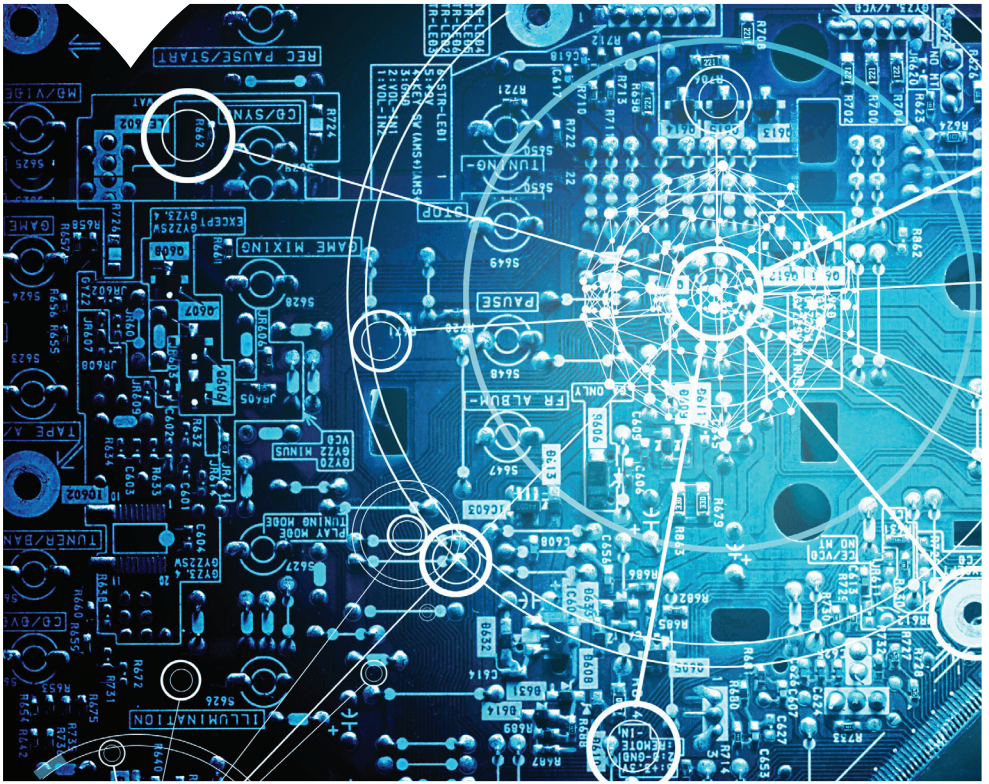
MAYER · BROWN

Thriving in an Age of Digital Transformation

Insights from Mayer Brown's Technology Transactions Practice



Mayer Brown's Technology Transactions Practice

For more than 20 years, Mayer Brown's cutting-edge Technology Transactions practice has helped customers develop and manage high-value relationships with providers of critical services and technology in some of the largest outsourcing and software transactions ever attempted. In recent years, we have orchestrated technology transactions that have helped a growing number of clients implement digital and data-driven strategies.

Our practice includes more than 50 lawyers throughout the Americas, Asia and Europe who have achieved top ratings from prestigious directory publishers and professional associations, including, *Chambers*, *The Legal 500* and the *International Association of Outsourcing Professionals*. Many of our lawyers have worked as in-house counsel for outsourcing providers and in business or technical roles for leading outsourcing, technology, and supply chain companies.

Mayer Brown's client roster includes some of the most recognizable names in the business world, including many who turn to us repeatedly as their technology transaction needs become ever more complex. We have leveraged this experience to drive value for our clients on thousands of technology transactions and to advise them on market-competitive terms in areas including:

- Data rights, use, privacy, and protections
- Digital services
- Outsourcing
- Software development, licensing, and integration

Authors

Marina G. Aronchik
Associate

David L. Beam
Partner

Lindsay T. Brown
(*Former Associate*)

Nickolas S. Card
Associate

Corina Cercelaru
Associate

Paul A. Chandler
Counsel

Qi Chen
Associate

Julian M. Dibbell
Associate

Rebecca S. Eisner
Partner

Daniel Gallagher
Associate

Rohith P. George
Partner

Marjorie H. Loeb
Partner

Daniel A. Masur
Partner

Donald J. Moon
Associate

Riley C. Moore
Associate

Brad L. Peterson
Partner

Mark A. Prinsley
Partner

Kevin A. Rang
Partner

Linda L. Rhodes
Partner

Lei Shen
Partner

Dean C. Won
Associate

Oliver Yaros
Partner

Contents

2018 Trends in Data, Digital, Outsourcing, and Software	1
The Future of Outsourcing	11
International Developments in Privacy Laws and Vendor Agreements	19
Software Development in a Dynamic Environment	29
How Smart, Connected Products Are Transforming Business	41
Data Licensing—Tips and Tactics	51
ERP in the Cloud	59
DOs and DON'Ts for Big Data Analytics	69
Blockchain for Business	79
Contracting for Facilities Management Services in the Proptech Era	89

2018 Trends in Data, Digital, Outsourcing, and Software

2018 Trends in Data, Digital, Outsourcing, and Software

2018 Trends in Data, Digital, Outsourcing, and Software

Rebecca S. Eisner, Daniel A. Masur, Brad L. Peterson, and Mark A. Prinsley

In this article, we provide an overview of four major trends that we anticipate will have a significant impact on technology transactions through the remainder of 2018: data at the core, data protection and security, continuing demand for digital services, and regulatory responses.

Data at the Core

In 2018, the hot technologies appear to be those focused on new ways to gather, store, analyze, and exploit data. Connected devices are gathering vast amounts of new data, which are then stored on new cloud-based database platforms and analyzed using new advanced analytics tools, often to deliver products and services that didn't exist a few years ago. These new technologies are spawning entirely new categories of companies, such as fintech, insurtech, medtech and proptech, where digital-native startups are competing with and even disrupting established industry leaders.

CONNECTIONS AND DATA

In this technology-saturated business environment, companies face an expanding number of digital connections and an explosion of data. As a result, value has shifted to how companies integrate, orchestrate and curate their connections and how they gather, store and exploit data to achieve their missions.

This shift in value naturally shifts the focus for technology transactions lawyers. Increasingly, technology transactions lawyers are looking beyond technology services, requirements and rights to integration, governance, decision rights, and outcomes. We also anticipate continued focus on data governance, privacy compliance and cybersecurity risk management to protect the value that companies have created in data.

BIG DATA ANALYTICS

The value of data is being unlocked with machine learning, artificial intelligence and other big data analytics tools. Those tools are delivering business value by producing actionable insights and augmenting human skills in judgment-based functions. One key fact is that the big data analytic tools "learn" instead of being programmed. As a result, it is often difficult or even impossible to limit how they use data or to explain why they deliver the insights that they deliver.

The exponentially growing power and wider implementation of big data tools demand attention in related technology transactions. The resulting insights produced may not be protected by intellectual property laws at all and therefore must be protected in different ways than traditional outputs. The big data tools must be restricted to the rights that the contracting parties have in the input data and, under some laws, only to explicable insights. Transactions must be designed around desired possible insights not a promise of meeting "requirements."

Data Protection and Security Issues Continue to Drive Negotiations

Privacy and cybersecurity requirements continue to be among the most hotly contested areas in technology transactions. The evolving law and technology in this area will continue to drive these negotiations as customers and providers alike scramble to meet requirements and develop reasonable contract terms and allocations of risk.

As described separately elsewhere in this booklet, 2018 will be another year of adapting to new privacy and data security requirements. In the United States, individual states and regulators have been active drivers of new legal standards. In the European Union, the General Data Protection Regulation (GDPR) introduces new legal standards, such as data protection impact assessments, privacy by design, restrictions on profiling and automated decision-making, data breach notification requirements, data portability, the right to be forgotten, and a host of other technical and organizational measures, with more laws following.

China's new Cybersecurity Law (CSL) requires that data collected or generated in China during business operations be stored in China unless the entity subjects itself to a security assessment and shows that cross-border transfer of the data is necessary for its business.

The Internet of Things, biometrics such as facial recognition, and other emerging areas that rely on regulated data will continue to drive new legal requirements and create new risks in technology transactions. Given the rapid pace of change accompanying these newer technologies, the continued string of high-profile data breaches with traditional technologies and the heightened requirements for compliance described above, 2018 is a good year for re-evaluating existing technology provider selection and due diligence practices, confirming that security and privacy standard clauses are up-to-date and refining the process for ongoing monitoring of third parties.

Demand for Digital Solutions Continues to Grow

We see businesses in all sectors continuing to quickly adopt digital solutions for existing processes and to use digital technologies to develop new business models.

Adopting cloud computing appears remains top of the agenda in the near term. Infrastructure as a Service (IaaS) cloud models continue to replace traditional data centers. Software as a Service (SaaS) cloud models are now readily adopted for even mission-critical, core applications, such as finance, human resources, customer relationship management, inventory and other "Enterprise Resource Planning" (ERP) systems. If done well, each requires a technology transaction.

On the near horizon, and in proof of concept, is automation of manual processes. Technology referred to as "robotic process automation" (RPA) is being used to automate rules-based processes, particularly in "swivel chair" applications. Artificial intelligence (AI) is being used for voice recognition, chatbots and other pattern-matching work, with more advances to come.

As described elsewhere in this book, these technology changes are changing outsourcing. Cloud, RPA and AI are increasingly allowing automation of repetitive tasks and some analytical work that is currently outsourced. Traditional outsourcing service providers are being challenged to integrate these new technologies while maintaining required levels of quality, consistency and speed. At the same time, faster change is reducing the willingness of customers to agree to the longer terms that traditionally allowed outsourcers to recover large initial investments.

On the far horizon are blockchain and other forms of distributed ledger technology (DLT). Blockchain and DLT are discussed separately in this book. The possibilities for blockchain to provide a trusted repository and facilitate trusted transactions without intermediaries appear limitless.

Examples of Regulatory Responses

INTEROPERABILITY OF DATA

Interoperability of data allows competitors to share digital data effectively. In the United Kingdom, the interoperability of data is central to the Small and Medium Sized Business (Finance Platforms) Regulations, whose impact will continue to grow in 2018. Essentially, under these regulations, banks that refuse to finance small business on terms that are acceptable to the small business will, subject to consent of the proposed borrower, be required to pass the information about the loan applicant to designated finance platforms, which will provide access to this data to lenders participating in the platform. The aim is increased competition and the availability of financing to small businesses in the United Kingdom. This type of initiative is unlikely to be a one-off; businesses should consider how new digital technologies might be adopted to share data among competitors in a rapid and open way.

ANTITRUST CONTROLS ON DATA PLATFORMS

We see increasing interest in 2018 by antitrust authorities in businesses using big data. Issues that might be relevant to the authorities are whether there is, in fact, anything unique about data that can be freely obtained from consumers and others and whether data businesses are innovating, offering customers new solutions. For example, the European Commissioner for Competition is looking at whether, in effect, one market participant's control of data excludes new competitors.

TRUMP ADMINISTRATION

Actions taken and actions proposed by the Trump administration will have a direct, and potentially profound, impact on the sourcing industry. These include:

US Tax Law. The US "Tax Cuts and Jobs Act," signed December 22, 2017, will directly impact the economics and structure of cross-border sourcing arrangements. Both customers and providers should evaluate existing and planned sourcing arrangements to determine whether they can take advantage of these changes. For example:

- Changes to the rules governing the deductibility of asset purchases may drive changes in whether the customer or provider acquires and retains ownership of equipment and software.
- New concepts with exotic names—such as "GILTI" (global intangible low-taxed income), "FDII" (foreign derived intangible income) and "BEAT" (base erosion and anti-abuse tax)—may drive changes in how sourcing transactions are structured, whether services are delivered from US or offshore locations, how services are delivered to a customer's non-US affiliates, and how charges are invoiced and paid.

The effects are complex and will vary from deal to deal and company to company, so it is important to consult with a tax adviser. (For more information, please see our January 9, 2018 Legal Update, *How the Tax Cuts and Jobs Act Will Impact Outsourcing*," which is on www.mayerbrown.com.)

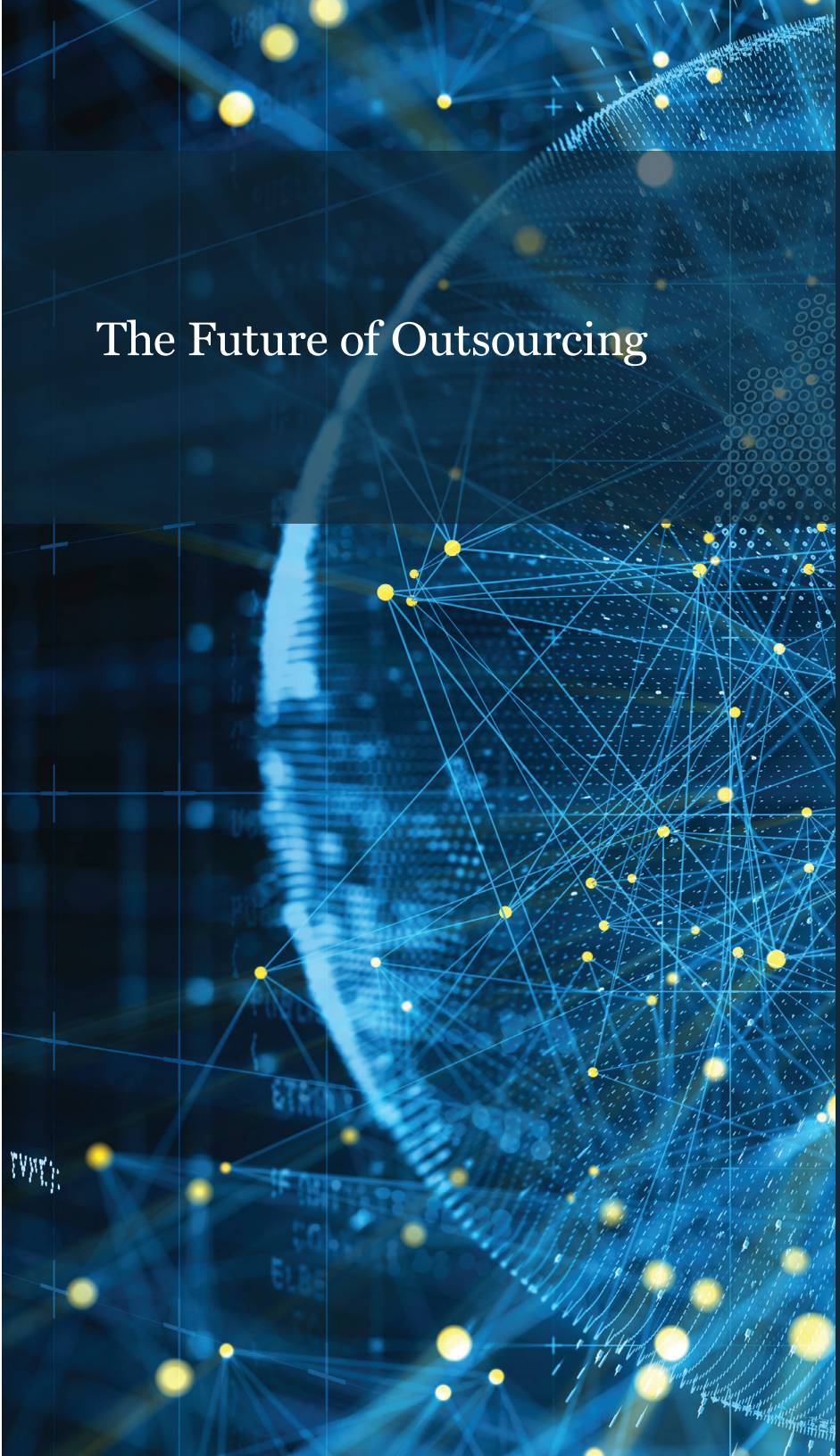
H-1B Visas. The Trump administration has proposed changes in the rules governing H-1B visas and has stepped up its enforcement of the existing rules governing those visas. The stated intent of the Trump administration is to avoid depressing US worker wages and to limit visa awards to what the administration calls the "best and the brightest." However, as a practical matter, the actions will significantly impact technology service providers, especially Indian heritage providers. The preferred service delivery model of many providers relies heavily on bringing offshore resources, particularly Indian nationals, to the United States using H-1B visas. For example:

- H-1B visas typically granted with ease to IT professionals with university STEM degrees are likely to be denied if the candidate is making an entry-level wage or has a degree that is not clearly related to the precise occupational category.
- The US Departments of Homeland Security and Labor are actively enforcing the "right to control" obligation of employer sponsors of H-1B visa holders, which requires the provider to directly supervise day-to-day activity and personnel actions. Failure to do so can result in denial of visas and even debarment of the provider from the H-1B visa program.
- The US Department of State is scrutinizing H-1B visa support documentation supplied by the customer in order to detect fraud. To ferret out abuses, the agency is directly contacting the customer to verify the job details of the H-1B resource and the genuineness of the documents being presented by the provider.

