
Market
Intelligence
DIGITAL
TRANSFORMATION
2020
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

**Senior business development manager**
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

Cover photo: shutterstock.com/Quardia


ISBN: 978-1-83862-564-1

Printed and distributed by Encompass Print Solutions

# Digital Transformation 2020

# United States

Paul Arne 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, intellectual property protection, privacy, and security worldwide.

Paul chair's the firm's technology transactions practice. He founded and chairs the firm's open source practice.

Recent publications address identifying risks in blockchain implementations, the latest open source developments, emerging law related to screen scraping and other data gathering methods, software development agreements in light of Agile methodologies and the protection, or not, of application programming interfaces and other interfaces. Paul's publications have appeared in *Journal of Internet Law*, *The Computer & Internet Lawyer*, *Georgia State Bar Journal*, numerous Practicing Law Institute books and *The SciTech Lawyer*.

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 multibillion dollar annual revenues.

Paul Arne

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

There are few laws and regulations which place restrictions on digital transformation generally. Most laws and regulations 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.

There are basic laws that apply, being mostly copyright, trade secret and contract law. For example, moving operations from internal operations to a 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 concerning privacy and use of personal information may not change when moving from an internal computer-based operation to cloud computing, but there is a greater need to be sensitive to those laws.

There are also many industry-specific laws and regulations, as well as 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.

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 at times inconsistent, set of laws pertaining to privacy and security. Because commerce is typically not limited to a single state, individual state laws frequently have consequences outside of their own state borders. Data breach notification laws are a good example of this, where almost every state has a law that requires the giving of notice related to a data breach, but the requirements of each state vary.

## 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?

There are three developments on the horizon that may have a significant impact on digital transformations generally.

There has been a growing dissatisfaction with the scope of section 230 of the Communications Decency Act. Enacted in 1996, section 230 was part of the earliest attempt by Congress to regulate activities on the internet. Generally speaking, section 230 protects online providers of information from liability resulting from making available information that comes from another source. Over the years, this law has been broadly interpreted to protect online services from liability, including liability for defamation; violations of the US Fair Housing Act; fraud; money laundering; negligence claims; and making available terrorism-related information. The protections of section 230 related to sex trafficking were largely removed by Congress in 2018. There are a large number of proposals related to further erosion of this broad protection for companies that provide information services on the internet.

The US Supreme Court recently heard arguments in the long-running litigation between Oracle and Google, concerning the development of Google's Android mobile operating system. This case involves Google's use of the names of Java components – methods, classes and packages – as well as the syntax of inputs and outputs, rather

than the actual programming that accomplishes a particular result. The results of this case may have a broad impact on the scope of copyright protection for interface information, APIs, web scraping, software programming environments, metadata of all sorts and even the scope of a number of popular open source licences.

The California Consumer Privacy Act of 2018 (CCPA) took operative effect this year. The CCPA more closely resembles the European Union's General Data Protection Regulation (GDPR) than any other US law. In November 2020, California voters broadened and strengthened this legislation by passing the California Privacy Rights Act (CPRA). Frequently, laws related to technology and the internet are first enacted in California and then adopted, with some variation, in other states over time. The impact of the CCPA and CPRA on other states' laws may have a broad impact on the laws of privacy and security in the US.

## 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 their 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 no longer have the infrastructure, which means that you may not have the capacity to quickly take an application back into your in-house data centre. 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. Your 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 things 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.

"Companies should recognise the differences between having an in-house data centre and operating your business using someone else's data centre."

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 service (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 SaaS, 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 by a backhoe killed both systems. How much bandwidth

Photo by Sean Pavone on Shutterstock

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.

It is important to understand the roles and responsibilities of the parties. This is especially important in co-location (CoLo) relationships. Will the CoLo provider be responsible for rebooting the servers or installing the OS and virtualisation?

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 become important.

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 operating systems.

As time has progressed and organisations gain experiences with cloud services, on average they have become more and 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?

We 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 themselves. 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 safe, 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 possible to protect computing systems and data. Spending more money can improve the chances that a data breach or other untoward event will not 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, it may be that the amount of damages to be paid 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 level of detail in a security specification.

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 may be 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. These days, it is fairly rare that a SaaS provider will not want to use customer data for some purposes, especially outside of the healthcare and financial services industries. 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 and the right to exclude others from using data.

"It is important to understand that the responsibility for data breaches is not only a risk discussion but also a price discussion."

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 change the law related to privacy and security. For example, in this year alone, our cybersecurity and privacy practice group has regularly provided advice related to compliance with the CCPA and significant new privacy legislation in New York and Illinois, to name just a few. Privacy and security are constantly moving legal targets.

Photo by cate_89 on Shutterstock

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 is 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, such as isolating various computer systems from each other so that the compromise of one system does not necessarily compromise another, are critical.

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

As mentioned above, privacy and security laws and regulations are a moving target. Complying with these 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. 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 incorporates OpenSSL to encrypt data, 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 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 communicate with a software company that hasn't 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. 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 development normally requires the development 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. Often, the customer should be participating in the process of developing the tasks to go in the sprints.

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

In a large company context, 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 will frequently 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 and development standards.

Paul Arne
parne@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?**

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 concerning 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 how it is delivered. This is an education process with clients. Creating such a contract also frequently forces emerging companies to hone their business model. My job involves the ability to talk technically to software developers and translate what they tell me into accurate contract language. There is a certain talent that one must develop in order to get the needed information out of a software engineer.

**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 evaluate and mitigate risk. Outside of very rare criminal-type activities, it is our job to fully inform our clients and then let them decide whether to take a risk or not.

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

an LBR business

ISBN 978-1-83862-564-1