MAYER·BROWN

Article

The Future of Outsourcing

By Authors 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.

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.

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.

MAYER·BROWN

International Developments in Privacy Laws and Vendor Agreements

By Authors 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.

MAYER·BROWN

Article

How Smart, Connected Products are Transforming Business

By Authors Marjorie Loeb, Linda Rhodes, Riley Moore, Dean 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: (1) explain your data collection practices up front; (2) get consumers' consent before you collect and share highly specific information about their entertainment preferences; and (3) 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

MAYER·BROWN

Article

Data Licensing – Tips and Tactics

By Authors Dan Masur, Brad Peterson, 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.

MAYER·BROWN

Article

Do's and Don'ts for Big Data Analytics

By Authors Dan Masur, Brad Peterson, Donald 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 do's 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.

Contacts

Rebecca S. Eisner
Partner
+1 312 701 8577
reisner@mayerbrown.com

Marjorie H. Loeb
Partner
+1 312 701 8833
mloeb@mayerbrown.com

Daniel A. Masur
Partner
+1 202 263 3226
dmasur@mayerbrown.com

Brad L. Peterson
Partner
+1 312 701 8568
bpeterson@mayerbrown.com

Linda L. Rhodes
Partner
+1 202 263 3382
lrhodes@mayerbrown.com

Lei Shen
Partner
+1 312 701 8852
lshen@mayerbrown.com

Oliver Yaros
Partner
+44 20 3130 3698
oyaros@mayerbrown.com

Corina Cercelaru
Associate
+1 312 701 7464
ccercelaru@mayerbrown.com

Qi Chen
Associate
+1 312 701 8735
qchen@mayerbrown.com

Daniel Gallagher
Associate
+44 20 3130 3537
dghallagher@mayerbrown.com

Donald J. Moon
Associate
+1 312 701 8823
dmoon@mayerbrown.com

Riley C. Moore
Associate
+1 312 701 8773
rmoore@mayerbrown.com

Dean C. Won
Associate
+1 312 701 8901
dcwon@mayerbrown.com