Photo by Fit Ztudio on Shutterstock

LEXOLOGY
Getting the Deal Through

Market Intelligence

DIGITAL TRANSFORMATION 2022

Global interview panel led by Kemp IT Law

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by Kemp IT Law, this *Digital Transformation* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Government policy
Procurement best practice
Contractual negotiations
Cybersecurity & data protection

START READING

About the editors

Richard Kemp and Deirdre Moynihan
Kemp IT Law

Richard Kemp is a partner at Kemp IT Law. He has advised clients on digital transformation projects in the professional services, transportation, retail and market data sectors. Widely recognised as one of the world's top IT lawyers, he is in *The Legal 500*'s Hall of Fame and is one of *Who's Who Legal*'s 20 global elite data law thought leaders. Richard set up Kemp & Co in 1997, Kemp Little in 2001 and Kemp IT Law in 2014. Under the strapline 'IT Law at the Apex', Kemp IT Law has won over 100 awards for client service and innovation since 2015.

Deirdre Moynihan is a partner at Kemp IT Law LLP. She routinely advises organisations in all sectors on digital transformation projects, and has a particular focus on data-related issues and on supporting law firms procuring and deploying new technologies. Deirdre, a Certified Information Privacy Professional and Manager, has been recognised as a 'Next Generation Lawyer' by *The Legal 500* from 2021–2023, including for 'adeptly handl[ing] digital transformation projects'. Deirdre is included in *Who's Who Legal* 2021 as an expert in data law and is recommended by *Chambers* and *The Legal 500* for 'deep sector expertise' in IT and as a 'formidable and effective negotiator and a pleasure to work with' by 'providing clear and decisive advice'.

