Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Outsourcing 2021

USA: Law & Practice
and
USA: Trends & Developments

Randy Parks, Jeff Harvey, Andy Geyer
and Cecilia Oh
Hunton Andrews Kurth LLP

practiceguides.chambers.com

USA

Law and Practice

Contributed by:
Randy Parks, Jeff Harvey, Andy Geyer and Cecilia Oh
Hunton Andrews Kurth LLP see p.15

CONTENTS

1. OUTSOURCING MARKET

1.1 IT Outsourcing

The key market developments in information technology outsourcing include:

- the continued shift of physical IT assets to cloud environments and software programs to SaaS environments;
- the provision of services and solutions that are supported by artificial intelligence and robotics; and
- the digital transformation of traditional business data flows into revenue-generating products and analytical tools. Buyers of services continue to focus increasingly on the Internet of Things (IoT) and the transformation of their businesses into digital offerings.

From a legal perspective, these new technologies and approaches further break up the traditional sole-source agreements into a multitude of different agreements, with more providers competing for and providing smaller chunks of services, and more demands placed on client procurement departments. The legal issues themselves have not changed dramatically, but there are important nuances associated with these technologies and approaches. Intellectual property ownership and data security remain chief among customer concerns and present the most significant risk for providers. Accordingly, those provisions continue to be heavily negotiated.

For the most part, the "human" element is removed from the robotics and artificial intelligence delivery model, but there may be personnel issues nonetheless, as these technologies tend to replace existing workforce. Accordingly, involvement from the customer's human resources department early in the process is essential.

COVID-19

COVID-19 and related government shut-down orders have forced most providers to shift to work-from-home models. Customers have had little choice but to accommodate those changes and there has been a scramble to implement appropriate security controls. Eighteen months into the pandemic, new transactions increasingly carve-out COVID-19 from force majeure clauses, since the risks and work-arounds are well understood, though the Delta variant has caused parties to consider whether "material exacerbations" of COVID-19 should still be addressed as force majeure events. The forced transition to work-from-home has suppliers and customers both thinking about whether the shift – and related cost savings – can or should be made permanent.

1.2 Business Process (BP) Outsourcing

The key market developments in business process outsourcing include:

- an increased focus on social media as the primary tool for communicating with customers;
- the provision of services and solutions that are supported by robotics, artificial intelligence and smart learning; and
- swings in emphasis between value/innovation and cost savings, depending on industry-specific conditions and opportunities.

From a legal perspective, these developments present issues that are unique to the outsourcing market, but not necessarily unique to most technology lawyers. As companies increase their presence on and use of social media, they open themselves up to potential exposure in a more public and less controlled environment:

- managers of social media websites may inadvertently post proprietary or confidential information;

- customer complaints are now more public and companies risk a "piling on" of complaints; and
- customers may post proprietary, defamatory or harassing information on a company's social media site. In addition, companies must be aware of the unique terms applicable to each social media platform, as the companies' rights and obligations vary by platform.

The use of robotics and artificial intelligence in the business process outsourcing market present similar issues as noted above with respect to information technology outsourcing market developments, namely: intellectual property ownership, data security and ownership, and potential human resource issues arising from the displacement of workers due to increased usage of these technologies. As firms lean into outbound communications through social media, compliance with applicable regulatory regimes (eg, the Telephone Consumer Protection Act), exposure to a robust plaintiffs' bar become key issues.

1.3 New Technology

The impact of new technology (eg, artificial intelligence, robotics, blockchain and smart contracts) is most evident in the information technology workforce. Low-skilled workers across all industries are being replaced by various forms of technology that are able to perform the same tasks as those workers, and do so more cheaply, without sick days, without raises and without vacations. While low-skilled workers are feeling the brunt of these new technologies (as well as more restrictive immigration policies preventing lower-skilled workers from entering the USA), higher-skilled workers tasked with their development and management (eg, developing platforms for the cryptocurrency market) have greater opportunities.

As various industry leaders contemplate using provider AI offerings to optimise their core competitive advantages, negotiations over intellectual property ownership now involve much higher stakes. Customers are concerned that their leadership positions will be eroded if their highest-value IP is shared and then incorporated into AI engines that are resold to their competitors or, worse, commoditised and distributed to thousands of users. Providers worry that the value of their innovations will be lost to customer-imposed restrictions or endless, complex IP battles.

