

2022 Trends for Technology Transactions

January 13, 2022

Announcer:

Welcome to Mayer Brown's Tech Talks Podcast. Each podcast is designed to provide insights on legal issues relating to technology transactions and keep you up to date on the latest trends in data, digital, outsourcing and software, by drawing on the perspectives of practitioners who have executed technology transactions around the world. You can subscribe to this series on all major podcasting platforms. We hope you enjoy the program.

Julian Dibbell:

Hello and welcome to season three of our Tech Talks Podcast. Our topic for today's season-opening episode: top trends for technology transactions in the year 2022.

I'm your host, Julian Dibbell. I am a senior associate in Mayor Brown's Technology Transactions practice. I'm joined today by my colleagues Marina Aronchik, Joe Pennell, Vivek Mohan, Brad Peterson and Rohith George.

Marina, Joe, Brad, and Rohith are partners in our Technology Transactions practice, and Vivek is a partner in the Cybersecurity & Data Privacy practice.

We have brought this team together for a look at the year ahead, but like any discussion about where things are heading, this one is very much informed by where we've been. The last two years have been, if nothing else, a lesson in the futility of making near-term predictions about just about anything that matters. After a very disruptive 2020, many of us started 2021 with a sense that the trajectory of the pandemic was on a clear path back to normalcy with all that that entailed for businesses and the economy. Fast forward to today and we are still wondering when this thing will end, when and how our supply chains will ever get untangled, and what the ongoing effects on prices and other economic indicators will be.

That said, one of the safer predictions we can make right now is that the accelerated pace of digital transformation brought on by the pandemic is going to continue. Businesses are going to keep exploring new ways to build on the potential of the cloud, artificial intelligence and data analytics. They're going to seek new partnerships to help them leverage these technologies. They're going to face increasing threats to the security of their digital enterprises and regulatory challenges associated with those threats. At the same time, they will also be grappling with the

social and environmental sustainability of some of the emerging digital business practices. And finally, they're going to have to keep on keeping an eye on and preparing for longer range innovations, such as cryptocurrency, the blockchain and the metaverse.

We're going to talk about all of these topics today. But I want to turn first to Marina and ask about those three core technologies I mentioned: cloud, AI and data. These are topics we have focused on individually in the past, but as, Marina, in discussing this episode we all had the clear sense that these are now coming together as a kind of convergent phenomenon that is a driving force in its own right. Can you tell us a little bit about how the pieces of this phenomenon have developed and what it means for the year to come?

Marina Aronchik:

Hi Julian, thanks and happy New Year. Yes, when we were talking about top trends in the last five years, we kept coming back to cloud, AI, data and data monetization, and over time we saw cloud services move from early test cases to material wide scale adoption for critical applications.

AI has advanced as well. It morphed from an interesting futuristic idea to excitement by early adopters and now Gartner is putting worldwide AI software revenue for 2021 at just over 51 billion dollars. We have seen an increase in AI-related licensing deals, partnerships and collaborations. It's also become clear that, in order to see a return on investment, businesses need to use AI either in or with applications that are scalable and always on, and scalable and always on means cloud. So wide scale adoption of the cloud is enabling AI.

Next, with data moving to the cloud and increasingly generated in the cloud, it's become more suitable for data analytics at scale including AI. That means that the businesses can now unlock the value of the data and monetize it.

As a result, what we're seeing on the horizon for 2022 is this fascinating convergence of data, AI and cloud computing that you've mentioned. The cloud is enabling AI to monetize data and that monetization, in turn, is driving more interest and more investment in gathering data and using cloud services.

Julian Dibbell:

Now last year we talked about the efforts to make data accessible, resulting in challenges like loss of data provenance and privacy and security concerns. Has the move to the cloud or increased use of AI resolved these issues?

Marina Aronchik:

That's a good question. So the challenges that you're describing were coming up largely in connection with the efforts to make data accessible by moving silo data from legacy systems into data lakes. What we're starting to see now, and expect to continue in 2022, is a different

approach – the implementation of a so-called data fabric that's happening in part through use of AI as you mentioned. So the idea behind the data fabric is that rather than moving data into a single repository, you stitch together various existing environments, including, importantly, cloud – and then you incorporate technology that addresses the challenges that you describe through data governance, security and integration tools.

