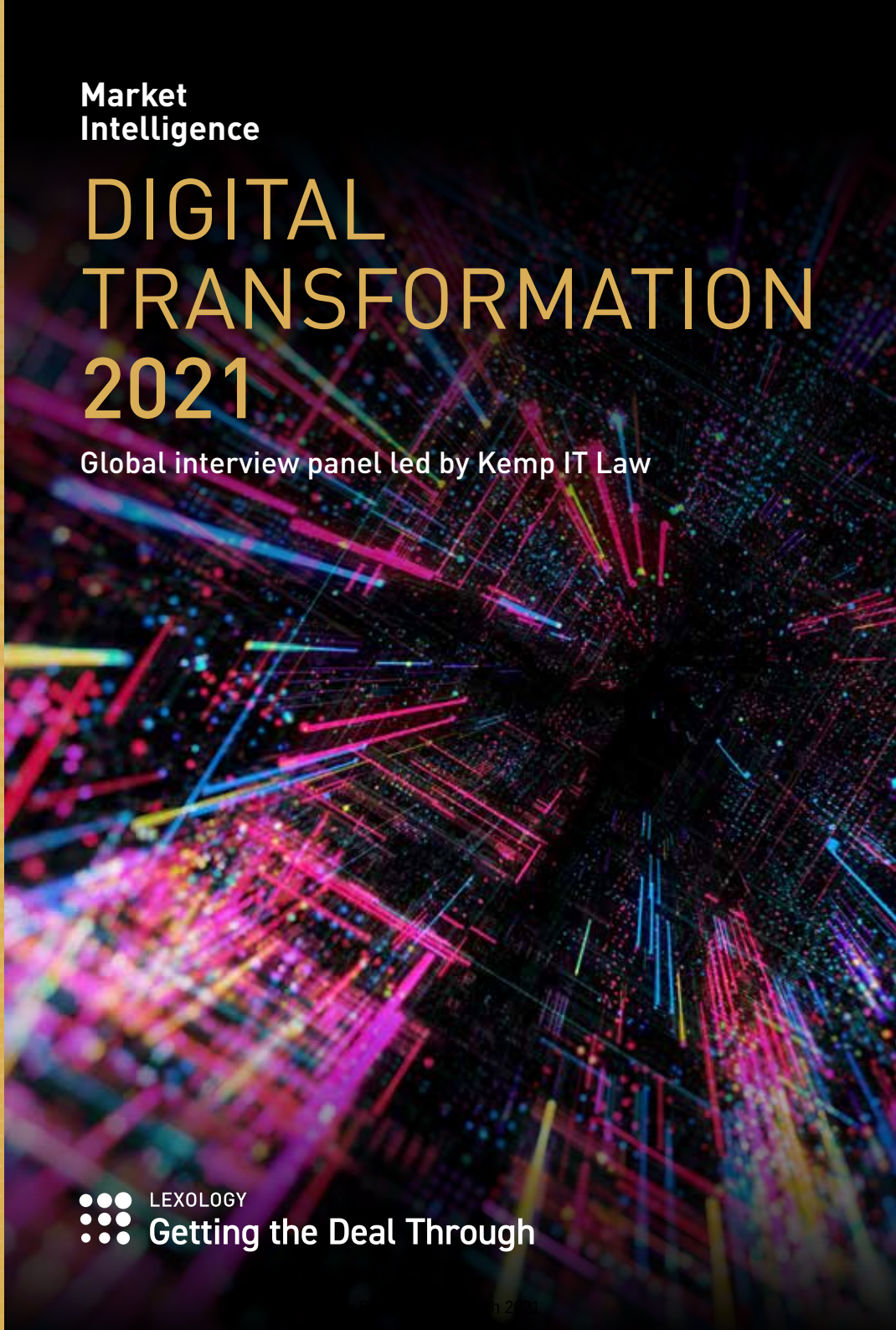
Market
Intelligence
DIGITAL
TRANSFORMATION
2021
Global interview panel led by Kemp IT Law
LEXOLOGY
Getting the Deal Through

LEXOLOGY
Getting the Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Printed and distributed by Encompass Print Solutions

DIGITAL TRANSFORMATION 2021

United States

Paul 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 healthcare IT company with multi-billion dollar annual revenues.

Austin 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 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.

Photo by Sean Pavone on Shutterstock

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 that impact businesses from a data processing perspective 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 that run in the cloud. Many of the laws that do apply actually favour internet-enabled processes over their paper counterparts, such as the safe harbours in the Communications Decency Act and Digital Millennium Copyright Act.

There are basic laws that apply, being mostly copyright, trade secret and contract law. For example, moving operations from internal operations to a third-party cloud environment may require modification of existing software licences. Software licensed on a per user basis may be impacted when the individual user is replaced by an AI implementation. Laws related to privacy and use of personal information do change when moving to internet-enabled solutions, so there is a greater need to be sensitive to those laws.

There are also many industry-specific laws and regulations and standards set by particular industries that may impact digital transformations, especially related to privacy and security. These regulated industries include financial services, healthcare, credit cards, governmental services, education and credit reporting, to name a few. There are a few US laws that 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. Information related to most commercial transactions, especially over the internet, and social media information does 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. The US simply does not have a comprehensive law for privacy or security. However, state law is starting to step into that void.