2. REGULATORY AND LEGAL ENVIRONMENT

2.1 Legal and Regulatory Restrictions on Outsourcing

Despite state and federal lawmakers' efforts to pass sweeping legislation to regulate offshore outsourcing, there is no overarching federal framework in the USA that specifically restricts outsourcing in the private sector. As discussed in further detail below, certain regulated industries, such as the financial services, energy, insurance and healthcare industries, are subject to federal and state regulatory frameworks that extend to the regulated entities' third-party vendor relationships, including outsourcing arrangements. In most cases, regulated entities that outsource operational responsibility of regulated functions to third-party vendors continue to be primarily responsible for their regulatory compliance obligations (even if a regulatory failure was ultimately caused by the third-party vendor).

Public contracts are highly regulated at the federal, state and local levels. In addition to explicit restrictions on the performance of certain government functions by non-government employees, the highly complex public contract framework, which imposes onerous review and

approval procedures on government outsourcing initiatives, often has the practical effect of restricting large outsourcing arrangements in the public sector. Public contracts often are subject to scrutiny by elected officials, watchdog organisations, consumer groups and media, which can complicate and delay negotiations.

In addition, offshore outsourcing may be limited or restricted under certain government-sponsored programmes. For example, the Main Street Lending Program, a federal programme established under the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") which offers loans small- and medium-sized businesses affected by the COVID-19 pandemic, restricts recipients from outsourcing or offshoring jobs during the entire term of the loan and for two years after repayment.

2.2 Industry-Specific Restrictions

In the USA, various state and federal regulators oversee financial institutions through a system of functional regulation. Financial regulators have issued a wide range of interpretive guidance regarding outsourcing to third parties. For decades, prudential regulators have charged banks with establishing and maintaining risk management practices designed to ensure the safety and soundness of their activities and protect consumers that are commensurate with the level of risk involved. The application of these practices extend not only to the bank's own activities, but those of any third party engaged by the bank, including outsourcing providers. The Consumer Financial Protection Bureau (CFPB) imposes third party risk management guidance embodying similar principles on certain non-banks in the consumer financial markets, including credit unions, mortgage originators and servers, and private lenders that fall under the CFPB's supervision.

On 13 July 2021, the Federal Reserve, the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) jointly issued proposed guidance on the management of risks associated with third-party relationships. The proposed guidance reflects the prudential regulators' increased focus on banking organisations' use and reliance on third parties and outsourcing arrangements to perform business functions, deliver support services, and provide new products and services to its customers. If adopted, the interagency guidance, which is largely based on the OCC's existing guidance, would replace and harmonise the independent guidance issued by each agency.

The proposed guidance provides a multi-disciplinary framework and objectives for each stage of the third-party risk management life cycle, namely:

- planning – examination of risks and development of a plan to manage the relationship and related risks, particularly when critical activities are involved;
- due diligence and third-party selection – performing due diligence on third parties, including the party's ability to perform and comply with applicable laws before selecting and entering into relationships;
- contract negotiation – clearly specifying the rights and responsibilities of each party to the contract; seeking additional contract provisions when appropriate; understanding the consequences of any resulting limitations; and engaging legal counsel for significant contracts;
- oversight and accountability – overseeing management of and implementing strategies and policies to address third-party risks; establishing responsibility and accountability for such risks;
- ongoing monitoring – performing ongoing monitoring after the third-party relationship is

established in a manner commensurate with the level of risk and complexity of the third party relationship; and
- termination – termination of third-party relationships in an efficient matter, including consideration of appropriate transition services.

Similar to the existing guidance of these regulators, when circumstances warrant, the agencies may use their authority to "pursue corrective measures, including enforcement actions" against banks that fail to properly manage risks associated with their third party relationships.

Healthcare

Within the healthcare industry, outsourcing is impacted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) which seek to ensure the privacy and security of protected health information (PHI). HIPAA and HITECH and their implementing regulations impose significant and onerous obligations on "covered entities" (ie, health plans, health clearing houses and healthcare providers that transmit any health information in electronic form in connection with a covered transaction) and their "business associates" (ie, vendors of covered entities with access to PHI that perform certain functions on behalf of such covered entity), including compliance with HIPAA's Privacy and Security Rules. When entering into outsourcing arrangements with business associates, covered entities are required to enter into written agreements (in the form of a business associate agreement) that protect the use and security of PHI. Under HITECH, business associates may be subject to direct civil and criminal penalties imposed by regulators and state authorities for failing to protect PHI in accordance with HIPAA's Security Rule.