Julian Dibbell:

Okay got it. You mentioned monetization as key to the convergence of data, AI and cloud because, in effect, it's the monetization, the result of the convergence of technology that drives businesses to invest further in gathering data and using cloud. Is this monetization resulting from new data-driven products and services?

Marina Aronchik:

Yeah to some extent. Data monetization is really a broad term that's used to refer to any valuable insights that businesses draw from data. These insights can be used to improve operations, reach new customers or newer adjacent markets or advance higher-level goals like those relating to ESG and sustainability.

The key here is that approaching the cloud, AI and data as an integrated solution, rather than a set of disparate technologies, gives the enterprises a powerful tool to address business needs by continuously recalibrating data sources, their cloud computing needs and data analytics. Doing so requires businesses to rethink and continuously invest in this different operating model and as they do so, and as the approach delivers tangible benefits and shows its value, it will fuel further investment and interest.

Julian Dibbell:

Okay and then what should we as technology lawyers be thinking about or discussing with our business clients in connection with this convergence?

Marina Aronchik:

Well I think we're going to continue to see a wide range of transactions, including, increasingly, collaborations and partnerships that contract for data, AI and cloud as the single integrated solution. Because each of these components come with their own risks and considerations, including, increasingly, regulatory requirements, working on tech deals in 2022 will be less about following a specific checklist or precedent and more about understanding the business objectives, drivers and intricacies of each technology solution and then identifying relevant sets of considerations and putting them together, really like a puzzle, in a way that makes sense for your deal.

Julian Dibbell:

Okay so now you mentioned collaborations and partnerships as being a key to taking advantage

of some of these technologies. I want to get into that because that raises a whole set of puzzle pieces as you said.

Joe, can you talk to us a little bit about some of these collaboration and partnership deals? What are the driving dynamics behind these and what businesses need to look out for?

Joe Pennell:

Yeah absolutely. So like Marina and you were just saying, we've been seeing an accelerated trend of companies entering into novel complex collaborations to deliver new digital solutions to end customers, and companies are really viewing these collaborations with their tech partners not as just a back office cost-cutting measure but as a way to enter new businesses or transform their existing customer-facing businesses.

Julian Dibbell:

Okay so what are some examples of these types of collaborations you're talking about?

Joe Pennell:

There are a lot of them out there but we've been increasingly seeing a lot of efforts to build crypto- and blockchain-enabled consortiums, managed services firms partnering with hyperscale cloud vendors, traditional financial institutions partnering with cryptocurrency exchanges or high-speed algorithmic trading firms, companies exploring robotics as a service, truck as a service, transport as a service models, joint ventures between regulated and non-regulated companies, like mortgage lenders and home builders, and a lot of different insurtech collaborations, and I could go on and on but that, that should give you a feel.

Julian Dibbell:

Yeah a lot to unpack in each of those examples and each has its own particularities with respect to the particular industry and application but the overall trend here, what's driving it?

Joe Pennell:

So, like I already mentioned, a lot of these companies are looking to drive new sources of revenue and, in tandem with that, I think a lot of companies are viewing these tech collaborations as a way to not get left behind as tech becomes the driver of new developments in just about every industry.

So for example, equipment manufacturers like big auto companies have realized that the future of their industry is going to be driven by the software tech and services that they can offer in their vehicles. So that's been driving partnerships with, or outright acquisitions of software and tech companies, by these manufacturers.

As another example, fintechs and big tech companies are increasingly entering into the financial services space, and banks want to partner with them on banking as a service offerings to reach

new customers and provide technology that could be impractical for a bank to build itself in-house. So if the bank can, for example, offer treasury and other banking services directly through the interface of its partner's market dominant ERP platform, the bank services and the ERP provider services are going to be much stickier and more desirable to their mutual end customers. That kind of the end goal. From the tech companies perspectives, partnerships with traditional economy companies allow them to acquire new customers, like I already mentioned, and both parties are really interested in gaining insights from data that are generated by these collaborations.

So summing it all up, these trends have led to dramatic increases in customer-facing digital platform deals, embedded finance arrangements and other types of collaborations, and in some ways it seems like the tech industry is becoming less distinct from all these other types of industries because the technology is becoming so embedded and vital to the products and services that are offered in just about every industry out there.

Julian Dibbell:

So what kinds of issues tend to come up in these deals?

Joe Pennell:

So, like you said that the companies and the technology solutions might vary from deal to deal but we see a lot of the same recurring issues – and Marina kind of previewed this a little bit – but you know these deals typically aren't amenable to a traditional service provider-service recipient contracting approach. Both parties often have complex interrelated performance obligations to one another, and that requires some careful structuring to clearly segregate the party's roles and responsibilities.