Political Uncertainty. Finally, as we noted last year, the sourcing industry is impacted by political uncertainty in both the United States and abroad. The Trump administration has repeatedly promised to protect American jobs by making major changes in trade agreements, regulations, corporate taxes and visa restrictions, all of which may ultimately impact outsourcing models based on global labor arbitrage. As we just discussed, these are not idle threats—the administration has already taken decisive action in at least two of those areas.

In addition, in our view, the political climate is accelerating the move to the cloud, "as-a-service" offerings, robotic processing, artificial intelligence, utility offerings and other sourcing models offering cost savings not based on offshore labor arbitrage. While these sourcing strategies may result in the elimination of American jobs, they cannot be attacked as offshoring jobs to foreign countries.

The Future of Outsourcing



The Future of Outsourcing

The Future of Outsourcing

Rebecca S. Eisner, Daniel A. Masur, and Brad L. Peterson

The future of outsourcing is digital. Outsourcing providers will increasingly use digital systems to offer faster, smarter, better and cheaper services. Functions currently performed by people will increasingly be automated. Outsourcing contracts built on the traditional assumption that the services are provided by people supported by tools will be fundamentally changed to reflect that the services are provided by digital tools supported by people.

Traditional Outsourcing in the Rear View Mirror

Traditional outsourcing started with IT specialists running massive computing equipment in data centers in the 1960s using knowledge and skill developed from serving numerous customers. Later, outsourcing innovators found ways to use shared service centers to have teams of people deliver a wide range of business processes to many customers. When low-cost global connectivity became available, outsourcing innovators created shared service centers using people in low-cost locations to share the benefits of those services across a global customer base. More recently, advances in grid computing and virtualization allowed outsourcing innovators to share use of standardized IT infrastructure in what has been called "cloud" and cloud-based software in one-to-many "Software as a Service" (SaaS) models.

Adoption cycles for new types of outsourcing have begun with waves of small, innovative deals, including pilot projects and deals with previously unknown players. In the offshoring era, buyers were puzzled by, and later embraced, previously unknown Indian companies. The cloud era surprised buyers with new leadership from an online bookseller, a software company and a search engine provider, along with hundreds of venture-funded point-solution SaaS providers. As integration challenges increase and some providers develop winning solutions, leading providers have emerged.

Each new type of outsourcing has added a lane to outsourcing instead of fully replacing prior types of outsourcing. For example, customers continue to outsource data center management. With each new lane, the ecosystem of outsourcing providers and advisors have pivoted—successfully thus far—to find new ways deliver the next 10 percent to 30 percent of customer savings and value using new processes and technologies, while outsourcing lawyers have found contractual and compliance solutions to address the new risks in the new lane.

The Digital Outsourcing Lane

Switching our gaze from the rear view mirror to the road ahead, we see a new lane that we call "digital outsourcing." Unlike traditional IT and business process outsourcing, the services in digital outsourcing are performed entirely by machines instead of people. In this new lane, people create digital execution strategies, maintain and configure digital systems, handle exceptions, integrate across digital platforms, monitor outcomes, and interpret data. However, people do not directly perform the services. Unlike a traditional cloud provider, a digital outsourcing provider takes responsibility for performing a customer-specific business function instead of providing a standardized one-to-many service.

In the near term, the quick wins in the digital outsourcing lane are coming from software dubbed "robotic process automation" (RPA). RPA software operates at the presentation layer (so it looks to a software application like a human user). RPA software can be programmed to carry out rules-based tasks now performed by people in traditional outsourcing deals.

A larger opportunity, but further away, is artificial intelligence (AI). AI is being used today to replace human spoken conversations with "chatbots," to replace drivers with autonomous vehicles and to derive human-like insights from patterns in data. In the future, AI may be able to provide services that are beyond human capabilities.

Still farther down the road, we see digital outsourcing providers providing and maintaining blockchains and other shared digital

ledgers to store information and effect transactions for multiple customers. These technologies would create savings by having a single system of record for many companies instead of having each company maintain its own system of record.

Digital outsourcing will gradually replace the work in the other lanes, but we expect the other lanes to continue. There is a great deal of currently outsourced work that is too idiosyncratic, unstructured or inherently human to automate. Innovation, creativity, relationship building, physically delivered services, software maintenance, and adapting to technological and market changes are well beyond the headlights of digital technology for the near future. We thus expect to see both digital and traditional outsourcing lanes for years to come, much as providers have delivered both offshore and onshore outsourcing services in past years.

Changing Lanes from Traditional Outsourcing Terms to Digital Outsourcing Terms

The best contract terms for digital outsourcing are fundamentally different than the best contract terms for traditional outsourcing. The differences are not merely a few terms to be addressed a simple rider but are instead pervasive. For example:

- **Transition** is no longer merely knowledge transfer and training but also includes programming, testing and acceptance of the provider's automations and integrations with retained systems. However, transition investment is reduced, because fewer people are trained and fewer assets are transferred. These changes continue the long-term trend of reducing transition costs and thus reducing the need for long contract terms to recover the provider's investment in transition.
- **Scope** is not FTEs performing designated tasks in accordance with policy and is instead completing defined actions, producing specific outputs, or achieving specific outcomes. This requires a shift from role descriptions and sweep clauses to defining what problems the

provider is to solve and how to measure how well the provider has solved those problems.

- **Service levels** do not measure processing speed and accurate transcription (which are almost inherent for digital labor) and instead measure, for example, how quickly coding defects are corrected, the percentage of work slowed by exception handling or the value of the outcomes generated.
- **Governance provisions** become more important because the seamless digital interface removes the opportunity to solve problems by talking directly with the people performing the services. Governance provisions must establish a connection to the "bot managers" who can change how the digital service works and the "exception managers" who can change how people do what the automated service cannot do.
- **Personnel** provisions requiring good and workmanlike effort by adequate numbers of suitably experienced, qualified, trained and drug-tested people, which serve as a proxy for quality in traditional outsourcing agreements, become less important. Promises of quality shift to the quality of actions, outputs or outcomes versus the quality of the humans who are acting.
- **Pricing** moves from charging for effort to charging for actions, outputs and outcomes. Pricing thus is less about wage costs and the difficulty of scaling human operations. Pricing based on actions, outputs and outcomes requires higher levels of drafting skill and understanding of the business, particularly if the results depend on actions by the customer.
- **Change control** becomes focused on changes that will require changes to the automations and integrations. The customer can no longer assume that the people on the supplier team will figure out minor changes. The complexity of change control is thus increased, particularly if the digital outsourcer is acting as an integrator of evolving third-party technologies or running processes that are deeply integrated with processes retained by the customer.

- **Technology standards** focus on the customer's ability to exchange data effectively with the provider and to take back responsibility for the service upon an expiration or termination. A common approach, for example, is to designate the type of RPA software used to create "bots" to automate repetitive tasks. That allows the customer to take back responsibility for a function by getting a copy of the RPA scripts and licensing the RPA software.
- **Data security** focus less on policies designed to teach and control the people performing services to and more on policies and tools designed for digital cybersecurity threats.
- **Data localization** requirements might be addressed by having local processing of local data on local servers (although this represents a real challenge to blockchain and distributed ledger systems).
- **Data rights** become more central and more contentious because the digital system may generate derived data and insights that human workers could not identify. This may be a new source of value in the outsourced process, generating new revenue or savings opportunities for the customer if the supplier has the obligation to pass them along. Increasingly, we are seeing providers asking for the right to monetize the insights they gain from sitting astride flows of customer data.
- **IP rights** fundamentally change, and must be addressed by contract, because machine creations may not be property under copyright laws written to protect only human creations.
- **Third-party consents** may be required for use of automated services with licensed software or cloud subscription agreements. Some prohibit interfaces with robotic users. Some deem use by RPA software as "indirect use" by the people who get data through the RPA software, which could create noncompliances or surprise charges.
- **Exit rights** continue to include the return of customer data and the provision of reasonable transition assistance. However, if the digital outsourcing is performed on a multi-client platform, there may be no people, software, equipment or facilities to transfer. Functions that

are performed using "black box" AI technology may be impossible to transfer to other AI platforms. Additional services may be required to decouple integrated processes.

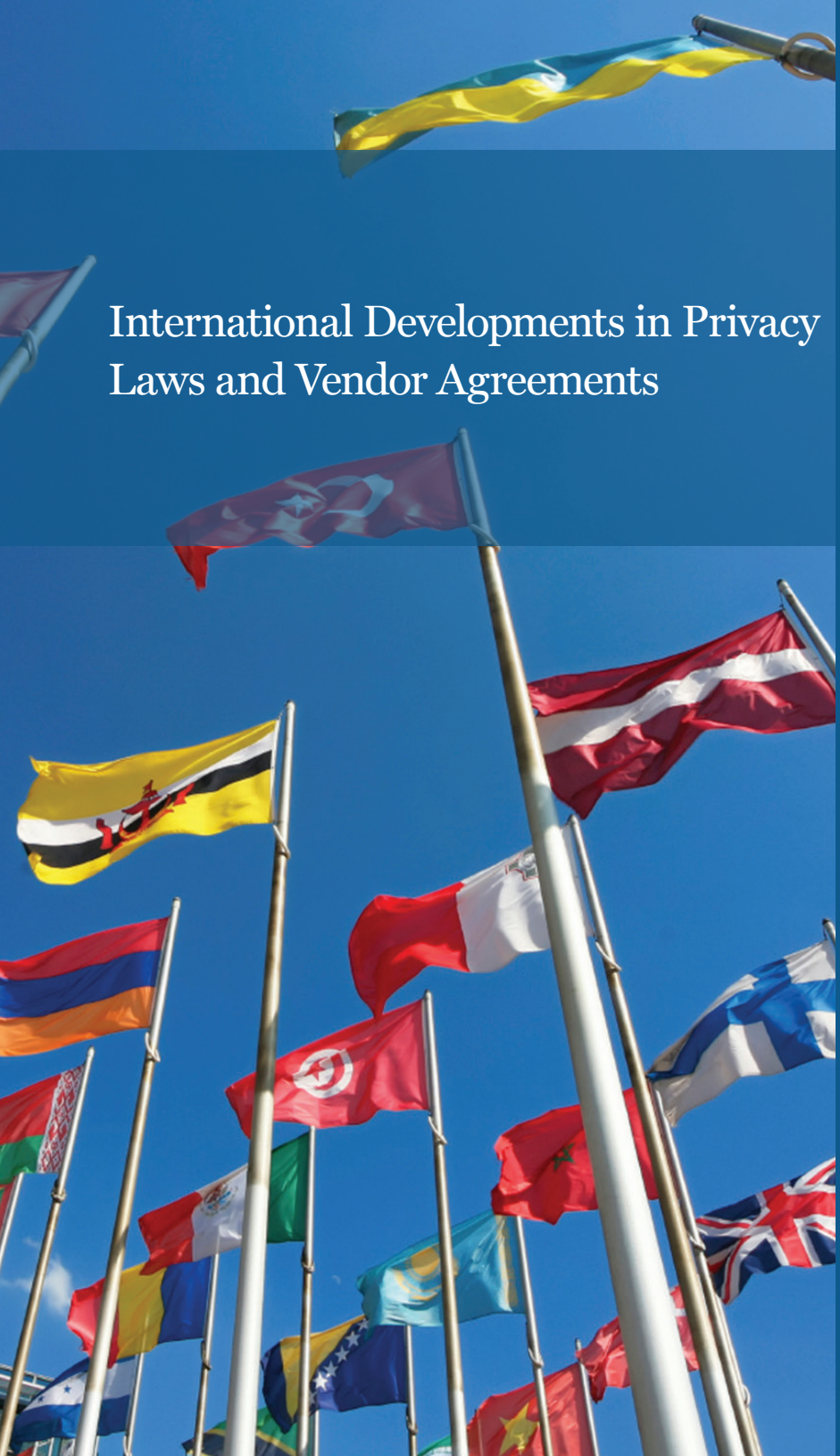
Where to Go Next

Digital transformation is creating a new lane for outsourcing. For you to maximize value and avoid pitfalls in that new lane, you need new and different contract terms in both existing and new contracts and to adapt third-party contracts to digital outsourcing. That adaptation requires investments in understanding the digital outsourcing model and outsourced businesses and adopting new sourcing, contracting and governance approaches.

The opportunities are not limited to new deals. Your current outsourcing providers likely have begun digital outsourcing under traditional outsourcing terms. They may have stayed quiet about the changes, preferring to capture all of the cost, data and other benefits of new technologies and to avoid taking on new contractual obligations described above. To maximize value and avoid pitfalls, we recommend that you identify the changes that existing providers have made, send correspondence noting the changes required approval under your contract and renegotiate to obtain suitable protections.

With respect to both current and new deals, smart investments include updating forms and policies to include digital outsourcing terms where applicable, planning larger investments in deal structuring and negotiation to address novel issues, and adapting governance specific for digital outsourcing. With those investments, your company will be able to maximize value and avoid costly pitfalls in digital outsourcing, the new lane on the outsourcing highway.