In addition to the federal HIPAA and HITECH, many states have enacted state healthcare laws governing the use of patient medical information. While the federal HIPAA pre-empts any state law that provides less protection for PHI, state laws that are more protective will survive federal pre-emption.

Insurance

The insurance and reinsurance industry has continued to outsource a variety of functions and implement emerging technologies, which are designed to decrease costs and improve the efficiency of outsourced insurance functions. Outsourced functions often include insurance and reinsurance accounting services, actuarial analytics, underwriting analysis, insurance policy and endorsement drafting and processing, claims reporting and handling, business process management, insurance software development, data entry and customer service. Companies in the insurance space – whether policyholders, captive insurers, insurers, agents, brokers, intermediaries, or others – looking to outsource insurance functions in the USA face unique challenges because, unlike many other industries, insurance in the USA is primarily regulated at the state level. As a result, there is a patchwork of rules that may vary from state to state and may affect insurance outsourcing operations.

Energy

In the energy and utility sector, regulated entities must comply with the Critical Infrastructure Protection (CIP) Reliability Standards, which are mandatory proactive cybersecurity requirements issued and enforced by the North American Electric Reliability Corporation (NERC) and its subsidiary regional entities, and overseen and backstopped by the Federal Energy Regulatory Commission (FERC). The CIP standards are designed to protect and secure cyber-assets associated with critical assets that support the Bulk Electric System (ie, North America's power

grid). All owners, operators and users of the bulk power system, which may include both public and investor-owned utilities, generation and transmission cooperatives, and non-utility owners and operators of electric power generation, and transmission facilities are required to comply with the CIP standards.

A CIP compliance issue may arise in the context of outsourcing when a regulated entity outsources its IT infrastructure or business processes involving access to critical cyber-assets (eg, monitoring and maintenance functions). Regulated entities may run into challenges when choosing foreign outsourcing providers, even if the outsourcing agreement contains robust contractual obligations around compliance with the CIP standards.

Failure to comply with the CIP standards may result in fines and penalties of up to USD1 million per violation per day.

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

As a general matter, the USA does not have a comprehensive federal data protection law. Rather, there are many sources of privacy and data security law at the state, federal and local level. In the USA, there are no specific legal or regulatory restrictions on cross-border data transfers. It is worth noting, however, that there are privacy and data security laws that might apply to the processing of certain data.

Federal Requirements

At the federal level, different privacy and data security requirements tend to be sectoral in nature and apply to different industry sectors or particular data processing activities. For example, Title V of the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to ensure the security and confidentiality of the non-public personal information they collect and maintain. As part of its implementation of the GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule, which states that financial institutions must implement reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of non-public personal information.

Another key example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which was enacted to help ensure the privacy and security of protected health information (PHI) and is discussed above. Industry standards are also relevant, although they do not have the force of law. For example, the Payment Card Industry Association's Data Security Standard (PCI DSS) specifies requirements for relationships between companies and their vendors that process credit card holder data.

In addition to federal requirements, a number of states have enacted laws that require organisations that maintain personal information about state residents to adhere to general information security requirements. For example, California's information security law requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorised access, destruction, use, modification, or disclosure. Additionally, information security laws in Massachusetts and Nevada impose highly prescriptive requirements on organisations with respect to the processing of personal information.

State Requirements

All 50 states, Washington, DC, Guam, Puerto Rico and the Virgin Islands have adopted various legislation requiring notice to data subjects of certain security breaches involving personally identifiable information. Companies who have outsourced data processing tasks to ven-

dors remain responsible for security breaches by those vendors. As a result, outsourcing contracts usually address these issues in some detail, including extensive security requirements, reporting and audit obligations and carefully constructed limitations of liability and indemnities. Customers seek to allocate these risks to providers, arguing that they control and secure the information technology and other infrastructure that is attacked and that risk and liability should follow that control.

Providers attempt to avoid liability for security breaches not caused by their breach of contract and to strictly limit their financial liability for those resulting from their fault. As providers have insisted on limiting their liability, many customers have sought their own insurance coverages for these risks.