If either party of the collaboration is in a regulated industry, compliance and law provisions quickly turn into a key topic for the parties, as well there's often a clash of cultures on those types of topics.

Both parties are also going to be keenly interested in control of end customer relationships, including rights across market to end customers who were introduced by one party to the other party as part of the collaboration and, you know it – as mentioned several times already – these collaborations also tend to generate valuable data and the scope of each party's right to use, commercialize or monetize that data, especially in regulated industries where there may be limitations on what you can and can't do. These turn into very key issues that are often heavily negotiated and really the heart of the deal.

Julian Dibbell

Right. And you've touched on the core of it here, the value of data and the value of protecting that data which leads us to, you know, the question of data security and data privacy. Vivek what can you tell us about what we're seeing on that front?

Vivek Mohan:

Thanks Julian. As many of you were likely aware, 2021 was a banner year for cyber security and not in a good way. The news is filled with high-profile cyber incidents impacting the supply chain, as well as a number of high-profile ransomware incidents. This has naturally lead boards, c-suite executives and ultimately us lawyers to continue to re-tune and refocus on these issues. We've seen this flow down on how security is operationalized and how risk is managed on a day-to-day basis, whether in the context of measures that are put in place to protect data in contract, new focus by lawyers on understanding and assessing technical risks, as well as an overall refocus on the idea of cyber security as a key priority, and one of the highest priorities for companies that are seeking to engage in any sort of transaction.

These are important issues no matter how you're positioned. Whether you're processing data on behalf of a third party whether you're asking a third party to process data on your behalf or whether you're entering into one of the newer types of deals, as Maria mentioned, complex multi-tenant cloud environments working across jurisdictions or engaging in cross-border data transfers. We've seen this really change the way and nature and style of contractual clauses that are in place, as I'll talk about a little bit later.

In Europe, the release of the new model contractual clauses included a renewed focus on security measures that companies put in place to protect data as it flows across borders. We've seen in transactions lawyers paying an increased amount of attention to how they assess and understand and capture technical measures that are in place to protect data, including things that have traditionally been left to IT departments in the past. This takes place both proactively and reactively. It means that diligence involves an increased focus on understanding the data landscape of a potential target or counterparty but also means that lawyers have to understand this and find a way to describe risks to business decision makers, to executives and to reflect mechanisms that they put in place to manage and address these risks, whether through contract insurance or otherwise.

This is something that is really going to continue to be a sharpened focus – we think – in 2022 and going forward as cyber security continues to be something that dominates the news cycle and the risk landscape continues to evolve and thus continue to grow globally.

Julian Dibbell:

Okay so businesses and their lawyers are obviously paying a lot of attention to cyber security for very important reasons, but as we know there's been a lot of regulatory attention to cyber security as well. How is that and how are developments there impacting how lawyers are going to be looking at these issues on a day-to-day basis?

Vivek Mohan:

Yeah it's a great point Julian. You know, the regulatory attention to cyber security has been

really notable and has been really significant over the last year, and we think that this is going to be one of the most important trends for the coming year.

The FTC announced – the Federal Trade Commission for those of you that don't follow in the United States – announced in December that they are considering rulemaking on data security as well as privacy and some other topics, and this is really a new and big step for the FTC. It hasn't pursued this type of making in recent history, and this will be a really important milestone for companies as the FTC is the de facto federal privacy and security regulator. We haven't seen an advance notice of proposed rulemaking, we just know that they have this on their mind, but it will be really interesting to see what they put out because I think that there is a range of options. They could go from very, very high level, which is aligned with the NIST cyber security framework, an adaptable framework for cyber security rules, all the way down to the very prescriptive such as the New York Department of Financial Services which went so far as to prescribe the number of days that companies should retain logs.

We'll see where the FTC lands on this but this is going to be really interesting because we expect that whatever the FTC puts out there is going to be adopted by companies even before it comes into formal effect as a proxy for reasonable security. So we expect to see this in the coming year and we expect to see these provisions work their way into contracts, because in the absence of a binding rule people will look to what the regulators have articulated they expect.

This is also the case with the Securities and Exchange Commission and, this is a really interesting development from the SEC which has not been traditionally a cyber-security regulator, but has paid an increasing amount of attention to this issue over the last year and really ultimately over the past decade.