International Developments in Privacy Laws and Vendor Agreements



International Developments in Privacy Laws and Vendor Agreements

International Developments in Privacy Laws and Vendor Agreements

Lei Shen, Oliver Yaros, Qi Chen, and Daniel Gallagher

Cybersecurity and data privacy increasingly have been a topic of focus around the world, and developments in this realm are increasing at a rapid rate. Several countries have recently implemented new laws and regulations focusing on data protection. These developments will have an impact not only on how companies operate, but will also affect what they need to include in their agreements with their third-party vendors that have access to personal data. Below are some of the recent developments in the United States, the European Union, and the Asia-Pacific region.

Developments in the United States

STATE LAWS

In 2017 and early 2018, several states moved forward with legislation addressing security and data privacy concerns. In March 2018, Alabama became the 50th state to enact a data breach notification law, which, like a small group of others, imposes a specific notification deadline of 45 days after the discovery of a breach. A number of states have broadened the definition of personal information (e.g., a user name and password) in their state laws in recent years. Since many national and international companies do not distinguish data by state residency, when data that are subject to different state requirements are intermingled, companies must observe the strictest state standards for all of the data. On the privacy side, Washington State became the third state—after Texas and Illinois—to enact a law regulating the commercial collection and use of biometric information.

NEW YORK STATE FINANCIAL SERVICES REGULATION

The New York State Department of Financial Services (NYDFS) adopted a cybersecurity regulation that mandates cybersecurity

standards for all institutions authorized by NYDFS to operate in New York, including many banks, insurance entities and insurance professionals. Significant provisions of the cybersecurity regulation became effective in 2017, and other provisions will be phased in throughout 2018 and 2019. The cybersecurity regulation is quite comprehensive and addresses everything from access controls and encryption to data disposal and employee training. It requires covered entities to report to NYDFS on the occurrence of a broad range of cybersecurity "events" that include attempted or successful data breaches, security incidents, hacking and intrusions. It also includes requirements for third-party service providers. Following the enactment of the final cybersecurity regulations for New York's financial services sector, state financial regulators in Colorado and Vermont adopted their own cybersecurity rules that would apply to certain entities doing business in their states.

Developments in the European Union

GDPR

The new European General Data Protection Regulation (GDPR), which will replace EU Data Protection Directive 95/46/EC (EU Directive) on May 25, 2018, will bring with it a number of significant changes from the EU Directive, including significant fines, breach notification requirements, a change in jurisdictional scope, new data subject rights and direct processor requirements. Even businesses that are established outside the European Union will be subject to the GDPR as data controllers if they process personal data in relation to the offering of goods or services to individuals within the European Union or to the monitoring the behavior of individuals in the EU. Accordingly, businesses that previously were not subject to the EU Directive may become subject to the GDPR.

Under the GDPR, businesses must notify the relevant EU data protection authority of a data breach without undue delay and, where feasible, within 72 hours (unless the breach is unlikely to result in a

risk to the individuals concerned). They must also notify individuals of a data breach without undue delay if a breach is likely to result in a high risk to the individuals concerned.

The GDPR will introduce significant other changes and additional requirements that will also need to be addressed by businesses, such as data subjects' "right to be forgotten," the requirement to implement data protection by design and by default, and the requirement for data protection impact assessments.

To address concerns regarding how to comply with the various new requirements, several data protection authorities, as well as the A29WP, have been releasing and will continue to release guidance concerning the GDPR. For example, the A29WP has released guidelines on the right to data portability, data protection officers (DPOs), data protection impact assessments (DPIAs), data breach notification, and other topics. The UK's ICO has also released draft guidance on contracts between controllers and data processors and how to obtain consent under the GDPR. Additional guidance is expected in 2018.

NIS DIRECTIVE

The EU Network and Information Systems Directive 2016/1148 (NIS Directive) will also take effect in 2018. The NIS Directive requires providers of essential services (which, for the purposes of the NIS Directive, are services that are essential for the maintenance of critical societal and/or economic activities that rely on network and information systems, which, if subject to a cybersecurity incident, would have a significant disruptive effect on the service) or digital services with an establishment in the European Union (or not established within the European Union but offering an online marketplace, search engine or cloud computing service in the European Union) to notify of cybersecurity incidents to the relevant authority without undue delay if those will have a significant (essential services) or substantial impact (providers of an online marketplace, search engine or cloud computing service) on the continuity of the services being provided.

Developments in the Asia-Pacific Region

While many countries in the Asia-Pacific region have lagged behind North American and EU countries with respect to cybersecurity and data privacy in the past, recent developments show that countries in this region are starting to make significant changes in this area.

CHINA AND THE CSL

One big development is China's enactment of its new Cybersecurity Law (CSL), the first comprehensive law in the country's history to focus on cybersecurity. The CSL took effect in June 2017. The law is controversial as it may require data collected or generated in China during business operations to be stored in China unless the entity subjects itself to a security assessment and shows that cross-border transfer of the data is necessary for its business. Many of the details on the data localization requirement (such as exactly which entities must comply with the requirement) are still ambiguous, and China is expected to release new measures and specifications related to the CSL in the future to clarify these ambiguities. China released one such specification in December of 2017 called the "Information Security Technology – Personal Information Security Specification" (PI Specification). The PI Specification is not mandatory but provides detailed guidance on the collection, storage, use, transfer and disclosure of personal information, as well as organizational standards and data breach responses for personal data controllers, which will likely be referenced by Chinese regulators in their enforcement of the CSL. The contents of the PI Specification generally reflect the requirements of personal information standards adopted by other jurisdictions around the world (e.g., consent to collection of personal information and obligation to protect the personal information collected). While many have criticized the data localization requirement in the CSL, it appears other countries in the region, such as Vietnam, are also considering similar requirements in their draft cybersecurity laws.

OTHER DEVELOPMENTS IN THE ASIA-PACIFIC REGION

Other countries across the Asia-Pacific region are also moving toward tighter regulations and stronger enforcement with regard to cybersecurity and data privacy.

Korea is requiring service providers to obtain permission before accessing data or functions on a user's smart phone, and such providers may not deny service to users if the user refuses to give permission for data or functions that are not necessary to the provision of the service.

India is expanding the definition of cybersecurity incidents to include attacks in addition to actual breaches and is moving toward requiring all businesses to report cybersecurity incidents to the Computer Emergency Response Team (CERT), India's official cybersecurity agency.

Australia passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016 in February 2017 requiring organizations to immediately notify the Office of the Australia Information Commissioner and the affected individuals of data breaches that are likely to result in serious harm. The amendment will take effect in February 2018.

Smaller countries have also been active in the cybersecurity and data privacy area. Singapore and Vietnam both released comprehensive draft cybersecurity laws for public consultation in 2017. Taiwan is deliberating a bill to require providers of its critical infrastructures to develop information security plans and notify the authorities in the event of security breaches. Indonesia established its first national cyber agency in June through a presidential regulation.

Updates to Vendor Contracts

In light of the developments above, agreements with third-party vendors that will have access to your personal data should be reviewed in order to ensure that they comply with these developments in data protection laws. Below are some of the issues that should be considered when undertaking a review of your vendor agreements.

GDPR

The most significant issue that you will need to consider is whether you are subject to the GDPR and whether your vendors will be processing EU personal data on your behalf. If so, you will need to revise your vendor agreements to comply with the GDPR—in particular, its Article 28, which sets out a list of items that data controllers must include in their contracts with vendors that process EU personal data on their behalf. If your agreements already comply with the EU Directive, some of the requirements of Article 28 may already be adequately dealt with (for example, that the processor only processes personal data on the documented instructions of the controller and that it has appropriate security measures in place). The new requirements for contracts with vendors that process EU personal data on your behalf include the following:

- The contract must include a description of the subject matter and the duration of processing, its nature and purpose, as well as the types of personal data being processed in respect of which categories of data subjects.
- There must be an obligation on the vendor to assist you with your obligations under Articles 32 to 36 of the GDPR, which include assisting you with notifying a supervisory authority or a data subject of a data breach and conducting data protection impact assessments.
- The vendor must agree to assist you so that you can comply with your obligations with respect to requests from data subjects that are exercising their rights under the GDPR.
- The vendor must make available to you all information necessary to demonstrate compliance with its obligations under Article 28 of the GDPR and must allow for and contribute to audits by you or another auditor mandated by you.

- The vendor must ensure that all of its personnel who process personal data are bound by confidentiality obligations.
- The contract must require the vendor to delete or return (at your option) all of the personal data at the end of the services relating to such processing and to delete any existing copies of the personal data (unless otherwise required by EU law).

In addition to the above, you should also review and consider whether other provisions need to be updated to reflect the GDPR's requirements, including data transfer restrictions and liability provisions, to address the increased potential fines under the GDPR.

DATA BREACH NOTIFICATION REQUIREMENTS

Several new laws and regulations, including the GDPR, add new data breach notification requirements. For example, the GDPR adds data breach notification requirements for both data controllers and data processors. You may need to update your vendor agreements to include data breach notification requirements or update the time frame in the agreement to ensure the vendor notifies you with enough time for you to meet your own notification requirements.

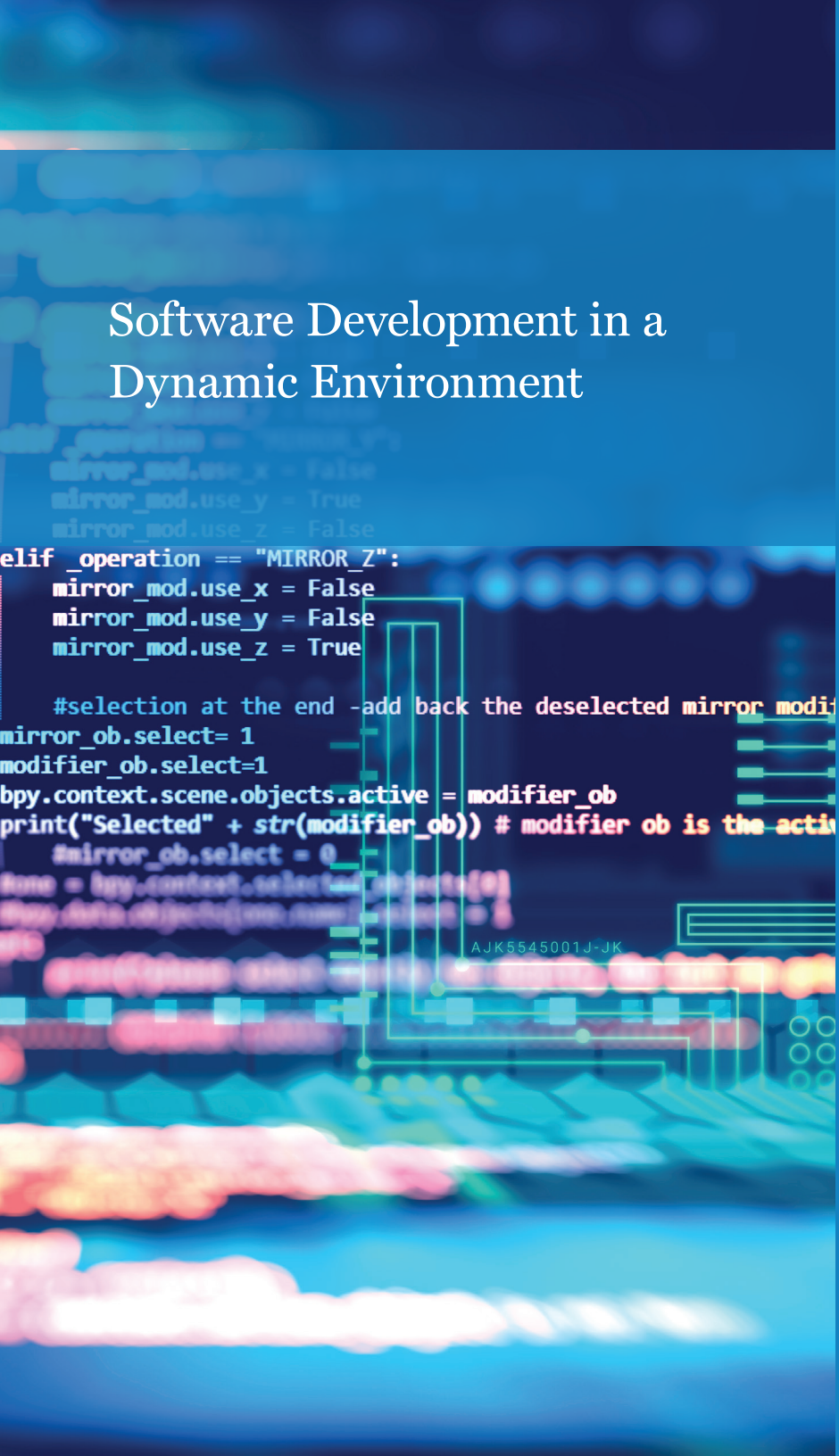
CYBERSECURITY REQUIREMENTS

You may also need to update your vendor agreements to ensure that your vendors meet certain minimum cybersecurity requirements. You may also want to consider drafting your own minimum security requirements that your vendors must meet to handle your data.

DATA LOCATION

Finally, you may want to require that the vendor only store and process your data within certain jurisdictions, both to address any data localization requirements and any data transfer restrictions.

Software Development in a Dynamic Environment



Software Development in a Dynamic Environment

Paul A. Chandler and Nickolas S. Card

Introduction

Software systems, and efforts to develop them, are growing increasingly complex. In the past, software commonly operated in a stand-alone manner and often was built to meet a business's detailed specifications. Today, most software must interact with a range of external systems. Development happens rapidly, often without detailed specifications, based on evolving goals, leveraging open source software, "SaaS" offerings and other pre-existing building blocks. While these trends reduce development costs, shorten project timelines and offer new capabilities, they also increase the complexity of software development and undermine traditional contracting and licensing approaches. Today's contracts for complex software development should therefore be different than those for traditional software.

This article will describe key trends in modern software development and related contracting concepts, the impacts of using of open source and other third-party software on software development, and the management of software integration with SaaS offerings and other changing third-party systems. This article will also explore contractual approaches to mitigate risks and promote the success of the software development process.

What Makes Today's Software Systems So Complex?

Today's software systems provide capabilities unimaginable before the rise of the Internet and cloud computing, while at the same time keeping the extreme complexity of these systems largely hidden from users. Everyday examples include ecommerce websites that process sales transactions, enterprise resource planning (ERP) systems that

manage the operations of global companies, IoT (Internet of Things) applications that process streaming data from large numbers of remote distributed sensors, and mobile navigation apps that generate routing guidance from real-time location data collected simultaneously from a multitude of users. A key common thread among these systems is their integration with a variety of external systems. By comparison, the stand-alone software of the past (for example, an accounting system running on a mainframe computer) seems simpler, and frankly, quaint.

Not surprisingly, as features, capabilities and integrations of modern software have grown, so has the complexity of the effort to develop and implement such software. One commentator described the situation in the following way: "There are lots of moving parts and they're all buried under lots of other moving parts, so that you can't even see half of them!"[1] Managing the changes and integration points can seem a bit like changing a tire on a moving car.