Contents

While reading, click this icon to return to the Contents at any time

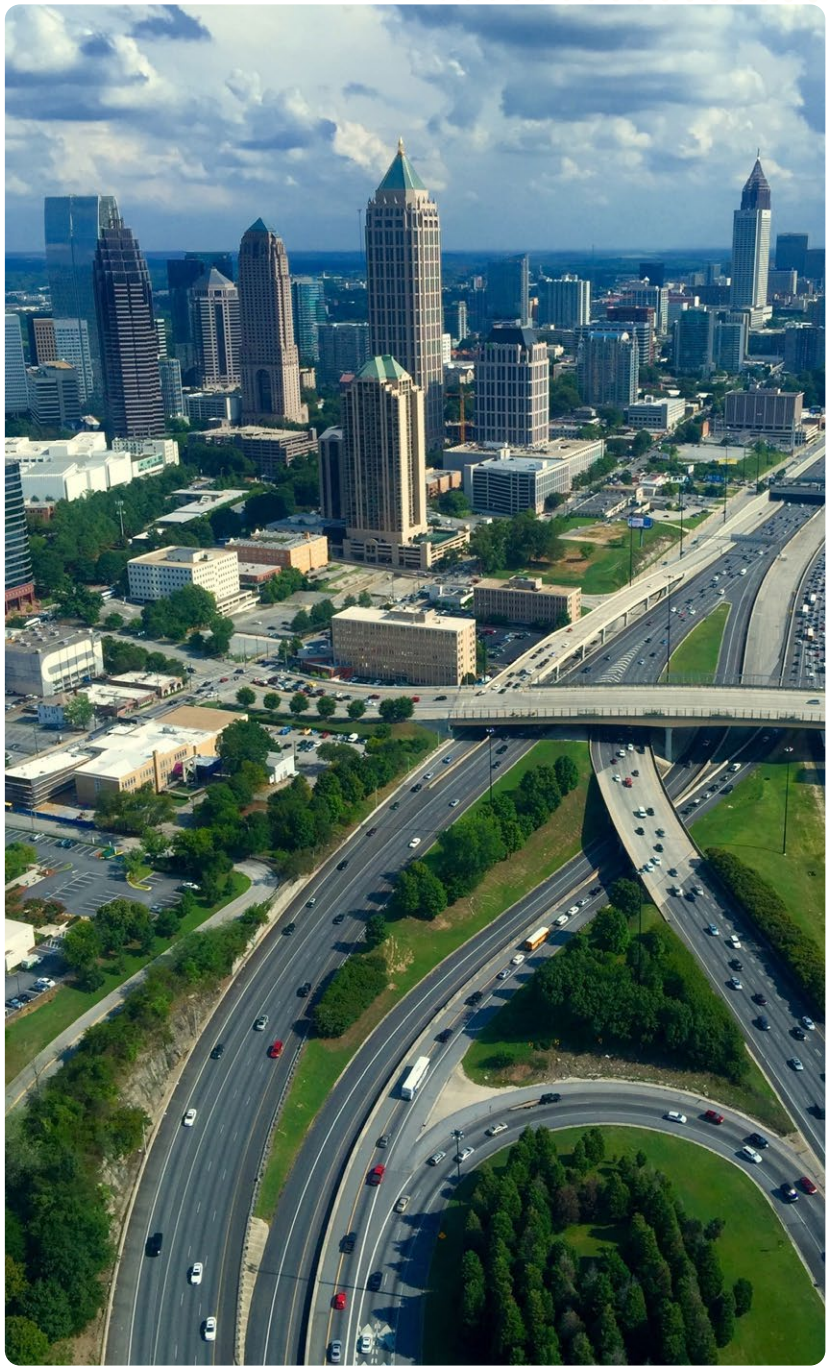


Photo by Brett Barnhill on Shutterstock

United States

Paul H Arne at Morris, Manning & Martin, LLP advises clients in legal and business issues involving computer technology and the internet, with a special emphasis on complex transactions and difficult legal issues. His practice focuses on the law and business of technology, privacy, security and revenue recognition worldwide. Representative transactions include the development of distributed sales force automation software for all US sales activities of a large pharmaceutical company and outside counsel for the development of all sell-side form agreements for a multibillion-dollar healthcare IT company.

Austin B Mills represents clients in complex matters including technology transactions, blockchain, cryptocurrency, payments, financial technology, and privacy and security. Austin advises clients on transactions and the application of laws relating to technology, particularly blockchain and financial technology. He also advises technology, blockchain, cryptocurrency and financial services clients regarding regulatory compliance and data and information security and privacy matters and helps clients establish compliance programmes.

Michael R Young focuses his practice on data privacy advising. As chair of the cybersecurity and privacy practice, his primary areas of concentration include managing complex technologies and sensitive, confidential or personal data. Michael works with legal and business teams to create legal architecture related to the development of new products or services and has advised global organisations in navigating crucial issues such as international data transfers, information security regulations and complex privacy and information security compliance.

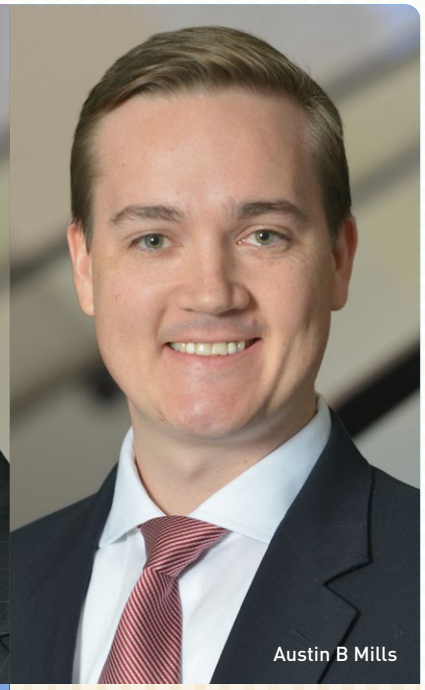
1 What are the key features of the main laws and regulations governing digital transformation in your jurisdiction?

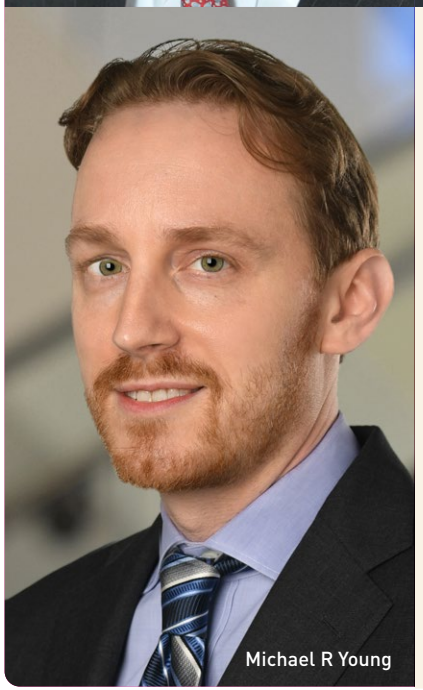
There are few laws and regulations that place restrictions on digital transformation generally. Most laws impacting data processing are the same, whether a business uses paper-based data and processes, internally-operated electronic data and computer-based processes, or electronic data and computer-based processes running in the cloud. Some of these laws actually favour internet-enabled processes over their paper counterparts, such as the safe harbours in the Communications Decency Act and Digital Millennium Copyright Act.