The California Consumer Privacy Act of 2018 (CCPA) requires covered businesses to provide a number of rights to California consumers with respect to accessing, deleting and opting out of the sale of personal information. As discussed below, the CCPA offers reduced compliance obligations to businesses that share personal information pursuant to a written contract containing certain prescriptive language. The California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and goes into effect on 1 January 2023, includes requirements for different types of contracting parties, including "service providers" and "contractors". Virginia's Consumer Data Protection Act and Colorado's Privacy Act, both of which also go into effect in 2023, require contracts between "controllers" and "processors", which must include certain provisions. Under these laws, a controller is the party that determines the purpose and means of processing the personal information, and a processor is the party that processes the personal information on behalf of the controller. Notably, these laws in California, Colorado and Virginia also includes requirements when sharing de-identified data with third parties.

Companies in the USA also self-impose limits on the collection, use and sharing of personal information through representations made in privacy policies. Companies are held accountable to these representations through state and federal consumer protection laws.

2.4 Penalties for Breach of Such Laws

There are a variety of penalties that might result from a violation of privacy and data security laws in the USA.

At the federal level, the FTC is the primary regulator that enforces privacy and data security requirements. Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce", has been used by the FTC to bring wide-ranging privacy and data security enforcement actions against entities whose information practices have been deemed "deceptive" or "unfair". Typically, when a company settles an FTC enforcement action, the company signs a consent order requiring it to undertake certain obligations, such as implementing a comprehensive written information security programme and obtaining assessments by a qualified, objective, independent third-party professional, certifying that the security programme is operating with sufficient effectiveness to provide reasonable assurance that the security and confidentiality of sensitive consumer information has been protected. Settlements also often require companies to pay a monetary civil penalty.

At the state level, state attorneys general enforce various state mandates regarding privacy and data security. The attorneys general are granted enforcement authority by state "little FTC acts" as well as state laws that are specifically directed at preventing privacy harms. Many of the little FTC acts also provide for private rights of action

based on the same proscribed deceptive and unfair practices. AG enforcement and private rights of action are also remedies available under the state data breach notification laws.

2.5 Contractual Protections on Data and Security

As a general matter, there is no legally required content that must be included in contracts under current US state and federal privacy and data security law. There are, however, more general requirements for businesses to provide oversight of their service providers, which results in the inclusion of certain data privacy and security provisions in vendor contracts.

Federal Level

At the federal level, for example, under the FTC's Safeguards Rule, financial institutions must require relevant service providers to agree contractually to safeguard non-public personal information appropriately. Pursuant to HIPAA's Privacy Rule, which governs a covered entity's interactions with third parties ("business associates") that handle PHI in the course of performing services for the covered entity, the business associates' obligations with respect to PHI are dictated by contracts with covered entities known as "business associate agreements" (BAAs). BAAs must impose certain requirements on business associates, such as using appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA.

State Level

At the state level, certain state laws require businesses that disclose personal information to non-affiliated third parties to require those entities contractually to maintain reasonable security procedures. Regulations in Massachusetts, for example, require that covered businesses contract with service providers in addition to taking reasonable steps to "select and retain third-party service providers that are capable of maintaining appropriate security measures to protect... personal information..."

Additionally, in order to not be considered a "third party" under the CCPA, a written contract must prohibit the entity receiving the information from selling the personal information or retaining, using, or disclosing the personal information for any purpose other than for the purpose of performing the services specified in the contract, or outside of the direct business relationship between the business and the entity receiving the information. The contract also must include a written certification from the entity receiving the information that it understands and will comply with these restrictions. Also, as noted above, Virginia and Colorado's newly enacted comprehensive data privacy laws, which go into effect in 2023, require contracts between "controllers" and "processors", and such contracts must include, among other things, obligations relating to the confidentiality and security of personal information. Furthermore, the New York State Department of Financial Services' cybersecurity regulations require that covered entities develop and implement a third-party service provider policy that addresses minimum cybersecurity practices of vendors, the due diligence processes used to evaluate vendors, and any contractual provisions required in the agreements with vendors.

Even where there is no legal requirement to do so, it is common practice for companies in the USA to include privacy and data security terms in vendor contracts that establish the vendor's responsibility to protect the data it receives and that assign liability as appropriate in the event of a data breach or other privacy or security violation.