The absence of US Federal law means that each state has the ability to regulate. Accordingly, the United States is home to a growing and varied set of state laws related to privacy and security. We are starting to see state laws that 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 their own state borders.


Paul H Arne


Austin B Mills


Michael R Young

"The absence of US Federal law means that each state has the ability to regulate."

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?

Comprehensive new privacy laws in California, Colorado and Virginia come into effect in 2023. Many companies' existing compliance programmes will leave them poorly prepared to face these requirements, especially companies outside heavily regulated industries or without an international presence. Many of the following actions cannot be completed quickly, so prompt action is needed.

Map your data. Knowing the what and where of your company's data processing is practically necessary to support restrictions on sensitive information (such as social security number, health data or precise geolocation data) and required data retention limitations.

Review and revise notices. Updated notices and links are needed. Existing notices are unlikely to suffice.

Review third party relationships. There are new requirements on data sharing with third parties, including digital marketing providers. Existing contracts with vendors may need revision.

Establish new processes. The new laws expand consumers' rights to correct information. Companies will need to create a new 'appeals process' if requested changes are denied.

Undertake data protection assessments. Companies need data protection assessment policies for certain data processing, including targeted advertising.

Also, two recent developments at the US Federal level are likely to impact blockchain and crypto participants, particularly with respect to cryptocurrency: (1) the Infrastructure Investment and Jobs Act (Infrastructure Bill), and (2) the Sanctions Compliance Guidance for the Virtual Currency Industry (Compliance Guide) published by the Office of Foreign Assets Control (OFAC).

The Infrastructure Bill authorises the Treasury Department to require all brokers in digital assets to report personal information of counterparties, not only with respect to exchanges and trades, but also mere transfers (including to self-hosted wallets). The definition of 'broker' has been expanded such that miners, lightning nodes and similar participants may be impacted. However, the new requirements do not take effect until 2024 and may be revisited between now and then.

The Compliance Guide demonstrates that digital assets are a focus for sanctions enforcement. OFAC holds participants in the space – technology companies, exchangers, miners, wallet providers – to the same standards as non-blockchain technology providers. Companies are expected to screen available transaction or identifying data to prevent transactions with sanctioned parties and jurisdictions.

> “The Compliance Guide demonstrates that digital assets are a focus for sanctions enforcement.”

Extending the requirements to miners create special challenges, as miners may not have any practical way to perform the requisite transaction screening.

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 a cloud infrastructure. Data centre operations, with its 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 your business using someone else's data centre. When you use someone else's infrastructure for your business, you may not have the capacity to quickly take an application back into your in-house data centre. Frequently, cloud implementations mean that you don't 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 don't 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 no longer available unexpectedly? How are you going to get an infrastructure to operate your business? How long will this take? All of these questions should be asked and answered 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. 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?

Photo by f11photo on Shutterstock

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 have access to 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.

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.

It is important to understand that the responsibility for data breaches is not only a risk discussion but also a price discussion. No one does everything that is

Photo by Sean Pavone on Shutterstock

possible to protect computing systems and data. Spending more money can improve the chances that no data breaches event 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. One can also analyse and negotiate based on the types of damages that might occur and whether the agreed-upon obligations for data security 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 damages 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 these damages 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.

Customers of SaaS providers were much more likely a few years ago to insist that the data was 'owned' by the customer without thinking much more about this issue. Insisting that one 'owns' data tends to be less useful in negotiations than dividing 'ownership' into two different subparts: the right to use data for certain purposes and the right to exclude others from using 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 they are resolved varies significantly based on the industry, the type of data, the proposed uses and the relative negotiating strength of the parties.

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. Privacy and security is a constantly moving legal target.

Companies need a good privacy and security framework. While each new law should be examined, it is very useful to develop a framework that assesses what data it being obtained, used and generated by the company, 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. This is also a moving target, especially since the Privacy Shield has been invalidated and new standard contractual clauses are now required. Other than export and related regulations, which can be quite complicated, there is little regulation of data exports. US export law can be a challenge. For example, OpenSSL is an open source product, available to almost anyone in the world with an internet connection. If a company creates a product that invokes OpenSSL 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 exemption under the export regulations. The exemption frequently requires a filing with the US Bureau of Industry and Security. Export law covers more than many companies think it does.

8 What do organisations in your jurisdiction need to do from a legal standpoint to move software development from (traditional) waterfall through Agile (continuous improvement) to DevOps (continuous delivery)?

It is rare that we speak with a software company that hasn't moved to some form of Agile development methodology. Agile and SaaS tend to work well with each

"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. Development shops in large companies have more of a challenge in moving to Agile. Software development agreements, where third parties are providing development services, need to be different from traditional waterfall development agreements. The contractual means for managing risk in a waterfall development can be very different from managing risk in an iterative development. 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 be participating 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?

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 between scrum teams, such as standard data models or 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

The Inside Track

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

Part of our 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?

We provide 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.

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.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Covid-19 response
Government policy
Contractual negotiations
Cybersecurity & data protection