Basic laws, such as copyright, trade secret, patent and contract law, continue to apply. For example, moving operations from internal operations to a third party cloud environment may require modification of existing software licences. Virtualisation and clustering technologies can increase the complexity of software licensing and compliance. Laws related to privacy and use of personal information do change when moving to internet-enabled solutions, and are rapidly changing.

There are many industry-specific laws and regulations and standards that may impact digital transformations, especially those related to privacy and security. These industries include financial services, healthcare, credit cards, governmental services, education, and credit reporting. Some US laws also regulate certain activities or classes of information, such as the CAN-SPAM Act, the Telephone Consumer Protection Act, the Child Online Privacy Protection Act and certain activities of the Federal Trade Commission. Most digital commercial transactions and social media information do not normally fall into these industries and categories of information and are, therefore, readily available for use by those companies able to legally capture that information, at least based on US federal law.


Paul H Arne


Austin B Mills


Michael R Young

"Laws related to privacy and use of personal information are rapidly changing."

US federal law does not have a comprehensive law for privacy or security. States are stepping into that void, with a growing and varied set of state laws related to privacy and security. State laws are beginning to cover privacy on a more comprehensive basis, analogous to the GDPR. Because commerce is typically not limited to a single state, individual state laws frequently have consequences outside of their own state borders.

2 What are the most noteworthy recent developments affecting organisations' digital transformation plans and projects in your jurisdiction, including any government policy or regulatory initiatives?

Very early in the internet age, the US Congress passed section 230 of the Communications Decency Act, which has broadly shielded internet information providers from liability when using content obtained from third parties, insulating providers from liability for libel, US Fair Housing Act, etc. This law prevents providers from being considered the 'publisher' of this third party content.

For the first time, the US Supreme Court will review the scope of section 230. The specific question raised is whether the use of algorithms to direct third party content to certain users results in the provider being the publisher of the third party content. The recent change in membership of the Supreme Court has resulted in some decisions that show a greater willingness to overturn precedent generally. Any substantial reinterpretation of section 230 can have a very important impact on those companies with US operations that obtain and use content from customers and other third parties.

Recently, two standards for open source management have become recognised as international standards. The SPDX specification, which is an XML schema for keeping track of open source usage, has been adopted as ISO/IEC 5962. Open Chain, a standard for managing open source software in the enterprise, has been adopted as ISO/IEC 5230. Open source software is readily available and frequently provides many advantages over commercially available software, yet it has been difficult to manage effectively by large enterprises. The adoption of these standards may be quite helpful in managing this important part of corporate data centres and IT operations.

Photo by Nate Hovee on Shutterstock

We expect 2023 to see the continuation of several important emerging developments regarding US privacy law. In 2023, comprehensive new privacy laws – similar in concept to the GDPR – will go into effect in California, Colorado, Virginia, Utah and Connecticut. These laws require notices, offer broad consumer rights to access, correct, delete and restrict data processing, impose requirements on data use and retention and require specific forms of contracting around data. Companies that are still behind in implementing these laws may face a rude wake-up call when consumers, regulators, and others start demanding compliance.

> "Companies who seek to contain data breaches without legal or forensic assistance may be reviewed by regulators years later."

Other legal developments raise substantial issues for online tracking used to support behavioral profiling and targeted consumer ads. These developments include: (1) explicit opt-out rights from such tracking in some new state privacy laws; (2) an enforcement action from the California Attorney General clarifying that certain online tracking is an in-kind regulated 'sale' of data; and (3) an appellate case holding that certain third party tracking requires all-party consent under Pennsylvania's wiretapping law.

Taken together, these show that policymakers, enforcement authorities and private plaintiffs' lawyers are starting to push hard against current online tracking practices. This pushback could have big implications for the online analytics and the ad-supported internet.

2022 also saw increased regulatory focus on past incidents. Companies who seek to contain data breaches without legal or forensic assistance may be reviewed by regulators years later, with substantial fines and enforcement actions. We predict that after-the-fact enforcement will continue in 2023, with a focus on companies in regulated industries, like finance, or companies undergoing public sales or acquisitions.