Even if more complicated, by comparison with the software of the past, today's systems can often operate with increased stability and be deployed faster and at lower costs.[2] One reason for this trend is the proliferation of collaboration in software development, including the use of open source and other third-party code.

Open source software can provide up-front benefits by reducing the amount of custom code in a project, and providing proven technology, thereby shortening the time it takes to create working software. As a result, the use of open source software has increased significantly in recent years, with 86 percent of organizations reporting that their use of open source software increased or remained constant in 2017.[3] In similar fashion, developers have increasingly turned to SaaS and other "as a Service" offerings to reduce the scope of software development projects, improve serviceability, and reduce the ultimate cost of ownership. According to a 2016 survey, 49 percent of companies used one or more SaaS solutions and another 23 percent planned to implement at least one SaaS solution within the next 12 months.[4]

However, despite the benefits of using these building blocks, there are disadvantages. Open source and third-party code and SaaS offerings are dynamic, subject to performance problems and security vulnerabilities, and are not within the control of the business or the developer. For example, a change or error in third-party code or a SaaS offering may create incompatibilities or malfunctions in other parts of the software. In addition, as has been widely discussed elsewhere,[5] open source software risks can create a variety of legal issues, including (i) the risk of being required to share a business's proprietary technology with third parties or without charging a fee, (ii) the absence of warranty and protection against infringement risks, and (iii) the potential for conflicts among the various license terms that govern open source code. Managing these concerns is a major challenge in modern software development. Each aspect of the project, including items from third parties, must be managed so that the software building blocks and use of external software continue to meet project specifications, remain compatible with the project-at-large, and can be used without license conflicts or compliance issues, all while avoiding a major delay to project execution. This challenge is even greater where the project lacks an agreed upon contractual framework for reviewing and approving the use of third-party building blocks.

Traditional Software Development

Traditionally software development was based on a set of practices known as the "Waterfall" model. This model is characterized by a sequential process with clearly defined steps (for example, design precedes coding, and coding precedes testing, and testing precedes deployment). Because it is linear, the Waterfall model is often viewed as inflexible.

But the Waterfall model is often well-suited for projects where (i) detailed specifications for the software to be developed exist at the project start, (ii) there is limited use of third-party code (i.e., there is significant custom code developed), and (iii) the software to be

developed will have limited interactions with external systems (such as with an application that executes in a stand-alone manner on a workstation or mobile device).

Contracts for Waterfall projects mirror the structure of this model. For instance, such contracts often (i) incorporate a schedule listing detailed specifications and delivery dates, and (ii) tie acceptance of, and payment and warranties for, deliverables to their compliance with specifications.

Development Methods for Today's Complex Software

The Waterfall model may provide a useful starting point, but it is often a poor fit for today's software development projects. As noted above, modern software development often relies more on the use of pre-existing third-party building blocks and linkages to external systems, and less on the creation of custom code. As more third party elements are added to a project, it becomes ever more difficult to analyze potential compatibility and other interactions among these elements and to define specifications for the entire project. In addition, businesses today require more rapid development and deployment of software to gain market advantage and to keep pace with evolving technology, such as use of social media platforms. Those businesses want to start development without the time-consuming job of defining specifications in advance.

In response, Agile and similar software development methodologies have become popular alternatives to the Waterfall model. While the details of each vary, such methodologies generally (i) enable development to happen rapidly without detailed, up-front specifications, (ii) accommodate evolving business goals for the final product, and (iii) emphasize early and continuous delivery of software to the business.[6] For example, Agile accomplishes this by breaking down the project into smaller units, each with its own coding and evaluation iterations, and enabling the business to change the direction of (or even terminate) the project at any point.

Due to its flexibility, Agile has become commonplace in the software development industry with 77 percent of software development companies reporting the use of Agile for their projects.[7] Yet Agile is not without challenges for lawyers and their business clients. For instance, it does not mitigate the difficulty of managing the use of third-party building blocks and the external systems that need to be integrated with the software being developed (and which could delay or derail the project). In addition, without detailed up-front specifications, businesses may have less certainty regarding the features, price and delivery date of the final product.

Likewise, the lack of detailed up-front specifications undermines traditional acceptance and warranty provisions, which are based on deliverables meeting requirements, and that places a greater burden on businesses when they need to show that a final product is deficient. Agile and similar methodologies are designed to provide "workable" code in a series of short term, smaller pieces of projects. Typically, businesses have relatively liberal termination rights, which allow exit at any point during the project. However, businesses often find that walking away from a developer is not a practical remedy. For instance, even if workable code is delivered with each coding cycle, the business may incur significant additional costs if it terminates and a successor developer needs to analyze and possibly rewrite parts of the original developer's code. In other words, once the business invests in an Agile-development project, it may need to invest much more than was originally budgeted to achieve the desired outcomes or risk scuttling the project entirely and losing the value of the original investment.

What Can Be Done to Mitigate Risks in Complex Software Development Projects?

DOCUMENT KEY REQUIREMENTS AND SUCCESS FACTORS TO EVALUATE THE RESULTS OF THE PROJECT.

As noted above, projects for modern software development often start without detailed up-front specifications that tie milestone

acceptance and warranties to compliance with requirements. Even without such detailed specifications, the modern software development contract should document, at a minimum, (i) the business objectives to be met, the promised value to be delivered, the desired outcomes and other criteria for evaluating the "sufficiency" of the final product, and (ii) key system requirements, such as the technology stack to be supported and requirements for compliance with specified standards. For example, these criteria could include a minimum percentage increase in processing speed over the business's legacy system, or require the successful deployment of the software for a specified number of end users. It is also important to keep in mind that even where specifications for the software are to be developed during the project, the scope and pricing for other developer services (such as ongoing maintenance, support and hosting services) should be detailed in the contract.

SET RULES FOR USING OF THIRD-PARTY BUILDING BLOCKS.

The modern software contract should specify guidelines for third-party building blocks, including (i) compliance with the business's open source software and IT security policies and, if applicable, technology architecture standards, (ii) the business's right to review and approve the use of such building blocks, including governing license and other legal terms and impact assessments prepared by the developer, (iii) an allocation of responsibility for licensing such building blocks (in terms of both administrative and financial responsibility), (iv) the requirement for the developer to provide bills of material and, if applicable, the results of open source code scans, with each delivery of the software, so that existence of open source and other third-party materials are known to the business, and (v) the business's rights to assume the developer's license to such building blocks (for example, at the end of the project).

DUE DILIGENCE OF THIRD-PARTY BUILDING BLOCKS.

Before approving the use of any third-party building blocks, the customer should confirm, among other things, (i) the stability, maturity, quality and security of such item, (ii) that the legal terms governing such item permit the business' intended use for the software and confirmation that there are no conflicts among the various governing legal terms, and (iii) the availability, cost and terms of support and maintenance of such item. The contract should also detail what happens if the project begins but the business ultimately does not approve the key building blocks for the project.

ADDRESS THE IMPACT OF CHANGES OR OTHER PROBLEMS IN THIRD-PARTY BUILDING BLOCKS AND EXTERNAL SYSTEMS.

Third-party building blocks to be used for, and external systems to be integrated with, the software are subject to changes and problems, as well as the risk that the third-party provider will disappear. The modern software contract should address these issues by specifying (i) which party is responsible for identifying, assessing and bearing the costs of such issues and managing the relationship with the applicable third party to resolve problems as they arise, and (ii) the business's right to approve the handling of such issues (whether through rewriting code, using a replacement product or eliminating a feature). As changes occur, the parties should evaluate any impacts on project objectives and success factors to validate that they remain relevant. In addition, depending upon the criticality of the third-party component, it may be appropriate to require that the applicable provider establish a source code escrow arrangement for the business's benefit (for example, in case such provider becomes bankrupt). Businesses should also take into account their need to have control over changes when considering whether to require a private or public cloud implementation of a SaaS offering.

ADDITIONAL (NON-SOFTWARE) APPROACHES TO MITIGATE RISK IN MODERN SOFTWARE DEVELOPMENT PROJECTS.

In addition to the items described above, businesses should consider addressing broader contract risks in software development projects, including (i) liberal rights for the business to terminate and to receive object and source code for the software and a broad license to the developer's intellectual property, all to permit the business's continued use and development of the software, (ii) warranties regarding sufficiency and qualifications of the developer's resources working on the project, (iii) the right to hire (or at least to receive knowledge transfer from) the developer's personnel working on the project, and (iv) avoiding giving the developer exclusive rights to develop the software or other commitments that may restrict the business from engaging a successor developer.

Conclusion

While modern software offers a range of new features and capabilities, it is more complex and dependent upon integrated third-party components than ever before. This complexity creates challenges for traditional contracting approaches that measure outcomes based on compliance with detailed up-front specifications. By understanding and anticipating these challenges, lawyers can guide their business clients toward more flexible contractual approaches that mitigate risk and promote the success of the project.

Endnotes

[1] Danny Bradbury, "How to Secure a Software-Driven Technology Stack in a Cloud of Moving Parts," The Register, https://www.theregister.co.uk/2017/11/01/how_to_secure_a_softwaredriven_technology_stack_in_a_cloud_of_moving_parts/

[2] For example, McKinsey & Company found that "companies can reduce the average number of days required to complete code development and move it into live production from 89 days to 15 days, a mere 17 percent of the original time" by adopting DevOps practices. Oliver Bossert, Chris Ip, and Irina Starikova, "Beyond Agile: Reorganizing IT for Faster Software Delivery," McKinsey & Company, September 2015, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/beyond-agile-reorganizing-it-for-faster-software-delivery

[3] Black Duck, "Open Source 360° Survey," https://www.blackducksoftware.com/open-source-360deg-survey

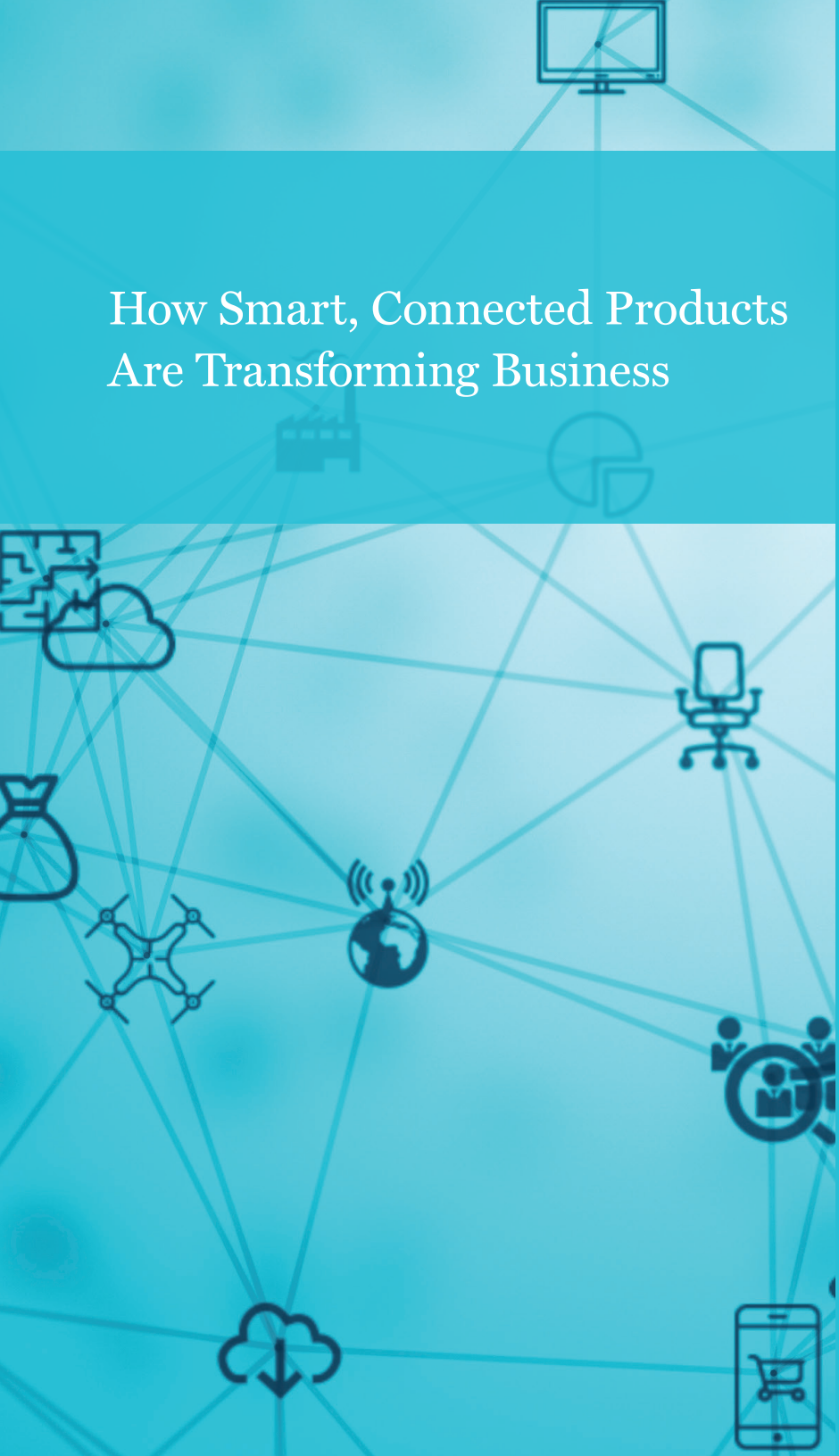
[4] James Sanders and Meghann Agarwal, "Software as a Service: Adoption rates, business benefits, and preferred providers," Tech Pro Research, January 2017, http://b2b.cbsimg.net/downloads/TRPro/Tech-Pro-Research-SaaS-Report-2017.pdf

[5] Derek Schaffner, "The Risks of Open Source Software in Outsourcing Transactions," Business and Technology Sourcing Review, https://m.mayerbrown.com/Files/Publication/891b2c9a-ceff-4ae9-be20-d5f879bc3927/Presentation/PublicationAttachment/f9a67ec3-5786-4c9c-8d46-9cf97b5efe5f/ART_RISKSOFOPENSOURCE_0308.PDF

[6] For example, the Agile manifesto asks developers to "Welcome changing requirements, even late in development." See http://agilemanifesto.org/principles.html.

[7] "Atlassian 2016 Report – Software Development Trends and Benchmarks," https://www.atlassian.com/whitepapers/software-trends-2016

How Smart, Connected Products Are Transforming Business



How Smart, Connected Products Are Transforming Business

How Smart, Connected Products Are Transforming Business

Marjorie H. Loeb, Linda L. Rhodes, Riley C. Moore, and Dean C. Won

Connected products are now ubiquitous, and their use is projected to dramatically increase in the foreseeable future. An estimated 8.4 billion connected "things" were used in 2017, the vast majority of which were consumer products and applications.[1] The prevalence of these connected products is projected to double between now and 2020.