3. CONTRACT MODELS

3.1 Standard Supplier Customer Model

Typically, outsourcing agreements take the form of a master agreement and accompanying statements of work, all of which are heavily negotiated. The master agreement provides an overall structure that should include provisions that are sufficiently detailed to cover a range of services, from long-term ITO services to one-off consulting projects. It usually includes a basic service-level methodology, security and data protection provisions, as well as legal terms of general application, such as compliance with laws, limitations of liability, indemnities, and dispute resolution. The statements of work include detailed statements of services, specific service level commitments, pricing methodologies and any other terms that are unique to the services.

Where multiple jurisdictions are involved, the master agreement may provide a framework for local country agreements to be entered into between local affiliates, which may take into account payment using local currencies (including associated allocation of currency risk), unique intellectual property or labour provisions, and specific compliance issues involving local laws. Also, because the markets tend to reward software revenues with higher share price multiples than services revenues, providers continue to shift revenue from services-only agreements to services agreements coupled with separately priced and separately negotiated software licenses.

3.2 Alternative Contract Models

Increasingly, providers are restructuring their commoditised outsourcing offerings to be delivered "as a service". In those cases, the delivery and pricing models assume that there is little variation in the services, service levels and the related risk allocations and contract terms. Accordingly, the service agreements are standardised and the providers are reluctant to negotiate terms. Customers will often hear that the services will be delivered using a "one to many" delivery model, which is the provider's way of indicating that it is unwilling to make certain concessions that may be specific to that particular customer.

Unique situations are sometimes addressed with alternative structures, such as joint ventures (often in the form of contractual JVs, but sometimes involving equity investments) and "build operate transfer" or other arrangements for captive delivery organisations. These are much less common in the market and are highly negotiated responses to special commercial circumstances.

3.3 Captives and Shared Services Centres

Shared Service and Global Business Services (GBS) Models

Research indicates that customers have generally increased their investments in various shared services and GBS models. This trend reflects broader trends in the outsourcing and information technology services market, including a collective desire for increased automation (including robotic process automation), standardisation of tools and processes, scalability, and the management of data as a strategic asset. By centralising services into a shared service centre and increasing the variety of those services by centralising into GBS models, customers may more easily adopt and implement these solutions at an enterprise level, rather than on a business-unit-by-business-unit basis. The adoption of hybrid shared services models (ie, those involving a third-party business processor) also continue to increase.

This particular trend is due to customers realising that there are certain areas of expertise and technologies that are still better performed by third-party vendors who specialise in those are-

as. Whether adopting a shared services model or a hybrid, contracts governing the provision of services must focus on accountability, quality of services and outputs. Of course, hybrid models involving third parties involve risks not necessarily present in a purely in-house shared services model, and those risks should be mitigated as they ordinarily would in a transaction involving a third-party provider. With that being said, the impact of COVID-19 on traditional delivery models has knocked down many of the barriers associated with shared services and GBS models that previously caused customers to be hesitant in their adoption (see "The Impact of COVID-19" below).

Captive Deals

While there has been a small handful of captive deals recently, adoption of captives appears to be on the decline. As with shared services models, the decline in the provision of services through captives appears to reflect broader trends in the outsourcing market, including a focus on value over cost savings, a reluctance to invest in owned IT assets, and policies of the current administration that favour retention and use of onshore resources. The inability to manage growth effectively and provide opportunities for employees within the captive model also continues to negatively impact the adoption of those models for customers. Contracts governing the creation and management of captives are far more complex than typical outsourcing arrangements and customers should understand the legal risks and transaction costs associated with the adoption of this model upfront.

The Impact of COVID-19

Due to COVID-19, companies around the world increased overall investments in remote work technologies, and have undergone or are in the process of undergoing a complete digital transformation. In the process, many have adopted several of the above models, using each to complement the other. There has been an increase across the board (although, less so with captives) of companies returning to outsourced service models complemented by a shared services centre (often using third-party providers) or a GBS model, where onsite employees are no longer necessary or desirable, and where remote delivery is preferred. Whether this trend continues as COVID-19 infection rates decline remains to be seen.

4. CONTRACT TERMS

4.1 Customer Protections

Protections for customers in outsourcing agreements come in many forms. The main protections for customers come in the form of indemnification obligations, representations and warranties (such as performance, malware/disabling code, services not to be withheld (ie, "no abandonment")), confidentiality and data security obligations, service levels, market currency provisions, disputed charges provisions, additional services provisions, cover services provisions, and detailed service definitions and gap-filler or "sweeps" clauses.

