognize that the AI revolution was here. With respect to data centers, data centers had already been using these Nvidia processor chips that are used for AI. They've been using them for a few years or earlier because the crypto boom had preceded that. And crypto mining—the effort of searching for and looking for, you know, free crypto by doing the math calculations of, for example, a bitcoin, that process was computer intensive and required essentially the same processors and equipment that ultimately have become part of a generative AI or a data center. So, what you have is now you have two drivers of data centers. You still have the crypto piece, which still exists. It's still out there. People are still mining crypto. This, you know, power requirements aside as to how valuable it is to mine. And now on top of that, they're also doing AI...generative AI in data centers or offering up platforms that allow for chat bots or agenetic AI through a data center facility. So both of those are occurring at the same time. So you have, what appears at least from the beginning of this year, if you look at press releases, articles, a lot of, proposals and discussions surrounding investment in data center infrastructure. You have that. And then you had, around a month ago now, DeepSeek coming out, which is an innovation and software that was somewhat unexpected in its in its arrival. But the concerns that come around that are whether or not the innovations in improving the efficiency of the operation of AI through software will then somehow mitigate and reduce the need for AI, you know, true, heavy hardware AI-intensive resources in a data center. So, you know, these are... there's sort of competing things that are happening out there in the market. One will that... will there be less need because of these innovations or will there be more need? So there's some debate somewhat out there in that regard.

[Kevin]: And, Michael, I know it's probably too early to tell, but I know that these AI-ready data centers require the so-called sophisticated chips manufactured chiefly by Nvidia. Nvidia today, some estimate has an 80% market share. And you touched on DeepSeek and again, maybe too early to tell. But if you were predicting or offering a prediction, what impact do you think DeepSeek's innovation, the R1 AI model, what impact will that have on the cost, the investment cost of a business in setting up a data center?

[Michael]: Yeah, I think, the actual cost of a data center may not change. I think the question will be whether or not the company needs as much support from a data center. So either if you're under a true cloud model, you may use... you may be able to use less resources or you ... there's so there's been concern that somehow that the efficiencies gained will then allow data center projects to be canceled or set aside because of, because you could use, for example, processors that are not as high end as these Nvidia AI chips or the latest and greatest chips. My personal opinion, setting aside again, this is all sort of conjecture on my part, is that development is happening, happening very fast, that any software efficiencies will be...just for example, DeepSeek is open source. Anyone out there in the market can see those innovations and can implement those and those innovations, they're being studied as we speak. And all of those in my mind will be the new baseline. They'll just be incorporated into the market and the ever-onward demand for faster processing, more demand for use of AI, and more context. All of that continues. And it's just it one does not stop the other in my mind. So when there's concern about data center projects being canceled, in that sense, probably in my mind, that's a very temporary situation, because I think that it's still in the in the long run, demand for AI seems to be, completely on the upswing.

[Kevin]: Right. Not, I don't think that's on the wane. Not going away anytime soon. Which begs the question, how does an organization struggle to comply with all of the labyrinth of federal, state, international laws that may implicate an AI data center? So let's turn to that now, Michael. What challenges does a business face in compliance, we have privacy, cybersecurity, state, federal, international laws? Walk us through that. And, I really want to, please feel free to drill down as deeply as you like, because I think this is the question that you and I focus on and that that keeps a lot of general counsel up at night.

[Michael]: Right. So, so you mentioned cybersecurity. So just, putting it into context: when you're putting your data in a data center, all of your, you know, you're in a sense, somewhat outsourcing. If it's somebody else's data center, if it's your own data center, you're going to have to provide your own protections. If you're allowing ...if you're taking in customer data and you're using it in your data center...all ...everything that would have already applied had that been in your own computer and on your own desktop, is now applicable to this data center. If you're considering those issues. And so it's everything, with respect to cybersecurity in a data center, you're going to have to have physical security. If it's a... constructed building, you don't want somebody going in there and accessing and taking the servers. And you're going to have to have full cybersecurity, just as you would in any other business operation. And the laws, the regulations that are applicable to you don't change just because you put the data in a data center. And that has several implications certainly in the data space. One might be that we... frequently comes up is cross-border transfers of data. Where do you locate that data center? A lot of the development of data centers you see in the news is, people are talking about building them locally. I mean, that that has benefits for efficiency and speed, and transfer of data, but also with respect to compliance with the law. If you don't have to send your data very far, and certainly across border to another country, that simplifies your requirements for compliance. If you are sending it across border, there's a lot of things you have to be concerned about. And in fact, some jurisdictions that we deal with have laws that are so restrictive that you cannot transfer your data outside of that jurisdiction absent some very specific exemption or exception. The GDPR, which we interacted with, in Europe, they have specific requirements that they have in place to send data outside of Europe and into the US. In particular, we have, we have a framework in place that, well, our third or I guess is I think it's our third iteration of a framework, that's in place... that could go away tomorrow if there's an action brought before the court in Europe. One of the other things that we do in that case is to have standard contractual clauses to comply redundantly with, not only with, the framework for transferring of data, but with having in place all of the protections, the idea behind the standard contractual clause is to capture in a contract all of the requirements that would have been required had had everything stayed in Europe. So those requirements can be onerous, and they require agreements and to put in place. So those are considerations that, you know, may, you know, you may need to think about those immediately at the point that you're setting up your data center, because the use model certainly could subject you to a lot of regulation.