While bringing significant benefits to consumers and businesses through enhanced functionality, convenience and customization, connected products also raise important considerations for technology transactions. In particular, connected products require the integration of complex technologies, creating challenges for achieving the interoperability required for functionality. In addition, this connectivity can unintentionally open multiple cybersecurity attack points with respect to which security measures and safeguards must be implemented and maintained. The fast-paced growth in this area will result in exponential growth in data collection, raising issues with respect to data usage rights and consent. Connected products are already used prominently in regulated industries, where the implications of regulatory compliance and consumer safety are key contracting considerations. Customers must be confident that their products work as intended and understand the technology and licensing restrictions and requirements of the technologies enabling the product functionality.

Accordingly products must be secure from unauthorized access or manipulation, must collect and use data consistent with applicable privacy and security laws, and must comply with other applicable regulations and industry standards governing functionality. Contracts between suppliers and customers for technology to build connected products must define responsibilities and allocate risk in support of these fundamental objectives.

Legal and Regulatory Landscape

In the United States, the legal and regulatory landscape is still developing, as legislators begin to propose and consider laws addressing the new issues raised by connected products, and existing regulatory bodies, including the Federal Trade Commission, seek to adapt policy and guidance to new circumstances.

CYBERSECURITY AND CONSUMER SAFETY

Connected products are highly networked, and access to one device opens up access to other devices connected to that network. For hackers looking to access either the broader network of a business or multiple devices of an individual, connected products are an attractive point of entry. In addition to the risks associated with general data breaches, connected products can present particular cybersecurity risks for consumers and companies alike. Specifically, with products like smart medical devices and connected cars, a security breach of the network on which those products rely could result in real-time death and bodily injury to end users.

Consumers have brought claims against businesses for transmission of product performance and use data, as well as consumer data, via unsecured transmissions.[2] While decisions have varied as to the standing of plaintiffs where no actual harm occurs, the DC Circuit held that, in a case brought for data breach involving credit card and social security numbers, a substantial risk of harm existed simply by virtue of the data breach and the nature of the data stolen, even if there were no allegations that harm (in this case, identity theft) had occurred.[3] This same principal, that a substantial risk of harm is enough, has been supported in the context of regulated devices. For example, NHTSA required the recall of vehicles to address security vulnerabilities even without a showing that anyone had tried to exploit the vulnerability.

Lawmakers are contemplating these issues and are beginning to set the groundwork for legislation. In September of 2017, for example, the US House of Representatives unanimously passed the SELF DRIVE Act (H.R. 3388 (115th)), a bill giving federal regulators the power to regulate self-driving vehicles. The bill includes a requirement for vehicle manufactures to develop a "written cybersecurity policy with respect to the practices…for detecting and responding to cyber attacks or unauthorized intrusions."[4]

DATA COLLECTION AND DATA PRIVACY

Data collection (both direct and incidental) through connected devices means providers of such technology must comply with increasingly stringent privacy requirements. In 2014, the FTC and Vizio reached a settlement related to Vizio's collection of consumer television viewing habits without viewer consent, which data could be aggregated with other data to derive personal information of the viewer. Vizio was required to delete the data it collected and put a privacy program in place to evaluate Vizio's practices and its partners.[5] In addition, Vizio must now disclose its data collection methods and receive consumers' express consent to collect this information.[6] The FTC applied established consumer protection principles grounded in transparency and consent and released best practice guidance that companies should follow when collecting data via connected products: (i) explain your data collection practices up front; (ii) get consumers' consent before you collect and share highly specific information about their entertainment preferences; and (iii) make it easy for consumers to exercise options.

Numerous additional privacy issues are raised by connected products. For example, many connected consumer devices are portable, requiring consideration of privacy laws in multiple jurisdictions relating to geolocation and other data protection issues.

Contractual Implications

To build successful supplier relationships for the design, creation, sale and maintenance of connected products and solutions, customers and suppliers will need to consider the risks associated with the connected products and allocate those risks in their supply agreements. Connected products may be used for business purposes or sold as consumer products, and the risks should be considered in relation to the context in which the products will be used.

That allocation of risk may be very different from more traditional technology acquisitions. One key difference is in the area of product liability, a concept that has not been a critical focus in traditional technology transactions. For example, contracts for the supply of software and services have limits on liability for warranty or other breaches and exclusions of damages that are typical to the technology industry but which sharply contrast with the warranty provisions and assumption of liability often expected by manufacturers from component suppliers in the sales of goods and services under purchase orders governed by the Uniform Commercial Code.

PRODUCT FUNCTIONALITY

Connected devices can be almost anything, in the case of consumer products, from smart refrigerators and televisions, wearable clothing, medical monitoring and dosing devices and personal assistants, to, in the case of business use, devices that gather data about heavy machinery operation, or track manufacturing parts or shipments. Whether used in a consumer or a business context, connected products rely on integrated or external technology, data collection and analysis. The technology, data collection, data processing and analysis are likely to be provided by multiple suppliers, creating numerous integration points, and potential points of failure. Building a connected products offering means managing an ecosystem of relationships and integrating different technologies. Accordingly, incorporating detailed design standards and requiring adherence

to protocols and best practices in supply contracts are key to developing products that work as intended and are compliant with industry standards governing functionality. Achieving and maintaining inter-operability among the components in the product ecosystem is critical to sustaining performance throughout the life of the product. In addition to determining product specifications for individual components, the parties will need to allocate responsibility for establishing and testing interfaces to integrate the necessary components and to test the functionality and security of the overall system.

The rapid pace of technology change necessitates the inclusion of contractual terms delineating responsibilities with respect to technical evolution and remotely delivering upgrades. The parties should consider a change management process to address both technology evolution and other necessary changes in one or more individual components or the potential need to substitute a supplier. An effective change management process will need to address the extent to which a supplier will be required to cooperate with the business customer, as well as other suppliers. In some cases, suppliers will need to share confidential and proprietary information with, or provide access to software code to facilitate the update by another supplier or the business customer, particularly in the case of a product comprised of many integrated components.

CYBERSECURITY

Businesses developing connected products and solutions need to build into their standards new approaches and requirements to address growing cybersecurity risks, pass through to suppliers the obligation to comply with these evolving standards and maintain flexibility to update standards during the contract term. External guidance and best practices related to cybersecurity are growing vastly. Technology contracts will need to consider the parties respective responsibilities for staying abreast of the same and build requirements

for compliance with appropriate external standards into their contracts. Additionally, the parties will need to work through the tension between cybersecurity principles, premised on providing each supplier access to technology components only to the extent necessary to supply the particular component or service, and the benefits of open architecture with broader access to share responsibility for testing and integration and enhance product innovation in support of product functionality as described above.

Further, although customers may have experience negotiating for cybersecurity protections in enterprise systems, they will need to rethink their approach as they seek to build cybersecurity protections into their products intended for consumer use. There are fundamental differences between enterprise cybersecurity practices, which are largely aimed at protecting against business risks arising from unauthorized access to confidential and personal data, versus product cybersecurity practices, which will require protecting individuals from actual physical injury or death , and rely on product liability concepts, in addition to data security concepts.

In the case of consumer products, the parties need to consider product liability concepts, including thinking beyond the prescribed use of the product to reasonably anticipated use or even misuse. This includes anticipating connections to devices and data sources from outside of the eco-system which is the subject of the contract, with the result that the parties must consider how to allocate risk and responsibilities for mitigation procedures (e.g., authentication procedures, fall back modes) from external factors.

DATA PRIVACY, DATA RIGHTS, AND DATA USE

As connected products collect large amounts of data, the parties need to understand the different types of data that will be collected, for example, safety critical data (e.g., crash event data), non-safety critical data (e.g., consumer preferences) or both (geolocation data)

and the purposes for which the data is collected (product performance, product improvement, including through machine learning, and customer preferences and marketing). There may be instances where government compels a business to collect specific data, such as event data records. Other data may be helpful in maintaining and improving the product. The interests of the parties in the data may vary and the rights and uses of the data will need to be negotiated.

In the case of consumer products a threshold concern will be the need to gain consumer consent for the collection and use of the data, including ensuring consent is obtained as ownership of the connected products that are readily transferable changes. The contractual terms around use of data will be driven by the consent obtained. The contract will need to specify which party is responsible for obtaining consumer consents, and which party is responsible for maintaining compliance with changing privacy laws that impact the personal data collected (both directly and indirectly) through connected products.

REGULATORY COMPLIANCE AND CONSUMER SAFETY

With connected products, particularly those providing services or functionality that if incorrectly performed or misused may raise consumer safety issues, the parties will need to consider the appropriate allocation of risk in light of heightened product liability concerns and other contractual terms. Regulated companies of consumer products are accustomed to passing through to traditional component suppliers obligations necessary for regulatory compliance and allocating the risk associated with consumer safety. Technology companies may be unfamiliar with both the contractual requirements necessary for the customer's regulatory compliance and assuming risks associated with personal injury. The parties will need to work to bridge those gaps.

Contracting for connected product technologies is becoming more challenging with the growth of safety and cybersecurity risks, the vast increase in data collection, the tremendous complexities of

interconnected systems and evolving laws and regulations. Customers can successfully contract for connected product technologies through an understanding of these challenges and through the use of flexible contracting requirements that allow for constant adaptation of the technology, business requirements, and compliance considerations in this area.

Endnotes

[1] https://www.gartner.com/newsroom/id/3598917

[2] In 2015, several automotive manufacturers were sued for manufacturing cars that transmitted car and owner data via unsecured transmissions. https://epic.org/amicus/cahen/Cahen-First-Amended-Complaint.pdf. The plaintiffs alleged that poor cybersecurity in the vehicle's wireless technology put drivers at risk of having their cars hacked and a hacker taking "control" of the cars. https://epic.org/amicus/cahen/Cahen-First-Amended-Complaint.pdf ¶ 33.

[3] CareFirst, Inc. v. Chantal Attias, No. 17-641.

[4] https://www.congress.gov/bill/115th-congress/house-bill/3388/text

[5] https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen

[6] https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen

Data Licensing—Tips and Tactics

Data Licensing—Tips and Tactics

Data Licensing—Tips and Tactics

Daniel A. Masur, Brad L. Peterson, and Corina Cercelaru

Companies obtain data from an increasing number of sources. Some of these sources are under contracts titled "data license agreements," but most are under other types of agreements. Those other agreements might include subscription agreements, website terms of use, outsourcing agreements, purchase and sale agreements, alliance agreements and other commercial agreements.

Data acquired from third parties generally come with license and use restrictions, and may come with restrictions that attach to personal data. In some cases, the license terms associated with the data are subject to significant negotiation. In other cases, however, a company accepts license terms with little thought as to whether they are aligned with the anticipated handling and use of the data.

To ensure compliance with applicable license terms, each item of licensed data must be linked to its source and to the specific terms on which the data was obtained. Unfortunately, data is often not tracked at all or the data provenance is lost when the data flows into a database or from one database into another. The danger, of course, is that data is used in ways and for purposes not contemplated by the license. This can result in license breaches, privacy law violations, intellectual property violations, and regulatory compliance failures.

Even keeping track of data can be challenging. Software often has a "software fingerprint" and may even be reporting on its use. By comparison, it may be costly or even impossible to identify all of the locations where licensed data is being stored or used. Thus, without advance planning and technology, it can be difficult or even impossible to demonstrate that a company's data use is consistent with the terms of the applicable license grant and may expose it to significant liability in the event of an audit.

Tracking data provenance and its related restrictions is new to many companies, and like many new areas, it requires that a company develop policies and procedures. When a company is licensing data from a third party, there are important considerations which, when properly managed, can lead to better data licenses. The following are important issues to be addressed when obtaining data from a third party.

Licensed Data

The core provisions of a data license agreement define the data that is being licensed, including the manner and frequency with which the data will be provided/updated, how current the data will be (that is, whether the data will be provided on a "real time" or close to "real time" basis), and the format in which the data will be delivered and the mechanism of delivery. Such terms may include the use of encryption and a secure delivery mechanism, designated communications technology platforms, and specific hardware or software configuration requirements. These provisions vary from a general license that may be accessible to the licensee during the license term to a specific license—for example, to market data on specific assets within a specific time after the market event occurs.

Users

The data license must also establish who is permitted to use the licensed data. For example, the license agreement may identify the people who are permitted to use the data or the devices on which the data may be used or may specify the maximum number of such users or devices. The licensee should be sure that any such restrictions are consistent with its anticipated use of the data. In addition, given the complex structures of many corporations, consider making clear that data use is not restricted to the entity executing the license and that the licensed data may be used by affiliates of that entity. Also, to the extent a company uses third-party contractors, it may be important to provide that the licensed data may be used by such third party contractors in performing services on behalf of the licensee.

Finally, depending on the business model of the licensee, it may be important to provide that the licensed data may be accessed and used by regulators or customers of the licensee and its affiliates. Of course, it is also important to flow down to the affiliates, third-party contractors (and their subcontractors) and customers any license restrictions on the use of such data.

To the extent relevant, the data license agreement should also address the issue of exclusivity. Most data license agreements are non-exclusive, where the licensor has the same rights to the data as the licensee and can also license the data to other third parties. Less often, a licensee may require an exclusive license to the data, which will only grant rights to the data to the licensee, not allowing use or access by any other parties, including the licensor. A sole license is another option. A licensee may seek a sole license if it does not want the data to be licensed to other third parties, but to allow the licensor to continue to access and use the data.

Purpose

In some cases, data is licensed for a specific purpose and only for that purpose. For example, in the case of a bank, a customer may provide data for the purpose of opening and maintaining an account, obtaining a mortgage or other loan, engaging in a corporate transaction, facilitating the completion of required "know-your-customer" checks, etc. However, in many cases, the data finds its way into other databases where it is unwittingly used for new or different purposes. It is thus important for the licensee to seek to include in the data license (which, in this example, might be a customer agreement) all of the possible purposes for which the data may be used including, to the extent possible, possible future uses. If the purpose clause is not as general with regard to those possible future uses, compliance processes are needed to avoid a possible license breach.

Location Restrictions

For companies that operate in many locations, it is important to focus on where the data can be stored, accessed and used. For example, the proffered data license may limit storage, access and use to the United States. If storage, access or use of the data outside the United States is contemplated now or may be in the future, make that clear in the license agreement.

Privacy and Security

Given the proliferation of data protection laws and the current focus on data privacy and cybersecurity, it is important to address in the data license the nature and sensitivity of the data to be provided, the steps the licensee is obligated to take to protect the data and the licensee's potential liability if a data breach occurs.

Quality

Licensors often seek to disclaim any representation or warranty with respect to the completeness, accuracy, timeliness or utility of the licensed data. A licensee may see the following disclaimers, particularly where the data is licensed to many licensees under a form agreement or where the licensor is not in the business of licensing the specific type of data:

- The data is licensed "as is" and "as available" and the licensor does not assume any responsibility for the use of the licensed data;
- The licensor provides no representations or warranties about the accuracy, completeness, authenticity, usefulness, timeliness, reliability, appropriateness or sequencing of the data; or
- The licensor does not represent or warrant the data or access to it will be uninterrupted or error-free, or that errors will be corrected.

Carefully consider whether, given the nature and anticipated uses of the data, the disclaimers are acceptable. If the licensor resists a requested warranty on the theory that the licensor's data is what it is, and has not been scrubbed, consider adding a knowledge or materiality qualifier.