Much like prior years, cryptocurrency and blockchain applications and market activity have been frequently discussed by US regulators with minimal movement on concrete regulatory and policy actions. The primary recent developments at the US federal level include: (1) President's Biden's 'Executive Order on Ensuring Responsible Development of Digital Assets'; (2) high-profile OFAC sanctions; and (3) further informal guidance from various federal regulators, including the SEC, OCC, and FDIC.

The Executive Order calls for a whole-of-government approach to regulating digital asset activity, focusing on: (1) consumer and investor protection; (2) financial stability and systemic risk; (3) the prevention of illicit finance; (4) US leadership and competitiveness; (5) financial inclusion; and (6) responsible innovation. It tasks the Treasury Department, Financial Stability Oversight Council, Commerce Department, and Federal Reserved to research, identify and issue recommendations.

Recent OFAC sanctions include sanctioning of (1) Hydra Market, the world's largest and most prominent darknet market; and (2) Tornado Cash, a virtual currency mixer allegedly used to launder more than US$7 billion worth of virtual currency. In what may be a first, the sanctions on Tornado Cash appear to extend to the technology itself, as opposed to specific individuals or addresses.

The SEC continues to assert that most issued cryptocurrencies and tokens are securities. It has identified three areas for its enforcement activities – platforms, stablecoins and tokens. In April 2022, the FDIC issued a letter to its member banks, telling them to inform the agency if they plan to engage in any cryptoasset activity, citing concerns that these activities may pose systemic risks to the financial system.

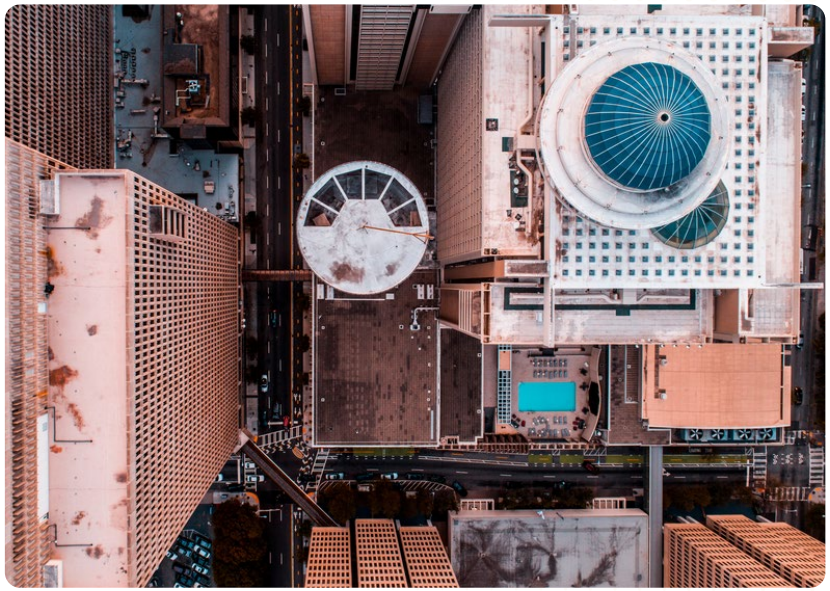


Photo by Main Focus Media on Shutterstock

Finally, the head of the OCC warned banks to consider the risks of trading crypto derivatives.

3 What are the key legal and practical factors that organisations should consider for a successful cloud and data centre strategy?

There are tremendous cost advantages to using cloud infrastructure. Data centre operations, with attendant requirements for data availability and data security, are frequently not within a company's core competencies. Using the cloud is increasingly becoming the standard for business operations.

However, companies should recognise the differences between having an in-house data centre and operating a business using someone else's data centre. When companies use someone else's infrastructure for their business, they may not have the capacity to take an application back into their own data centres quickly. Frequently, cloud implementations mean that you do not possess your own data. These differences pose additional risks to an enterprise. Part of a good strategy for using the cloud is to identify and attempt to mitigate these additional risks.

Just because a cloud provider is good at security does not mean that your company's implementation in the cloud will be secure. The company is still responsible for it. In their first cloud initiatives, many organisations were not as aware of this as they needed to be.

All contracts come to an end. Planning for that end, whether things do not work out with your provider or for other reasons, is critically important. How do you get access to your data? How do you keep your operations going if the cloud provider is unexpectedly no longer available? How are you going to get an infrastructure to operate your business? How long will this take? All of these questions should be resolved as a part of entering into a relationship with a cloud provider or a service provider that operates in the cloud.

4 What contracting points, techniques and best practices should organisations be aware of when procuring digital transformation services at each level of the cloud 'stack'? How have these evolved over the past five years and what is the direction of travel?