Indemnification Obligations

The claims covered by a party's indemnification obligations often are the subject of intense negotiation. Typical indemnification obligations requested by the customer include IP infringement/misappropriation, personal injury and property damages, violation of law, gross negligence and wilful misconduct, breach of confidentiality and data security, claims by the provider's personnel, and tax liabilities of the provider. Outsourcing providers may request reciprocal indemnities, though not every indemnity should be reciprocal in light of the asymmetrical relationship. Indemnities typically cover only third-party claims; claims by the customer

for the provider's breach are remedied through breach of contract actions.

Representations and Warranties

Remedies for breaches of representations and warranties typically are in the form of defect remediation and damages, but certain representations and warranties, such as services not to be withheld, include additional remedies such as injunctive relief. Remedies for breaches of confidentiality and data security typically take the form of damages, including notification-related costs, and injunctive relief. Remedies for service-level failures typically take the form of financial credits (which generally are not exclusive remedies and sometimes can be "earned back" by the provider) and termination rights.

"Market currency" provisions (eg, benchmarking) typically require the provider to make price concessions based on the results of a benchmarking or other market comparison and could result in no-fee or low-fee termination rights. Disputed charges provisions typically allow the customer to withhold payment for invoicing errors or deficient performance of the services. "Additional services" provisions typically require the provider to perform out-of-scope, but related services at a commercially reasonable price. "Cover services" provisions typically require the provider to cover the difference between the provider's fees and a replacement provider's fees when the original provider is unable to perform the services due to a disaster or other force majeure event.

Detailed scope definitions are typically the best defence against misunderstandings as to the work to be done, but "sweeps" clauses are typically included and require the provider to perform all services that are an inherent, necessary or customary part of the services specifically defined in the agreement as well as all services previously performed by any displaced or transitioned employees.

4.2 Termination

The customer typically has a myriad of rights to terminate an outsourcing agreement (eg, material breach, persistent breach, convenience, data security breach, extended force majeure events, service level termination events, insolvency of provider, regulatory changes, transition failures, change of control of provider). Alternatively, the provider usually may terminate only for non-payment of material amounts. Customers generally require robust exit protections.

These protections generally take the form of termination assistance, which typically includes continued performance of the services for a period of time in order to allow the customer to transition the services either back in-house or to another provider, as well as other exit activities (eg, knowledge transfer, return of data). Exit protections can also include rights to the provider's equipment, software, personnel and facilities.

4.3 Liability

The parties' liability exposure under the outsourcing agreement often is limited both by type and amount. Agreements typically provide that damages are limited to, among others, actual "direct" damages (ie, no consequential or incidental damages, such as lost profit, goodwill) and an aggregate dollar amount cap for claims under the agreement. The aggregate liability cap is highly negotiated. Commonly, the limit is defined as a multiple of monthly charges ranging from 12 to 36 months.

Exceptions to the consequential damages waiver and damages cap are also subject to intense negotiation. Typical exceptions include indemnification claims, gross negligence and wilful misconduct, breaches of confidentiality and breaches of other material terms of the

outsourcing agreement, such as services not to be withheld, compliance with law and failure to obtain required consents. Although an exception for gross negligence and wilful misconduct is sometimes subject to negotiation, many states do not allow a party to disclaim liability for such conduct as a matter of public policy. Also, due to the enormous potential liability exposure related to data breaches involving personal information, many providers will not agree to unlimited liability for such breaches and instead will propose a "super-cap" for such damages that typically is a multiple of the general damages cap.

4.4 Implied Terms

Implied terms, such as warranties for fitness for a particular purpose, merchantability, and non-infringement, are typically disclaimed by the provider and only the express terms in the agreement apply.

5. HR

5.1 Rules Governing Employee Transfers

In the USA, employees are not transferred to the provider as a matter of law. If the parties wish to accomplish such a transfer, they must agree to that as part of the transaction documents, and they must put in place an offer-and-acceptance process to effectuate the transition.

If the employees are not transferred as part of the transaction, the employees will remain employed by the original employer who can, in turn, redeploy the employees on other matters or terminate their employment. In the absence of an employment contract stating otherwise, the employees are employed "at will" and, in the absence of a WARN-Act qualifying event (discussed below), can be terminated at any time for any reason without notice and without the requirement of severance or redundancy pay.