Rights

It goes without saying that the licensor cannot grant the licensee broader rights in the data than the licensor possesses. So, it is important for the licensee to satisfy itself through due diligence and to document in the license agreement that the licensor possesses and is able to grant the licensee all of the rights the licensee requires to use the data for the anticipated purposes. This is especially true with respect to personal data where, in many cases, the licensor is not obtaining the personal data directly from the individual data subject. If notice to or the consent of the individual data subject is required, it is important that the licensor represents and warrants that it gave such notice or obtained such consent or that it obtained adequate assurances that the entity providing the data did so. In some cases, the parties will also need a mechanism that makes licensees aware if individual data subjects withdraw consent.

Term and Termination

Finally, it is important to define when your rights with respect to the data begin and end. Often, data is licensed for a limited subscription term, with the understanding that it will be returned or destroyed at the end of the subscription term. However, for practical reasons, the licensee may require a perpetual license for data previously received and incorporated in the licensee's systems. Given the proliferation of corporate databases and the ease with which data moves from one to another, it may be difficult or even

impossible to track down the data. In addition, to the extent the data has been co-mingled with other data sets, it may not be feasible for the licensee to extract or stop using the data. Finally, many companies, such as financial institutions, will require a perpetual license to meet regulatory or control obligations to maintain the underlying data for decisions and actions.

ERP in the Cloud

ERP in the Cloud

Rebecca S. Eisner, Marina G. Aronchik, and Lindsay T. Brown (*former associate*)

Enterprise resource planning (ERP) systems have revolutionized business. Now, the cloud is revolutionizing ERP. By 2020, four out of every ten large organizations will have at least 60% of their ERP applications in the cloud, according to Gartner. This article describes important contracting considerations for companies preparing to move ERP to the cloud.

First, let us review how we are using certain terms in this article. We use "ERP" as a general term for integrated enterprise applications. Examples of ERP providers include SAP, Oracle, Microsoft, Workday, Salesforce, and Infor. We use "on-premise" to refer to a business hosting and running ERP software on its own infrastructure or infrastructure managed for it by a cloud provider other than the ERP provider. "Cloud ERP" means the ERP software is provided in a "software as a service" model by the ERP software provider.

Contracting for Cloud ERP

Cloud ERP providers prefer to license Cloud ERP on their own forms, versus the customer's forms, though some customers succeed in using their forms. Use of the provider form presents a disadvantage to the customer, but in our experience, customers are usually able to negotiate reasonable changes to the terms, depending on the size and scope of the deal and the revenues involved. Customers must prepare to negotiate on issues common to all commercial technology contracts: indemnification, limits of liability, termination rights, provision of service during disputes, protection against suspension of license rights or services, and disengagement services (i.e., ramp-down rights), and clauses that permit continued use by divested entities for a period of time, or use by newly acquired affiliates and subsidiaries. In addition, the following are common hot issues in Cloud ERP negotiations addressing operational, risk and compliance topics:

OPERATIONAL ISSUES

Users and Use. Clearly defining how "use" and "users" and "direct" and "indirect" access will be applied by the cloud provider can eliminate costly surprises. For example, consider: Which members of your enterprise beyond your employees may need access to the ERP software? Will contractors, suppliers or customers have access? Does use (and incurring fees) apply during testing periods? If the customer accesses the system merely to extract data does that constitute "use"? What if one of your customers accesses the system to check status of an order or payment? What if access occurs only through an API, and does not grant full use of the software? The issue of licensed named users became the subject of contention in a case between Diageo, a British beverage company, and SAP[1]. Diageo licensed SAP and connected two Salesforce.com systems to the SAP system to allow sales representatives to access SAP, and to allow customers and distributors to place orders through the system. SAP claimed that all of these users needed licenses according to the definition of named user licenses and other terms under the SAP license, and the court agreed with SAP. SAP is not the only ERP provider to take this position regarding users and access, and customers should be careful to understand which types of system access and use (including data extraction and even data viewing) may trigger a claim of "use" of the system, requiring a supporting paid license for such use.

ERP System Performance and SLAs. Customers using on-premise ERP have the ability to architect the level of performance, redundancy, and flexibility that they need—within the limits of the software—to meet specific business needs. With Cloud ERP, customers must accept the service levels, maintenance windows, and other performance-related aspects of the software and systems made available by the cloud provider. Cloud providers are often willing to document processes, procedures and policies in the cloud agreement, but they generally are not able to

change operational components of the Cloud ERP, for example, to increase standard service levels. As a customer of Cloud ERP, it is important to document the critical performance requirements of the ERP software and system, recognizing that while you may not be able to negotiate improvements to these terms, documentation of them still provides value (and a basis for recourse and remedies).

Upgrades, Updates and Patches. For on-premise systems, within certain parameters, customers typically control the timing of the implementation of software upgrades, updates, and patches. Generally, this control is limited only by the period that the licensor supports previous versions of the ERP software. Thus, customers can delay applying changes during peak business cycles or at other times where implementation could cause a disruption. For example, retailers would not want to undergo system changes during the busy holiday season. In contrast, in Cloud ERP, the provider controls when upgrades, updates and patches are implemented. Typically, Cloud ERP providers offer roadmaps and the tentative schedule for such changes, but the cloud provider retains full control. Although customers do not carry the burden of implementing changes, customers must focus on the consequences that automatic updates may have on integration points and API's with legacy systems. Customers may mitigate some of this risk by securing rights to information about the roadmap for upcoming changes, advance notifications of changes, and access to technical account managers who may provide additional advance support, so that the customer may better plan for these changes.

RISK AND COMPLIANCE ISSUES

Data Locations. With on-premise ERP systems, the locations of the data centers and the hosting of data are entirely controlled by the customer (within limits of the applicable license). This is not necessarily the case with Cloud ERP systems. Some providers do allow customers to select one or more locations for the ERP system and primary data

locations. But, even in such cases, cloud providers advise customers that their data may be transferred or remotely accessed worldwide in connection with, for example, support, maintenance, security troubleshooting, back up and similar functions. Customers must understand the potential locations of their data and assess the intellectual property, ownership, use, compliance, and regulatory risks associated with those locations. Most Cloud ERP providers are willing to list the country locations of processing and storage of data. Some will also agree that the customer has the right to object to any proposed movement of data out of such specified countries on the list.

Subcontractors. Cloud providers typically subcontract some functions to affiliates or third parties. When licensing on-premise ERP software, the concept of subcontractors is only relevant to maintenance, support and implementation obligations. In Cloud ERP, the use of subcontractors is relevant to provision of the entire service. Cloud ERP providers generally do not grant rights for customers to approve particular subcontractors (because it is a one-to-many service), but customers should require that providers disclose the identity of subcontractors, specify the function each subcontractor performs, and permit good-faith objections to new subcontractors. Processing data in the European Union and in other jurisdictions can trigger additional data protection obligations regarding subcontractors. Customers should seek local advice to ensure compliance with data protection laws regarding subcontractor.

Data Security and Data Breaches. Cloud ERP systems typically contain tremendous amounts of customer data, including proprietary business, sensitive and personal data. Strong security requirements, data protection agreements, confidentiality requirements, restrictions on data uses, analytics and sharing, privacy protections, data breach notification, cooperation with regulatory authorities, requirements regarding customer audits and penetration testing, and a variety of other data and system security measures help to reduce the risk of

data security breaches. Cloud ERP provider agreements tend to contain only high level security information. Cloud ERP providers typically will not change their security practices for customers, but customers should request more detailed documentation and commitments from the provider, and seek to include it in the agreement. Global data protection laws and data transfers implicate a variety of laws, and customers will need to take local advice in all of the jurisdictions in which the ERP cloud provider will collect, store, process and/or transfer the data.

Compliance. Companies that run on-premise ERP software have greater control over related compliance functions – everything from data security and privacy to audit requirements, record retention, eDiscovery holds and production, incident management, security breaches, management of important controls, and a host of other compliance issues. With a Cloud ERP, the customer will have to rely on the availability of the system and data, the functions of the system and the cloud provider itself for achieving compliance in those areas that are under the control of the cloud provider. For example, if regulators request access to data logs regarding a data breach or potential violation, the customer will need the assistance of the Cloud ERP provider to produce that information in a timely, complete and accurate manner. Besides securing a commitment from the cloud provider that it will provide assistance with these compliance requirements, cloud customers must also consider if these requirements present hidden costs in the "total cost of ownership" for Cloud ERP. Cloud subscription fees may not include additional costs for services relating to compliance reporting, audits, litigation/discovery, and other services and access to systems and data for which the customer is dependent on the cloud provider. It is important for customers to assess the need for these additional services, confirm that they are available through the cloud provider, secure those rights in the agreement, and understand the costs that will be associated with provision of that additional service or support.

Floating Terms. On-premise software and cloud providers alike are increasingly incorporating terms into their ERP agreements by reference through URL links and reserving the right to change those terms from time to time, without the consent of, and often without specific notice to, the customer. Customers must be on the lookout for these "floating terms," as they frequently contain important risk, liability, performance, price and cost impacting terms. Customers may wish to mitigate the risk of floating terms in one of several ways. Customers may negotiate all terms referenced by URLs and actually append those negotiated terms to the physical or virtual agreement. Another workaround is to negotiate important terms in the main contract document and include an order-of-precedence clause where the negotiated terms prevail over floating terms. The clause also may be written to provide that URL links may not add, remove, or modify terms related to certain subjects, e.g., termination rights or disclaimers of liability. However, there is a risk that floating terms that do not conflict with a term with a higher order of precedence may become part of your agreement, and no precedence clause will eliminate all of that risk. For example, if floating service terms introduce restrictions on data storage, those new terms may not conflict with terms in the existing agreement, and as such, they will become part of the agreement unless the customer has included other terms to prevent such unilateral changes. The ultimate protection against undesirable floating terms is a right for the customer to terminate if the customer does not accept the floating term changes.

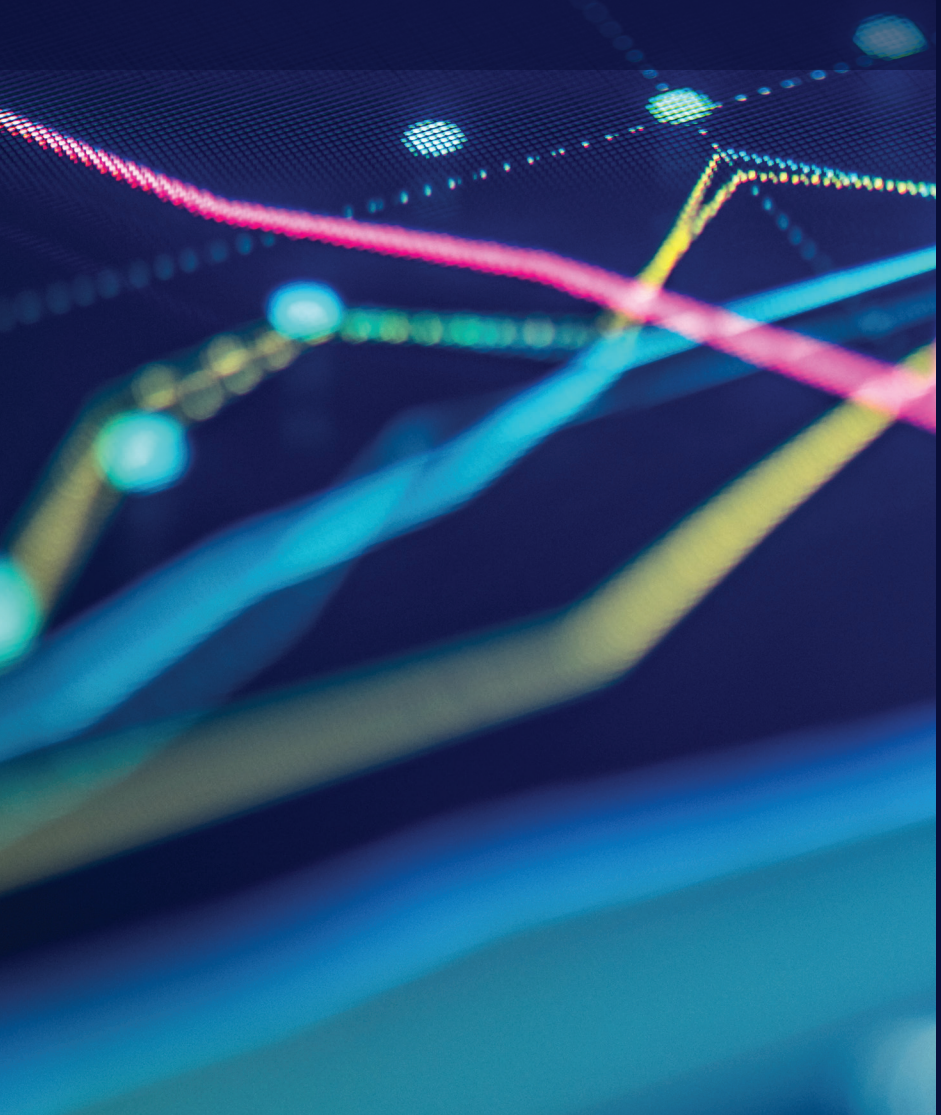
Be Prepared for ERP Cloud Negotiations

Before undertaking a renewal of an ERP agreement, or negotiation of a new ERP agreement (whether on-premise or cloud), customers should prepare for negotiations in advance using contracting best practices. First, develop a checklist of your requirements based on your own operational and technical requirements, risk tolerance, compliance, privacy, and security requirements. Prepare for negotiations with ERP providers on key terms and issues, understanding material terms, walk-away points, and potential compromise and fall-back positions that you are prepared to accept in the negotiations. Use the checklist and the key positions as a benchmark frequently during the negotiations with the ERP provider to help educate the business regarding risks and gaps in customer requirements. A bit of preparation prior to engaging with the ERP Cloud provider can go a long way toward a smoother, more successful contracting process and outcome.

Endnotes

[1] *SAP UK Limited v. Diageo Great Britain Ltd*, High Court of London, EWHC 189 (TCC) (16 February 2017).

DOs and DON'Ts for Big Data Analytics



DOs and DON'Ts for Big Data Analytics

DOs and DON'Ts for Big Data Analytics

Daniel A. Masur, Brad L. Peterson, and Donald J. Moon

Machine learning, artificial intelligence and other big data analytics tools are delivering business value by producing valuable insights and augmenting human skills in judgment-based functions. This trend is fueled by the exponential growth in data collection and the price performance of data storage and analytics. Technology is driving this growth in ways that were previously only contemplated in the movies and our imagination. Meanwhile, the legal constructs that had governed relationships between contracting parties need to be evaluated and updated to account for the changing landscape brought about by data analytics. One key fact is that big data analytic systems "learn" instead of being programmed, and it is often difficult or even impossible to understand or limit how they use inputs or to know why they arrive at the insights they deliver. Another key fact is that the data and the insights produced may not be protected by intellectual property laws and must therefore be protected in different ways than traditional outputs.