As you go up the cloud stack – from infrastructure as a services (IaaS), to platform as a service (PaaS), to software as a service (SaaS) – all of the issues from the lower parts of the stack still exist. If you are contracting to receive a SaaS service, all issues at the level of IaaS are still there.

In IaaS implementations, where the cloud provider is responsible for networking, storage, servers and related items, the IaaS provider is also providing electricity, bandwidth, HVAC, physical security, etc. How quickly can the IaaS provider make additional processing capacity

or bandwidth available? How redundant are these services? A friend of mine tells the story of a data centre where both the primary and backup access to the internet went down. Apparently, the primary internet access and backup internet access were wired through the same conduit leading into the building. One swipe of a backhoe killed both systems. How much bandwidth is available to the internet or between servers in the data centre? Depending on the importance of the system running on an IaaS platform and the need for availability, all of these systems may need to be investigated. Multiple warm or hot sites may be needed. We have seen companies consider using data centres on multiple tectonic plates for availability reasons.

Clarifying the roles and responsibilities of the parties is important. This is especially true in co-location (CoLo) relationships. Will the CoLo provider be responsible for rebooting the servers or installing and patching the OS? What services will the IaaS provider provide? If a server goes down, how quickly will server availability be reinstated on another server?

In working with PaaS providers, where the OS, middleware and possibly other software are frequently the responsibility of the PaaS provider, all of the issues related to IaaS providers still exist, but the issues related to the performance and availability of those additional software and services become important. While important in IaaS situations, the speed and coordination of patches becomes relatively more important in PaaS implementations. Protection against viruses and malware grows in importance as the amount of software managed by the provider increases.

SaaS implementations also bring additional issues. SaaS providers typically have more control over what data is stored and the customer's ability to access that data. Uptime availability becomes more important simply because there is more technology being provided, and applications are more likely to crash than server operating systems.

"SaaS providers typically have more control over what data is stored and the customer's ability to access that data."

As organisations gain experience with cloud services, on average they have become more aware of the due diligence needed in the selection process for cloud providers. Service recipients, especially larger companies, are much more sensitive to these issues than in the past. The availability of third party evaluations of security and operations, such as ISO 27001 and SSAE 18 SOC 1 and SOC 2, have become more important.

5 In your experience, what are the typical points of contention in contract discussions and how are they best resolved?

One of us once had a negotiation where the customer insisted that the cloud service provider take 100 per cent of the risk of data loss and data breaches, without limits. Prior to this transaction, the customer had always operated this system itself. During the negotiations, it became clear that the customer's system did not encrypt its data at rest, yet the service provider was going to store the data in encrypted

form. Even when the service provider was providing a more secure and robust system than the customer's existing system, the customer insisted that the service provider take all the risk. Risk allocation for data breaches is a normal point of disagreement in negotiations.

The responsibility for data breaches is not only a risk discussion but also a price discussion. No one does everything that is possible to protect computing systems and data. Spending more money can improve the chances that no data breach events will occur. Customers of cloud service providers, especially SaaS, should realise that they are not only buying a service; they are also buying a level of security.

Frequently, negotiations related to the responsibility for data breaches results in the negotiation of a 'super cap'. This is a relatively easy way to negotiate these issues, since you are only negotiating a single issue: the amount of the cap. However, these negotiations can be much more nuanced, based on the possible types of damages and whether agreed-upon data security obligations have been followed.

For example, the limits of liability may be different depending on whether the service provider's breach of its security obligations contribute to the data breach. If the data breach occurs while the service provider is living up to its security obligations, damage limitations may be different than when the service provider is not living up to those obligations. This kind of negotiation puts pressure on the accuracy and specificity of security obligations.

Some types of damage resulting from a data breach are more quantifiable than others. For example, information is available about the average cost of investigating a breach, providing data breach notices or providing one or more years of credit monitoring services, although these costs will vary depending on the industry and data involved. On the other hand, loss of reputation or lost profits arising from a data breach are normally much more difficult to determine, and are frequently more of a concern to the providers. Addressing

Photo by Sean Pavone on Shutterstock

these types of damage separately from each other in the contract can result in eliminating an impasse in negotiations.

As the years have gone by, the value of data and data analytics has become more apparent. SaaS providers may therefore be more incentivised to use customer data, especially customer data that is anonymised and aggregated with other customer data, as an additional service offering. There was a period of time where it seemed that every client with a SaaS offering wanted to monetise the data.