This is important to both public issuers of debt and equity, so really any public company in the United States, as well as regulated entities, but it's also just a good point of guidance and a touchstone for really any company doing business because the Securities and Exchange Commission is one that always gets c-suite attention. No matter what they say, CEOs are paying attention. And as the SEC has issued specific guidance for regulated entities that has undertaken enforcement actions in the past year and has undertaken an unprecedented industry-wide sweep following the SolarWinds data security incident, we have seen that the SEC is really going to continue to sharpen its focus on these issues, including, in particular, how companies think about disclosure of these issues. I think that disclosure is a really interesting topic in two contexts here for companies that are thinking about transactions because when we think of disclosures in the SEC context we're thinking about making something public. But I think that there's an equally important focus on thinking about disclosures that are made, particularly against representations that are made, for example, in transactional agreements. So we'll have to keep an eye on how the SEC's focus on this changes and evolves the way the companies think about this in the coming year and years.

It's not just at the federal level, though. As people likely know, several states have enacted privacy laws that include cyber security requirements, including particular requirements to maintain reasonable security. This is already in effect in California under a law known as CCPA but is being renovated in 2023 with a law called CPRA. Virginia and Colorado have also passed similar laws with similar requirements, and one of the things to really keep an eye out for over this year is regulations that are being issued by the various boards and agencies that are tasked with implementing these laws and coming up with implementing regulations.

We'll also keep an eye on state legislatures and that we expect it to be an active session. As laws come into effect, we are going to have to react. We're going to have to think about how to comply with these requirements, and I think that the list of jurisdictions that lawyers should be thinking about when thinking about cyber security risks and cyber security contracting are really going to continue to grow.

Julian Dibbell:

Well that's a lot going on here in the U.S., what about the rest of the world, what's going on out there?

Vivek Mohan:

Thanks Julian, you're right, I'd really be remiss not to think of this and make sure to contextualize this as a global issue, and the legal landscape is really evolving the world over. Since we just have a few minutes I'll just mention the increased attention to cyber security in the EU and in China in particular. As I mentioned earlier, in the EU we saw the release of the new model clauses which included a pronounced focus on the security measures in place to protect data, but we've also seen the regulators really focus on security, including a number of investigations and enforcement actions following data security incidents, and we also see a significant amount of legislative action including a rewrite of the network information security directive which will already does govern cloud computing, and this will be something that I think is going to be a really interesting area to watch in the coming year particularly for companies that are considering migrations or transitions into the cloud.

In China, we saw the enactment of a of PIPL, a new privacy law that supplemented several other frameworks already in place in China, including the cyber security law and data security law and the rapid enactment of this – I think quite a lot of companies by surprise. One of the things I think is particularly important to consider is that these requirements really relate to the life cycle of protection of data including a particular cross-border transfer. Companies transferring certain types of data out of China are required to conduct security assessments now, and while there is not a tremendous amount of implementing guidance that makes clear exactly what and how companies can comply with these requirements, this is something we've really been helping clients with in a number of contexts, either developing compliance programs or strategies to demonstrate compliance, figuring out how to work with vendors and ask vendors to

demonstrate their compliance when handling a company's data on their behalf or otherwise including through the use of software tools to automate some of these processes. This is going to be an increasingly complicated compliance burden as the laws continue to be enforced and enacted, and we're looking forward to seeing what's to come.

Julian Dibbell:

Thanks Vivek. Brad, what can you tell us about some of the challenges businesses will be facing with respect to sustainability of technological practices and otherwise?

Brad Peterson:

Thank you Julian. The risks that Vivek just highlighted are just a superb illustration of the growing focus on sustainability. And sustainability means whether we can keep doing what we're doing. Sustainability includes concerns like ESG or environmental, social and governance, which protect our planet and society. And sustainability also includes increasing focus on resilience, and by resilience we mean the ability to keep delivering despite surprises like these supply chain problems that you alluded to in your introduction.

In 2021, we saw increasing numbers of the world's leading companies, including a lot of our clients making public pledges for what they call "net-zero emissions", for equity and inclusion and for other sustainability goals. There's a lot in the press on this. A recent article in nature, for example, reported that one-fifth of the Fortune Global 2000 have made net-zero pledges. An organization called Science-Based Targets has a website that reports companies who have adopted science-based targets – as of today, 1095 of those – and companies that have ambitions for 1.5 centigrade as the maximum global warming, 1163 of those as of today. This is remarkable because up until quite recently, really in until the pandemic, businesses generally saw their mission as maximizing economic returns to stockholders.