Data analytics is a process of inspecting and analyzing data with the goal of discovering useful information in order to draw conclusions about the information.[1] Data analytics is often grouped into four key categories:[2]

1. **Descriptive:** What is happening? Descriptive analytics focuses on describing metrics and measures within a collection of historical data. It is useful for showing patterns that may offer insights into a business. As basic examples, a health care provider may review how many patients were hospitalized in a prior month and/or year; a retailer may produce a regular report of its average weekly sales volume; and an insurer may identify the number of in force policies and/or claims during a prior month and/or year.

2. **Diagnostic:** Why is it happening? Diagnostic analytics examines historical data to find out dependencies and to identify root causes of certain results. For example, a health care provider may learn that an increase in patient volumes for the prior month were for cases of the flu, which coincided with an increase in flu cases nationwide; a retailer may learn that an increase in average weekly sales volume coincided with a specific promotion it had implemented; and an insurer may learn that an increase in the number of auto claims during a prior month coincided with an extremely severe period of snowy and icy roads in the region.

3. **Predictive:** What is likely to happen? Predictive analytics uses the findings of descriptive and diagnostic analytics to help identify trends and forecast future results. For example, a health care provider may predict the severity of flu cases in its region based on results at the national levels, as well as based on the number of flu vaccinations administered compared to historical trends; a retailer may be able to evaluate and predict the success of a particular promotion based on the historical sales during a previous similar promotion; and an insurer may be able to predict the types and volumes of auto claims that may occur within a region during specific seasons.

4. **Prescriptive:** What do I need to do? Prescriptive analytics focuses on what steps should be taken in order to eliminate a potential problem or take advantage of a particular trend. Carrying forward the examples above, a health care provider may order extra flu vaccines based on predictions for a severe flu season at the national level; a retailer may adjust its staffing in order to accommodate an expected increase in sales during a particular promotion; and an insurer may factor in additional environmental risks and costs for certain snow-prone regions as part of its underwriting process.

Companies today are leveraging the power of data analytics to help them translate data into insights that are clear and meaningful and

that help them achieve a competitive edge. However, in doing so, companies need to consider the underlying rights and risks associated with this growing technology and information. This article provides recommendations on what to do, and what not do, to reduce legal risks in big data analytics. The risks include inadvertent loss of rights in data, violation of the rights of data providers, legal risks associated with using "black box" results from analytic engines where the law requires an explicable rationale for a decision, overdependence on third-party data analytics providers, and failure to adequately monitor and protect data that has been shared with other parties.

To assist clients with understanding the rights and risks associated with any big data analytics efforts, we have compiled the following list of nine DOs and DON'Ts to consider:

1. **Do review data license clauses carefully and understand their potential impacts.** For this purpose, think of any agreement where one company accesses the data of another company as a data license, whether styled as such or not. For example, consider an insurance company that has contracted with a third-party administrator (TPA) to process and manage its claims. In such an arrangement, the TPA will require access and use rights of certain policy and claims data from the insurance company in order to process and manage the claims. However, the insurance company should keep the license and right to use such data limited in scope and breadth to the services to be delivered by the TPA. Because data may not be subject to any intellectual property protections, a contract where you provide data to a third party without restrictions may be construed as equivalent to an unlimited license. Outsourcers, cloud providers and other third-party contractors often push to include in their contracts broad express rights to use customer data as well as any data or insights derived from such customer data. It is important to understand and limit those rights to use your data, especially in those instances when you yourself may have limited rights to use such data. In addition, if there is value to be derived from your data (even at

an aggregated level), then the business deal should also reflect a sharing of such benefits.

2. **Don't expect your digital business team or the data scientists to spot the legal issues in big data analytics.** Your digital business team is focused on the business opportunities, and your data scientists are focused on new ways to derive insights. Following the insurance and TPA example above, a TPA (and its data scientists) having access to claims data from multiple insurance customers (including your insurance company) is in a position to extract valuable insights that can then be marketed and sold to the insurance industry. If the agreement between the TPA and the insurance company (more specifically, the data license right) does not restrict or limit such data use, the TPA may be able to take advantage of and benefit from such access and use, even if the insurance company did not intend for its data to be used in such manner.

3. **Do consider the purpose of the data collection, including uses that may not be imminent at the time the data is gathered, and obtain appropriate consents and licenses.** The best chance to obtain an adequately broad consent and license is when you first obtain the data. Following the TPA and insurance company example above, the TPA would likely advocate for a broad data license right so that it can use the aggregated claims data to develop market information analyses and products that it can then sell for a profit. Such purposes may not come up during the initial contract negotiations between the parties, since the parties are likely focused on the in-scope claims processing services; however, since the TPA will have access to a larger pool of data from its insurance customers, it may be better positioned to aggregate data and conduct data analytics as compared to any single insurance company. If the insurance company were to permit the TPA to use its data for this purpose, then the insurance company should make sure that (i) it is able to grant the TPA the

right to use its data in such manner (remembering, of course, that the insurance company may itself be subject to restrictions in the licenses under which it obtained such data) and (ii) the business deal adequately compensates the insurance company for the data access it is providing to the TPA.

4. **Do know where your data is coming from and what rights, licenses, and consents you have.** A company's data often comes from multiple sources and is stored in multiple databases spanning the entire enterprise. Due to the volume of such data feeds and data stores, tracking and understanding your rights to the underlying data can become quite complicated. Best practice is to implement a process that tracks and even categorizes the data depending on its sensitivity (e.g., personal information, data subject to HIPAA, sensitive pricing information, etc.), as it is shared within and outside of the organization.

5. **Don't exceed those rights, licenses, and consents.** While this principle is easily stated, it is may be more challenging to implement across a large organization, where many different personnel have access to the various data stores. It is important for a company (and its personnel) to understand where its data is coming from, the rights it has to such data and where the data may ultimately flow. Following the insurance and TPA example above, consider a situation where the insurance company itself only has a limited right to use certain data from its policy holders, but the insurance company inadvertently grants a broad license to the TPA to use and process all of its data.

6. **Do monitor evolving data laws and regulations, including those relating to privacy, cybersecurity, import/export, eDiscovery and records retention in your industry and geographies (e.g., state specific insurance regulations) and for the types of data that you gather, store or use.** Data privacy is an evolving bundle of issues that impacts all types of businesses

and industries. A company cannot simply implement "reasonable" steps to be in complete compliance. There are federal, state and international laws, treaties and applicable regulations that need to be reviewed and complied with, depending on the business and industry. For example, insurance companies need to be aware of HIPAA with respect to personal health information, as well as additional cybersecurity requirements imposed by the New York Department of Financial Services (NYDFS) on insurance companies doing business in New York.

7. **Don't assume that having a consent, license or absence of regulation means that you can ignore reasonable expectations and potential ethical obligations.** Regulations are evolving quickly, and the market may punish perceived abuses. Consider where the laws might go as political sensitivities develop (e.g., as big data analytics enables insurance companies to better understand and identify risk groups for underwriting purposes, consider whether anti-discrimination laws may expand to prohibit denial of coverage based on data points having a disparate impact on certain protected categories).

8. **Do ensure that you are flowing down to your contractors and other licensees, and that they are flowing down to their subcontractors and sublicensees, any applicable data restrictions.** Just as points #4 and 5 above highlight the importance of knowing your rights and obligations with respect to data, it is also important to ensure that those obtaining data directly or indirectly through you are subject to terms consistent with such rights and obligations. In the example with the insurance company and TPA, the rights that the TPA has with respect to claims data from the insurance company may be expressly stated in their contract. However, the insurance company should also

require that any data restrictions be flowed down to any subcontractors that the TPA may use to perform its obligations.

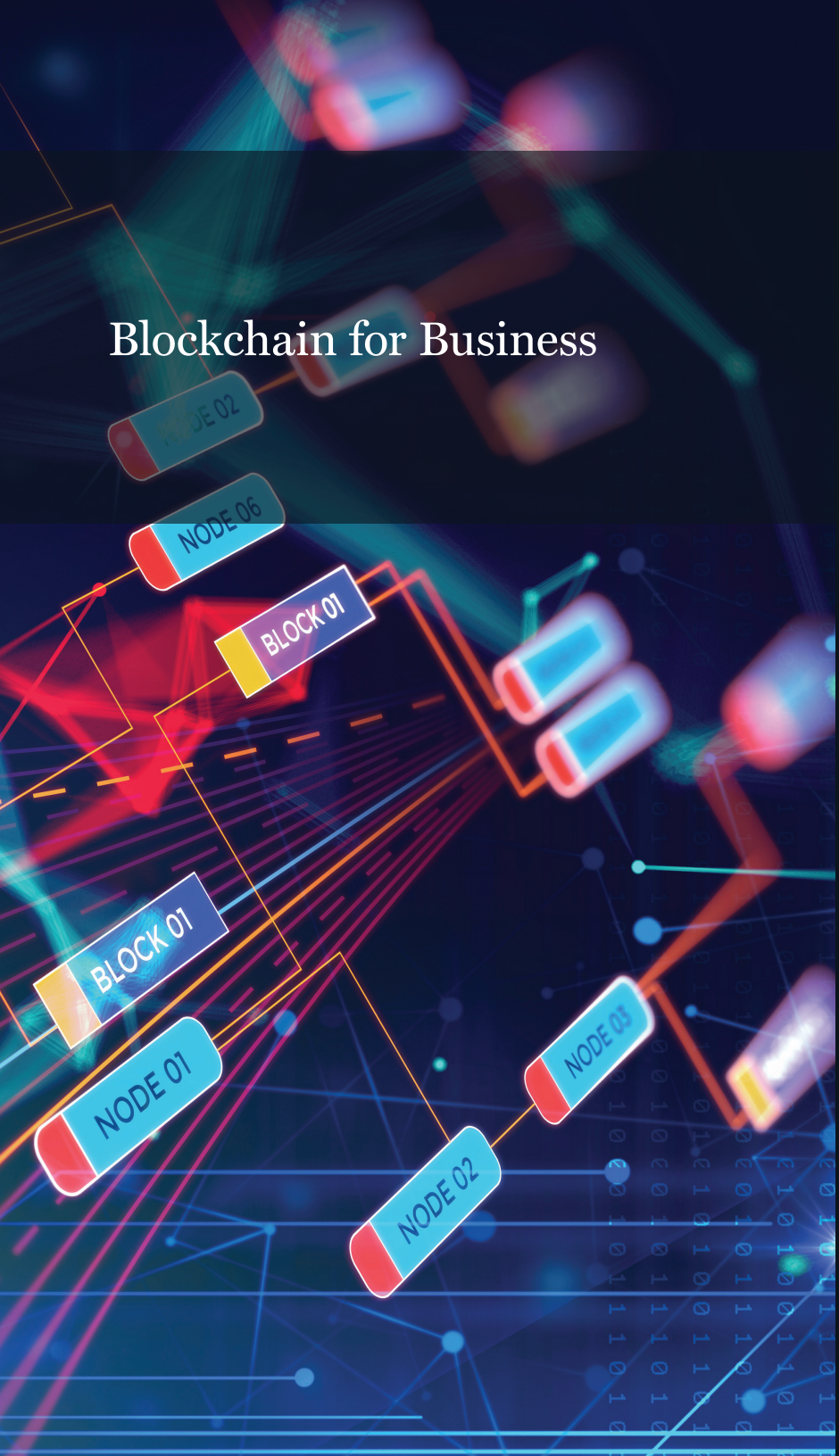
9. **Do document and implement rules, processes, procedures and a strong governance mechanism to govern and secure your data.** It is in both the sharing party's and the receiving party's interests to implement a strong governance authority that understands the rights to use shared data and helps regulate the use of such data. The sharing party should consider requiring the receiving party to notify and train its employees on the contractual restrictions regarding the use of shared data.

Endnotes

[1] http://searchdatamanagement.techtarget.com/definition/data-analytics

[2] https://www.kdnuggets.com/2017/07/4-types-data-analytics.html; http://www.ingrammicroadvisor.com/data-center/four-types-of-big-data-analytics-and-examples-of-their-use; https://www.dezyre.com/article/types-of-analytics-descriptive-predictive-prescriptive-analytics/209; and https://www.scnsoft.com/blog/4-types-of-data-analytics

Blockchain for Business



Blockchain for Business

Blockchain for Business

Rohith P. George, Brad L. Peterson, Oliver Yaros, David L. Beam,
Julian M. Dibbell, and Riley C. Moore

Introduction

Interest in blockchain has grown dramatically, with a rapid increase in investment and engagement. Over the course of 2017, numerous companies in financial, automotive, healthcare, insurance, real estate, retail, and other sectors have developed sophisticated proof-of-concepts and some are on the path to significant production deployments.

Despite the increasing attention to blockchain, the topic remains novel for many business lawyers. As companies begin to explore blockchain, however, it is increasingly important for lawyers to be able to spot the right issues and ask the right questions. In light of this, our goal is to introduce blockchain in simple terms, provide example use cases, and highlight some of the most pressing legal issues.

What Is Blockchain?

Blockchain technology was first implemented in 2009 as the underlying platform designed to solve the "double-spending" problem for Bitcoin (that is, how to transfer digital value without relying on a trusted third party). However, the attributes that make blockchain technology essential for Bitcoin can be used to solve a variety of other problems. A blockchain is:

- A **digital ledger** representing a history of transactions,
- That is **distributed** on computers (also called "nodes") operated by different participants,
- That allows participants to introduce records with **cryptographic protection** that are **validated** and **immutable**.

The records in a blockchain are immutable because information in the digital ledger is stored in blocks of data that are represented by a unique cryptographic identifier (or "hash"). Each subsequent block of data includes the hash of the prior block to create a chain that links all the way back to the first block of data (hence "blockchain"). If data in any block in the chain is later illicitly altered in any node's version of the ledger, the hash for that and every subsequent block must change, making such altered ledger readily identifiable as an illicit version. That illicit version is then rejected by consensus among the nodes.

A feature of some blockchains is the capability to create "smart contracts." For example, the Ethereum and Hyperledger blockchain platforms permit the recording of software programs within a block on the blockchain itself. This software automatically performs certain actions on the blockchain when a prescribed condition is met. As an example, a supplier who today ships goods to a customer, sends an invoice, and waits 30, 45, or 90 days for payment would prefer to have the order in a "smart contract" that pays automatically when the customer acknowledges receipt of goods on the blockchain. Alternatively, the software can trigger payment based on data from an outside source, referred to as an "oracle." For example, "parametric" travel insurance could pay automatically if an airline cancels a flight, with the airline's flight records being the "oracle."

Where Can Blockchain Be Useful?

Because of the shared and immutable nature of information stored on a blockchain, blockchains can be expected to drive the most value for businesses by solving problems in maintaining consistency of records between multiple entities, maintaining auditable information trails, efficiently settling and tracking exchanges of value, and authenticating user identity.

At this point, commercial blockchain is largely in the pilot or proof-of-concept stage across a wide range of use cases. Payments and supply chain are two of the most promising use cases.