[Kevin]: I'm thinking of different types of provisions that might come into play. I wanted to ask you about that, Michael. I mean, off the top of my head, I'm thinking... information security addenda, indemnification insurance, procurement. And across the panoply of vendors you're dealing with, we've got hardware, software, AI. So how important is it to make sure that these provisions, these protections are enshrined in all of the various agreements that you have?

[Michael]: Of course. Of course it's very important, critical. Just to give a, a little sense of that. So in… we talked about the construction, the lease or the rental model of a data center. All those different models can put you in a different position with respect to your ultimate customer. You could have service providers who are providing you services on the back end, maybe everything, including your cloud, the cloud infrastructure. All of those pieces could be provided to perhaps to you as a middleman providing services out to others, or perhaps as the end user. I think it's rare that anyone these days is completely an end user. There's usually somebody else downstream. Even as lawyers, we are servicing clients. And so you have to connect the dots between the upstream pieces and, and the downstream pieces. And that part is critical. So if your customer requires security at a certain level, and that customer could be, for example, a defense contractor or a government, and you will then need to make sure that all of the providers in the back end that are providing services that then go into that customer's, offering are covered, are covered off, so that that data security, information security is a huge piece in that puzzle, you know, use of…transferring of the data, use of data, protection of confidential information, all of those pieces. And then on top of that, service requirements for operational requirements, whatever is demanded ultimately at… that you are providing out to the world, you need to make sure that you have accounted for that in your agreements.

[Kevin]: You made me think of a more general subject, and I want to run it by you to get your thoughts. There are sometimes, especially with SMB, small to medium-sized businesses will say, well, you know, I'm not a government contractor. I'm not regulated by this particular statute or rule. And so, Kevin, I don't have to comply with this. I can just fly under the radar. Right. So have you ever had that question asked of you? And what's your best pitch for why a company that isn't technically subject to the rules and regulations should take care to comply anyway?

[Michael]: Right. That's very it's very common. I always see that is somebody says well I don't do business in Europe or I'm all in the US. So why do, I don't care about the GDPR, I don't care, you know, I don't want to deal with any of that. And the answer is have you looked at have you, have you looked at the entirety of how you're operating and, and who downstream is using what you're providing… and what are you committing to in terms of services. So it may be that you can write an agreement for your downstream customers that can somewhat shield you of liability if you ever… if you truly do not touch those pieces, whether they be taking data from people in Europe or doing government contract work, or all of those things that we know are highly regulated… or providing securities to the, you know, subject to regulation or the SEC. If it's possible and I and I'm, you know, definitely you need to think about it, but maybe there's a way to sort of limit your liability and limit the scope of what your obligations are in that contract. If your customers don't let you do that, then you hundred percent need to be aware of what it is that they are doing and what the laws are. And what you're getting yourself into. And that's where they do need to be knowledgeable. And they probably should be knowledgeable either way because they need to know how to say we're not doing that thing. But, but yeah, I don't think anyone can put their head in the sand and say, I'd like to simplify things by not caring about anything, but, you know, what's in these four walls? It's just not possible in today's world.

[Kevin]: Similar question, Michael. What do we do with the client who comes to us says, well, all of my data is in the cloud. I'm using a cloud-based service provider, so I don't need to worry about specific physical, electronic, and legal safeguards. That's all taken care of by the cloud service provider.

[Michael]: Yeah, I think that the answer is, is that you don't, absolve yourself of any legal or regulatory requirement as a result of putting data in the cloud. It is merely putting your data in a server somewhere else. And I think, I think when people are saying that what they're looking at is, well, don't I get the protections for Amazon or the, the web services provider is saying, you know, oh, you're protected. Your data is solid. Well, I'm willing to go with them on that and say, let's read and see what they offer and let's see what they, what the agreement actually says in that regard. And let's see what it says they don't offer and what and what you might be able to look, you know, what will they indemnify for. What will they not indemnify for now? How comfortable do you feel after reading and looking at these provisions as to whether or not you also need to similarly limit your liability downstream from that or reassess your insurance limits or coverage as a result of knowing what the actual contract says. So I think when people say that they're saying that just imagining I've gone to a blue-chip provider, therefore I don't need to look very carefully. And that's obviously not the case.