Julian Dibbell:

So companies at the top levels are making sustainability pledges. How does this affect technology contracting?

Brad Peterson:

Meeting those pledges is going to require changes in supply chain, including in the technology supply chain. A report from McKinsey in September of 2021 said, quote, "two-thirds of the average company's environmental, social and governance footprint lies with suppliers." Obviously a lot of that is potentially in the technology supply chain. Suppliers data centers require enormous amounts of energy and I know we've all seen the headlines in the, in the press about bitcoin in particular on that front. Suppliers algorithmic decision making processes may unfairly discriminate and may have other adverse social impacts. When companies rely on partner companies for critical functions, a company's own resilience depends on the partner's resilience, again, the supply chain problems that you've described.

Julian Dibbell:

Okay sure but what then do you actually contract for with the suppliers to make an impact on these things? Haven't there always been sustainability clauses?

Brad Peterson:

There have always been sustainability clauses, you're right, but those have tended to be either sort of aspirational and vague or they focus on a single law. If we're going to contract effectively we need to have measurable targets that can be used as standards in engineering and sourcing and accepting the goods and services. I think one of the reasons that we see a trend for 2022 here, is that we're seeing a lot of work on measurable targets from companies, from NGO's and from governments. Companies, for example, the standard wars has come out with the S&P Global Corporate Sustainability Assessment which provides a tremendous collection of metrics and allows companies to report. NGO's have been active in this area. The world economic forum came up with 21 core and 34 expanded metrics in September of 2020. Governments have been active. Vivek provided a lot of good examples in his talk, but it's more across the supply chain. Example, June 2021 the German Parliament passed a law that in English translates to a law on corporate due diligence and supply chains.

Julian Dibbell:

So, all right we will have some very specific metrics to contract around. That though seems to be just a first step, right?

Brad Peterson:

Yes Julian, I think you're right. This is going to require a great deal of innovation in technology contracting.

Technology contracting has long focused on what's provided and what's paid, it hasn't focused as much on how the partner company will do its work and of course here that needs to change so that companies can manage across organizations and caused their partner companies to act in more sustainable ways.

How are we going to do that? A great example of success in managing across organizations and being quite specific in managing how the other company works is in the area – is Vivek's area, data security. Today we see that major technology contracts almost inevitably have two things. One is a schedule of detailed information security requirements, and the second is a requirement that outside standards be followed. Those two requirements are often backed up by transparency requirements. For example there might be an obligation to provide notice of any data security breach or for example you might have an audit right to allow review of information security standards. Technology contracting lawyers and the technology contracting teams that we work with will need to do the same for critical sustainability objectives. We will need to identify third-party standards. We will need to draft new contract language, and we will

need to develop new governance approaches. I'm excited about the opportunities to do all that in 2022.

Julian Dibbell:

All right so, Brad, as you've highlighted – and every everybody else has – there's a lot for businesses to keep an eye on and grapple with as they engage with the emerging core forces of digital transformation that are front and center right now. At the same time, we've got longer range innovations out there that we keep being told are going to be part of this transformation as well. It's sort of farther out there types of things like blockchain, cryptocurrency, etc. How do companies need to think about those here and now, even though they're not necessarily right on the front burner yet? Rohith, do you wanna tell us what you think about that?

Rohith George:

Yeah sure. So, I'm a bit of a technophile. I'm always buying the latest gadgets, regularly reading my *Wired Magazine* or my *Tech Runs* or my *Gizmodo*. I'm hitting the metaverse with my oculus quest or trying to become a digital landlord. Everything I'm doing, pretty much everything you can think of, but my experience both in my personal life as well as in my professional life is that new tech follows a somewhat predictable cycle to business adoption, it's a theory, to application, to hype to than actual real world business use.

Marina talked a bit about AI and how it's seeing widescale adoption use in business today. I remember when four or five years ago the running commentary was whether or not AI was really ready for use in business or whether people were just throwing around AI as a buzzword.

When you think about it, AI and machine learning as an actually useful technology and business, it follows the same kind of cycle that I mentioned, just like cloud before it. At first there were years of academic research focused on theory and, application of theory and then there's some level of – something that ignites interest, like for example IBM's Deep Blue, in '97 beating the world champion at chess, and then from there the ice cycle begins and people start to try and improve use cases, get the proof of concept and various, business applications, and then from there, the businesses that enable this technology start to spring up around it.