The right of a SaaS provider to use the customer's data for some purposes is a regular point of contention in negotiations. How this is resolved varies significantly based on the industry, the type of data, the proposed uses and the relative negotiating strength of the parties.

"Significant recent changes in export regulations related to Russia and China have increased the need to be sensitive to US export regulations."

6 How do your jurisdiction's cybersecurity laws affect organisations on their digital transformation journey?

Cybersecurity is always a moving target, because technologies and corresponding threats to technologies are constantly evolving. In the US, however, over 51 legislative bodies (US federal, 50 states, various US territories, and the District of Columbia) have largely independent authority to enact laws related to privacy and security.

While each new law should be examined, it is very useful for companies to develop a framework that assesses what data is being obtained, used and generated, what systems are receiving, processing and storing that data, how important it is to protect that data, and what ethical, legal and moral obligations the company has to those that provide or receive the data and those whose information resides in the data. Good security practices are critical.

7 How do your jurisdiction's data protection laws affect organisations as they undergo digital transformation?

Complying with privacy and security laws is simply a part of any digital transformation. US companies are also regularly impacted by the GDPR and similar legislation in other countries. Other than export and related regulations, which can be quite complicated, there is little regulation of data exports. For example, OpenSSL is an open source product, available to almost anyone in the world. If a company creates a product that invokes OpenSSL in order to encrypt data, whether or not the OpenSSL executable is shipped with the product, then the product may be subject to export regulation, meaning that it can only be shipped to Canada without qualifying for an exception under the export regulations. The exception frequently requires a filing with the US Bureau of Industry and Security. Export law covers more than many companies think it does.

Significant recent changes in export regulations related to Russia and China have increased the need to be sensitive to US export regulations.

8 What do organisations in your jurisdiction need to do from a legal standpoint to move software development from waterfall through Agile to DevOps?

It is rare that we speak with a software company that has not moved to some form of Agile development methodology. Agile and SaaS tend to work well with each other. Development shops in large companies have more of a challenge in moving to Agile. In software development agreements, where third parties are providing development services, the contractual means for managing risk in a waterfall development can be very different from managing risk in an iterative development.

Photo by f11photo on Shutterstock

Because most Agile developments normally require the delivery of working code at the end of each 'sprint', the customer should consider testing after each sprint. Timing of when these tests should begin and end will normally need to be shortened. In many circumstances, the customer should ask for access to progress reporting that is consistent with how sprints are managed by the developer. The customer should normally participate in the process of determining what will be developed in the sprints.

9 What constitutes effective governance and best practice for digital transformation in your jurisdiction?

A recent *Harvard Business Review* article reported on its review of the results of various studies from academics, consultants, and academics, concluding that between 70 per cent and 95 per cent of digital transformations fail to meet their original objectives.

Preparation, engagement of stakeholders, training and governance are critically important to any digital transformation initiative.

Agile and DevOps will frequently change the way internal development projects are funded. Decisions that have historically been made at a certain level of an organisation may need to be moved either down or up in an organisation. For example, specific tasks may need to be decided at a scrum team level, while the presence of multiple scrums may require a higher level of coordination among scrum teams, such as standard data models and development standards.

Paul H Arne
parne@mmmlaw.com

Austin B Mills
amills@mmmlaw.com

Michael R Young
myoung@mmmlaw.com

Morris, Manning & Martin, LLP
Atlanta
www.mmmlaw.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

What aspects of and trends in digital transformation do you find most interesting and why?

As outside legal counsel, and especially as the senior attorney in my group, part of my job is to know the answer to questions that experienced in-house counsel do not. Accordingly, I tend to focus on areas of technology law that are not well-established or are rapidly developing. These currently include the laws related to the use of APIs, open source software, web scraping (especially the emerging impact of the US Computer Fraud and Abuse Act on web scraping), the boundaries of the idea–expression dichotomy, blockchain and AI.

What challenges have you faced as a practitioner in this area and how have you navigated them?

There is a frequent lack of understanding that a business model feeds directly into a sell-side contract, including the nature of the technology, how it is architected and the circumstances triggering additional compensation. This is an education process with clients. Creating such a contract often forces emerging companies to hone their business model.

What do you see as the essential qualities and skill sets of an adviser in this area?

I view myself as a person who provides business advice through a legal lens. We need to understand that businesses take risks all the time. Our job as legal counsel is to help our clients identify, evaluate, and mitigate risk. It is our job to fully inform our clients, help them quantify the risk, and then let them decide whether to take the risk.