[Kevin]: Both things can be true, right. You've gone to a blue-chip provider. You shouldn't assume that all of the protections are state of the art. They might be. But if something goes wrong, you're going to be responsible. And you may or may not need to shift that risk back on to the blue-chip service provider. But whether you can or you can't, you your organization will be on the front line with any third parties making claims or any regulator that may be investigating.

[Michael]: Right. Yeah. And what I mean, talking back in the data privacy in the security space, obviously incident response and negotiating those provisions obviously that… when you look at where things have sort of shaken out in the last several years, there's all sorts of instances where someone gets a letter from a vendor that says, we had a data breach somewhere out there. Now, you may have to then notify your downstream customers. All of the pieces that can be in place, I mean, you could have one obligation that says they don't need to tell you for three days that they've had an incident, and you've already agreed that you're going to tell somebody else in a shorter period of time. Right. And all of these things have to be thought through and considered at the time that you're setting up agreements on the back end and on the front end. And, the other thing I often notice is from the blue chip providers is that sometimes they put these things at hyperlinks where they can change the terms, even though you might have contractually agreed at the outset, if they can change it on the back end and you don't have the ability to change that same provision going out at the same, … or notice of it in order to make that change going out, you know, that's another issue that you have to be acutely aware of.

[Kevin]: Yeah, I think it's problematic because if there is an incident and you are in a discussion or you're subject to an investigation or regulatory investigation, they're going to ask those questions. And if too many of your answers are "it's in the cloud" or "we trusted this entity or that entity," you're not putting your best foot forward. And I think a lot of businesses out there, as much as I thought they didn't—like a lot of businesses out there, are under the misimpression that you set it and forget it. If it's AWS, you're good to go. If it's Microsoft, you needn't worry. And that's just not the case.

[Michael]: Right. And at the actual, you know, at the level now where others are building data centers, where they're putting their own servers in place, you have an industry, you know, an industry that really sort of grew up within…from the lawyer standpoint, from the real estate practice, where they were not at all aware of data privacy or security issues. And so they do an agreement at the outset of the creation in the offering of these services with the a paragraph, you know, they will comply with data security laws. Something along those lines. I think one thing that's sort of becoming more clear now is that there are multiple, functional sets of skills that lawyers need to have in order to work in this space and that it's not just simply a lease agreement. You know, something that that are more akin to a regular real estate contract.

[Kevin]: Right. Bring your data security and technology lawyer into the process as soon as possible. I remember in the old days, because in my other life, I'm an insurance coverage lawyer. The deal would be… getting signed in 20 minutes, and we get the call from the partner on the deal team saying, hey, can you look at these insurance provisions? And of course, it's just not enough time to try to make a dent in it. And I think what you're saying, applies equally. And so that's great advice. You've got to have your cybersecurity professionals in early and embedding that data protection, data privacy, data security at every stage of the project. Well, we are near the end of our time and I want to be respectful of yours. But before we go, I wanted to ask you very open-ended question. You're sitting here as a data center lawyer extraordinaire, among many other things. But if we could pick your brain and say, Michael, what are you seeing? What's coming along in the next 12 to 18 months, what changes do you envision? What challenges do you see? What would you say?

[Michael]: Yeah, I think that there will be a number of challenges, but, for companies, I think that incorporating AI and the use of AI into their businesses are challenges that will certainly go beyond even these next 18 months. But like, we can already see it as lawyers incorporating AI into our activities. This is happening. It's happening in every industry. And, that may lead to things, whether it's fewer employees or it may lead to more employees who have to manage the flow of the AI. But it's definitely causing a lot of disruption, dislocation, need for lawyers to look at contracts and review things that never would have been an issue before. But now are. Agenetic AI is becoming a hot issue at the beginning of the year. You know, that's something that could disrupt the entire software licensing model, which is that if a robot can use the software ten times faster than a human, then you don't need ten human login licenses for that software. You just need one… that it or it could be 100 to 1. But those are issues that are, that are facing software companies as a result of the adoption, mass adoption of AI. And, so that's just one issue of many that I expect will shake out over the next 18 months.

[Kevin]: I think you just scratched the surface, and I appreciate it. Michael, thanks for coming on to talk about AI data centers. I think for some in our audience, this topic may be old hat, but for many of us it's just coming over the horizon. And I think, our… folks are struggling to get their arms around what they need to do. Why and how do they protect their business and their data from all of the challenges that we read about every day in the newspaper?

[Michael]: Okay. Thank you. Kevin, I appreciate the opportunity.

[Kevin]: I think I just dated myself by saying, read the newspaper. I feel my children looked at me. "You don't read the newspaper…"

[Michael]: …you can read it on your on your phone, I guess.

[Kevin]: Okay. That's right. You saved me. Well, Michael Kurzer, thanks again for joining us. We appreciate it. And thanks to all of you for joining us. We will be back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. Like, follow, share, and continue to listen.

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied.

Barclay Damon Live *podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of* Barclay Damon Live *programming is the audio file. Thanks for listening.*