PAYMENTS

With the rise in global business and trade, financial institutions are focused on optimizing cross-border payment inefficiencies. Current protocols require correspondent banking relationships and include intermediaries, resulting in high fees and inordinate delays. Using a blockchain to handle such payments can permit a bilateral, immutable transfer of value while reducing the fees charged and delays caused by existing processes. A number of financial institutions have announced pilots testing such blockchain solutions. In addition, the R3 and Hyperledger consortia are each working towards creating blockchain standards for payment and other financial sector use cases.

SUPPLY CHAIN

Current supply chain processes rely on non-standardized paper and digital records held among various parties, often resulting in minimal or delayed ability to pinpoint where problems arise in the supply chain.

- Diamond companies are testing an industry-wide blockchain that allows suppliers to record each movement of a diamond, tracking its conflict status.
- Retail and e-commerce companies are developing in-house blockchains to similarly track authenticity of goods they sell and combat counterfeiting.
- Transport and logistics companies have tested using blockchain to track freight, reduce delays, and replace related paper processes with on-chain records.[1]
- A number of food giants have partnered with IBM to use blockchain to track foodstuffs from farm to store.

Possible Legal Issues

We set out possible legal issues below, including (i) issues that can be partially or wholly addressed by the way that the blockchain is designed, (ii) issues that can be partially or wholly addressed by a

separate off-chain agreement among participants, and (iii) other issues to be weighed in determining whether to implement a blockchain solution.

LEGAL ISSUES TO ADDRESS IN ON-CHAIN PROGRAMMING

Confidentiality Requirements. In a "permissionless" blockchain, data can be viewed by anyone on the Internet. For some applications, such as an online database to prove auto insurance coverage, that may be preferred. If there are obligations of confidentiality, however, the blockchain may be "permissioned" (so that participation is limited by either having an administrator determine ability to participate or having objective requirements that must be met to participate) and can limit viewing of the full record only to specific participants.

Accountability Requirements. Many public blockchains allow people to become participants and engage in transactions by revealing only their public key (as is the case with Bitcoin). However, if the use case requires that a known person be accountable for what is placed on the blockchain, the blockchain or its governing body can require proof of identify before a participant is provided access. The blockchain might then require that the participant's identity be visible to transactional counterparties, to trusted nodes, or to all participants, as applicable.

Data Privacy. Blockchains have key challenges in relation to data privacy laws. For example, a node in a non-EU country recording a block in the chain that includes personal data of an EU resident may be considered a cross-border transfer of personal data. As another example, recording personal data in an "immutable" ledger may violate a right for data subjects to require that their data be removed (the "right to be forgotten"). The blockchain could be designed to encrypt the personal data with an encryption key that can be forgotten or to store the personal data off-chain in a database permitting deletion with only links to such data stored on-chain.

LEGAL ISSUES TO ADDRESS IN OFF-CHAIN AGREEMENTS

Design, Build, and Run. A blockchain must be designed and financed by a team with deep understanding of the use and may be implemented using software developers on a licensed or subscription platform—a large effort involving numerous contracts.

Amendments and Modifications. A blockchain may need to adapt to survive and maintain its usefulness. For permissionless blockchains, success may depend on whether the participants can make the right modifications through consensus. For permissioned blockchains, however, the founders can formalize the governance process off-chain via a separate, manually signed, natural-language agreement. In that off-chain agreement, the consortium or founding participants can set rules and principles for how to come to agreement (or designate trust in an administrator) to modify the blockchain's programming.

Allocation of Liability. A participant may be damaged, for example, by a vulnerability in the underlying technology, an issue with one of the nodes, a participant's failure to protect their private keys, or an issue involving the way an external system integrates or operates with the blockchain. The law is at best unclear on whether the damaged participant would have a claim against other participants, the programmers, the technology providers or others. Blockchain consortia can address this problem by requiring participants to enter into a legally binding off-chain agreement that allocates responsibility and liability.

Jurisdiction, Governing Law, and Dispute Resolution. Blockchains, by definition, involve numerous nodes keeping simultaneous copies of the digital ledger in their own hosting locations, which may be in separate countries. Each node may participate in the process of creating consensus and recording information to the blockchain. Thus, it is not clear which country(ies) have jurisdiction or what law(s) govern. Again, a consortium or founding group can stipulate the governing law, jurisdiction and the agreed dispute resolution process (such as arbitration) for all participants in the off-chain agreement.

Smart Contracts. A "smart contract" is made up entirely of code. While one might argue that the digital interaction between "smart contract" software and a participant (or a participant's software) constitutes offer and acceptance and a legally binding contract, this would be a legally novel interpretation of traditional contract formalities. Until regulators decide how to approach this technological advancement (as they have had to do in the case of e-signatures, electronic contracts, clickwrap agreements, and other deviations from traditional contract formalities), a "smart contract" could be supported by appropriate off-chain natural language contracts. At that point, it will be critical to verify that the "smart contract" code actually carries forward the legal effect of the traditional contract.

Oracles. There is a risk that the oracle is incorrect, inaccurate, or ambiguous. In such scenarios, companies may document how such inaccuracies are to be handled and how risk and liability is allocated in such events in the off-chain agreement.

OTHER ISSUES

Distributed Autonomous Organizations. Some view a blockchain operating independently of a consortium as a distributed autonomous organization (DAO) consisting of code running on distributed servers. A key question in participating in a DAO is whether participants have any recourse against anyone for the actions of the DAO.

Functionality Limitations. Blockchain is an emerging technology with potential functionality limitations. For example, currently many blockchains have limited capability to perform advanced searches or otherwise retrieve information stored on-chain. Companies should weigh these limitations against the advantages gained, at least until the limitations are addressed.

Integration. Commercial blockchain will require the communication of data to and from each blockchain. Currently interoperability between blockchains is limited and few interfaces have been built to ERP systems and systems of record. Solving this problem will require participants to agree on technical standards and software providers to build interfaces.

Antitrust. Consortia created for the purposes of arriving at common technical standards and frameworks for industry blockchains might be viewed as improper collusion between the participants or as resulting in anti-competitive effects. For example, in a permissioned network, industry competitors who are not included may be disadvantaged. Antitrust and competition law advice are thus essential.

Endnotes

[1] https://techcrunch.com/2018/03/02/blockchain-will-work-in-trucking-but-only-if-these-three-things-happen/

Contracting for Facilities Management Services in the Proptech Era

Contracting for Facilities Management Services in the Proptech Era

Contracting for Facilities Management Services in the Proptech Era

Kevin A. Rang and Marina G. Aronchik

Technology is transforming the way companies use, manage and maintain their real estate portfolios. Shopping centers are leveraging big data and developing cloud solutions and applications to attract the next generation of shoppers and transforming their ordinary mall visit into an "experience." Large companies are increasingly seeking to monitor, on a real- or close to real-time basis, their facility occupancy rates and optimize their real estate portfolios, based on the analysis of such data. Facilities management providers are implementing and relying on sensors and predictive analytics to detect and remediate issues faster than they could in the past.

Facilities management agreements and related transactions need to reflect the growing transformational role of technology and the risks that technology creates. This article discusses issues in four key areas that clients with real estate portfolios need to consider and negotiate with providers in today's technology-laden facility management deals: data and related compliance obligations, intellectual property rights, new risks and liabilities, post-termination rights and termination charges.

Data Rights and Related Compliance Obligations

DOES THE CLIENT HAVE THE RIGHT TO COLLECT THE DATA IT WANTS?

Technology that is being used to collect data includes cameras, various sensors (water/humidity, heat, smoke, etc.), microphones and badge scanners, to name a few. Cameras, as an example, can be wired or wireless, can be placed in plain view or so small so as to be undetectable. Cameras can be used for security purposes, or, if coupled with facial recognition, they can be used to assist with facility utilization

assessments. Thermal imaging cameras can make it easier to identify failing motors or other electrical components, HVAC leaks, deficient ductwork, or leaking roofs. Although we can see significant potential value flowing from the use of cameras within facilities, that does not mean that they can be deployed anywhere and that the information gathered by those cameras can be used for any purpose. This is particularly true when cameras and sensors are gathering data that may be associated with individuals, whether directly or indirectly. For example, sensors that are monitoring the operation of certain equipment may also be providing incidental information about the equipment operator—was the equipment idle at a time when the operator was supposed to be working? Individual privacy rights and laws must be considered when collecting data through use of technology that is intended to help with facilities management, particularly where individual data collection is not the intended (and approved) use. (See *International Developments in Privacy Laws and Vendor Agreements* on page 27.)

DOES THE CLIENT HAVE THE RIGHT TO PROVIDE DATA (EITHER COLLECTED OR LICENSED FROM A THIRD PARTY) TO THE FACILITIES MANAGEMENT PROVIDER USING THE TECHNOLOGY AT ISSUE?

It is not uncommon for clients to have outsourced different functions to different providers who would benefit from sharing of the data. For example, the facilities management provider could be more effective if it could access data collected by the desktop support provider to determine when and where employees are logged into their computers. Whether that data can be used by the facilities management provider will have to be determined by reviewing the contract between the client and the desktop support provider (and as discussed in the paragraph above, there may be privacy issues to consider). The client may believe that this information belongs to it, but if it did not preserve ownership in that data in the desktop support agreement, it may not have the right to make that information available to its facility management provider.

ARE THERE OTHER LIMITATIONS ON COLLECTING FACILITIES-RELATED DATA?

There are laws in virtually every jurisdiction applicable to the collection and use of personal data. There are various state laws in the United States as well as the existing EU Data Privacy Directive that will be replaced in May 2018 by the more comprehensive and punitive GDPR. Clients need to ensure that their data collection, storage, transmission and usage practices are compliant with all legal requirements as missteps today can be significant public relations issues and costly problems to correct. A client operating in Europe might need to get the assistance of the supplier of technology to conduct a Data Protection Impact Assessment if it is required by the GDPR. There may be significant differences in implementation and compliance costs where data is being transferred internationally or stored in the cloud and this will be an area which will need careful consideration in light of the nature of the data being collected and analyzed. These data issues are not always top of mind in real estate and facilities deals, but they should not be afterthoughts.

Intellectual Property Rights

OWNERSHIP OF INTELLECTUAL PROPERTY

When people think about facility management and maintenance, they traditionally think about snowplows, tools, cleaning carts and cafeterias; they are not typically thinking about intellectual property. Facility maintenance providers may use procedure and maintenance manuals drafted by the provider. These manuals may be important to ongoing facility management functions. Today, some forward-thinking companies are using augmented reality/virtual reality (AR/VR) in place of procedure manuals. A real world example is the use of smart glasses by a maintenance worker to complete complicated assembly processes ensuring that all parts are assembled in the right order without the need to consult hardcopy manuals or other handheld devices. Programming for the collection of data from installed

sensors may be similarly important. As technology becomes more complex, the need for documentation regarding not only operation of the facilities but also operation of the technology being used to operate the facilities becomes more important. Whether the client is using hardcopy procedure manuals prepared for it by the provider or smart glasses to accomplish the same task, the client must give careful thought to the ownership or license rights of intellectual property and other information associated with these solutions so that the client may seamlessly continue services when the contract with the provider ends.

LICENSE OF INTELLECTUAL PROPERTY

As discussed above, the client may be using a number of providers to deliver services. It may be necessary or desirable for a provider to use technology owned or otherwise provided by a third party engaged by the client, or vice versa. In either situation, license rights flowing from one party to the other will be necessary in this situation. As with other technology licensing agreements, clients would be well served to include licensing permissions and use rights for the entire ecosystem of the client's providers who may need to use third-party licensed technology to assist the client in maintaining or managing its facilities and property.

New Risks and Liabilities

The use of technology to provide facility management services can create new risks and potential liabilities for clients.

SECURITY CONCERNS

As devices become connected, security concerns grow. Although there are a number of security issues that we could address, we will focus on two: (i) increasing access points to a client's network and (ii) proprietary systems running on these devices. Years ago, thermostats were mechanical devices (not connected) that controlled heating and cooling in defined areas. Today, many thermostats are connected to a

network in addition to the heating and cooling system. This connection to the network is another access point for a hacker. When you add up all of the thermostats in all of the facilities that are networked, those thermostats could constitute hundreds if not thousands of opportunities for hackers to gain access to the client's network. The sheer number of additional network access points that the networked thermostats create results in significant monitoring and intrusion detection challenges for IT administrators.

A SECOND SECURITY ISSUE IS PROPRIETARY SYSTEMS RUNNING ON CONNECTED DEVICES

When it comes to deploying computers into a company's environment, it is not uncommon for there to be approved software images that are loaded onto approved hardware that have been tested as secure configurations that are supported by the company. Many connected products such as sensors and networked thermostats, use proprietary systems that provide little or no ability for customization or security enhancements. In these situations, clients need to balance the productivity improvements and efficiency gains against the security risks associated with using the technology.

DATA AND SECURITY BREACHES

Clients need to recognize that the risk of data and security breaches by facility maintenance providers is as significant, and the consequences as harmful to the client's business, as any other data or security breaches. From published reports about third-party providers who caused or enabled significant data breaches, no third-party provider is immune from the potential to create a security vulnerability or incident.

LIABILITY CONCERNS ASSOCIATED WITH THE USE OF AUTONOMOUS SOLUTIONS

There is still a lot of uncertainty, both under applicable laws and with respect to a "market standard" for contractual provisions, over how liability will be apportioned for autonomous solutions if property is

damaged or people are injured. Over time, the law will likely develop in this area providing more guidance with respect to specific technology (e.g., self driving vehicles used in connection with facility management services). (See *How Smart, Connected Products Are Transforming Business* on page 49.) In the meantime, we expect these issues to be subject to extensive negotiation by the parties, with a range of possible outcomes and compromises depending on a number of factors, including the technology at issue and specific risks (and risk-mitigation strategies) involved.

Post-termination Rights and Licenses and Termination Charges

POST-TERMINATION RIGHTS AND LICENSES

As discussed above, even simple written documents created by the provider can be intellectual property. If the client desires to use third-party or provider-owned software or technology that is used by the provider in the provision of the services, then the client will need post-term license rights to continue to use such software or other IP. If the provider has deployed sensors to detect water leaks, do the sensors stay with the client when the contract ends? Does the software used to monitor the sensors stay with the client? The client should understand the entire landscape of intellectual property used by the provider and the exit strategy that works for the client, including post term license rights where applicable.

TERMINATION CHARGES

Absent some sort of investment by the provider, there typically are no termination charges in facility management contracts. A provider's investment in technology may result in the provider insisting on an early termination fee to help it recoup any stranded costs associated with that investment. If a provider is making such an investment, then those costs should be documented in the contract along with a clear mechanism for calculating any resulting termination fee should the customer terminate the contract early.

Conclusion

Technology is creating significant opportunities for cost savings, process efficiencies, safety enhancements and improved workplace morale. Technology is entwined with data, intellectual property, privacy, and security issues, and continued use of technology (including information about how to operate the technology) may be critical to the continued provision of facilities management services. These issues should be considered and addressed when technology is deployed in a facilities management outsourcing deal or by property owners or managers.

About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia, Europe and the Middle East. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and private clients, trusts and estates.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.