For AI it was data set providers that are actually feeding collecting data cloud providers and cloud solutions that can actually connect the data in an always-on state with the AI and then you finally start seeing wide scale business adoption and I think we're seeing blockchain technology following a pretty similar path except, maybe four or five years behind there were years and years of research, that finally culminated with something that hit the public consciousness in 2008, with the publishing of the bitcoin white paper and the genesis of the Bitcoin blockchain, which really provided kind of the first real application of blockchain technology to a real world use case, which is peer-to-peer payments. And since then, we've been in the hype cycle, with companies very much interested but only willing to kind of dip their toe in the water. We've seen some of our clients enter into consortiums to explore different use

cases, together with other companies for their particular industry. We've seen them enter into proof of concept or pilot agreements with particular blockchain technology providers, but, for the past several years the running commentary was the same as it was with AI, good for us to keep on top of but really too early, to invest any significant money or time into.

Julian Dibbell:

And do you think that's changing?

Rohith George:

Yeah, our experience over the last year suggests that we may be moving into the next phase heading into 2022 just as with AI we've seen the infrastructure around blockchain technologies bring up. There are now blockchain as a service solutions that have come to market that target businesses cloud providers like AWS. They have established offerings that'll host, for example, blockchain nodes on using different blockchain frameworks.

In crypto we've seen wallet providers – it'll handle some of the tricky areas like private key management for businesses. We've seen custodial solutions that'll custody funds so that actual businesses don't have to deal with some of the thorny regulatory issues associated with holding in custody and crypto. And there are now offerings, for example, like Coinbase commerce, that will allow businesses to accept cryptocurrency as payment for goods and services. And this kind of growth is similar to what we saw with cloud and with AI as those technologies began gaining traction. And I think you will only really continue to see this trend continue and grow in 2022.

Julian Dibbell:

Okay so if you're a technology lawyer looking at this, what's the best way to prepare for this trend?

Rohith George:

I think the thing to keep in mind, and this will be stating the obvious, but the thing to keep in mind is that these are all different agreements for different services that at their core are not all that different than technology agreements that you may as a technology lawyer be otherwise used to.

For example, an agreement with a blockchain as a service provider is going to be probably 90 percent similar to a software as a service agreement that you're accustomed to. And if you're hiring a company, as an another example, to develop an NFT or non-fungible token for your business that's going to be 90 percent similar to a technology development agreement. But the key is really understanding the underlying technology well enough to identify the risks associated with the remaining 10 percent that's different. A standard SAS agreement may, for example, have SLA credits as the sole exclusive remedy for downtime, but this may not be adequate when the staff solution involves the custody of customer funds. If you're using a standard API license agreement for the use of a blockchain platform that handles the transfer or

the purchase or the sale of crypto, well there may be some financial regulatory issues that you need to explore like what your role is as an intermediary in that transaction.

So I think the key will be to have a sufficient understanding of the core technology, as I mentioned, to be able to spot these issues and then once you do spot the issues, you have to involve the right experts, whether that's a regulatory lawyer or a tax lawyer or otherwise. But it's exciting to me to see some of these technologies mature. I think there are also a number of other areas that we could spend hours on that are even a little bit earlier in the hype cycle like how Web 3 is going to be so much different than Web 2 and what that impact is going to be. What decentralized autonomous organizations, or DOW's, what they mean to the future of companies and future organizations or even how businesses are going to enter the the Metaverse. But, we'll leave that for next season, for future podcasts.

Julian Dibbell:

All right, thanks, and thank you Brad, Vivek, Joe and Marina. You've given us a lot to chew on in all your remarks. I guess if there is one lesson to draw from all of your insights, it's that that level of resiliency and agility that businesses have had to demonstrate for the last two years is no longer something we can think of as a temporary requirement. We're not going back to the old normal anytime soon and it's time to get used to the new normal.

Listeners, if you have any questions about today's episode or an idea for an episode you'd like to hear about anything related to technology transactions and the law please email us at techtransactions@mayerbrown.com. Thank you for listening.

Announcer:

We hope you enjoyed this program. You can subscribe on all major podcasting platforms to learn about other Mayer Brown audio programming visit mayerbrown.com/podcasts. Thanks for listening.