5.2 Trade Union or Workers Council Consultation

The Worker Adjustment and Retraining Notification Act ("WARN Act") is implicated if the outsourcing transaction involves a "mass lay-off" or a "plant closing" as defined in the WARN Act. In the event of a mass lay-off or plant closing, the employer must provide 60 days' advance notice prior to termination. Many states in the USA have their own "Mini-WARN Acts", which must also be accounted for before implementing a termination programme as part of an outsourcing transaction.

5.3 Market Practice on Employee Transfers

Notification to any labour unions will be governed by the terms of any applicable collective bargaining agreements.

6. ASSET TRANSFER

6.1 Asset Transfer Terms

Asset transfers in outsourcing agreements have become increasingly rare, as customer financial teams have sought to avoid owning capital assets and provider service models have trended toward cloud-based models where the provider owns the assets. When asset transfers occur, they usually are made on an "as is" basis with no warranties provided by the party making the transfer, with the exception of clean title to the assets. The parties will often negotiate bitterly over whether the customer must warrant that the transferred assets are sufficient to allow the provider to perform the services and whether the provider is entitled to relief if the assets fail.

Typically, the customer seeks to avoid those provisions and to allocate all of the performance risk to the provider, arguing that the provider has had an opportunity to review the assets and to make provision for potential failures in its pricing

and delivery models. The provider argues that it cannot be asked to do more with the transferred assets than the customer could and that any due diligence is inadequate to identify all possible faults. Sometimes the parties agree to share these risks, limiting the scope of any customer warranties to subsets of assets or burning off the warranty and relief provisions over time or as assets are replaced by the provider.

Hunton Andrews Kurth LLP has more than 20 lawyers working in the outsourcing, technology and commercial contracting practice group. The practice has a global reach, with key office locations in Richmond, Washington, DC, New York, London and Belgium. Related practice areas include outsourcing, commercial contracting and contract life cycle management, information technology, digital commerce, corporate transition and integration services, and privacy and cybersecurity. The firm's lawyers, highly experienced in negotiating outsourcing transactions, have negotiated with all of the major service providers and cultivated deep relationships with all of the major sourcing consultancies. The team has significant experience with outsourcing transactions of all types, from data centre and infrastructure, business process, to HR, facilities management, and FAO.

AUTHORS

Randy Parks is a partner and chair of the global technology and outsourcing practice group, co-chair of Hunton Andrews Kurth's corporate team, and co-chair of its retail and consumer products industry practice group. He has negotiated and documented dozens of large-scale, complex commercial and technology transactions worth billions of dollars for multinational companies. Randy has been consistently recognised for his work on information technology and corporate law. His practice focuses on complex commercial transactions, particularly business process and information technology outsourcing, e-commerce, licensing, systems acquisition, development and integration agreements, manufacturing, supply, distribution, and complex services agreements and multi-country joint ventures.

Jeff Harvey is a partner at Hunton Andrews Kurth. His practice focuses on global outsourcing and technology transactions, complex e-commerce transactions, software audit management and compliance, IoT adoption and implementation, global ERP system implementation and integration, SMAC (social media, mobile technologies, analytics and cloud) transactions, digital media placement and buys, and cloud/as-a-service transactions across a wide variety of industries. He has negotiated and documented significant sourcing and other information technology transactions valued at several billion dollars across the globe, and assisted his clients with the post-execution management of those transactions.

Andy Geyer is a partner at Hunton Andrews Kurth. Highly regarded in the outsourcing space, he handles complex domestic and international business process and technology-related transactions for clients in a variety of industries. Andy offers clients innovative, value-driven solutions to challenging information technology outsourcing, business process outsourcing, procurement, licensing, commercial contracting and general corporate matters. Andy is lauded for his strength in IT outsourcing and overall IT contract negotiation. His extensive knowledge of the field and industry also enables Andy to counsel clients successfully on software audits and licensing, intellectual property and data management issues.

Cecilia Oh is a partner at Hunton Andrews Kurth with extensive experience with ITO/BPO outsourcing and complex technology transactions, including those involving technology licensing, software-as-a-service, fintech, application development, systems integration and e-commerce. She represents a wide spectrum of clients, including in the financial services, retail, healthcare, hospitality and transportation industries, ranging from industry leaders to start-ups. In addition, Cecilia advises clients on the use of electronic signatures, payment processing, private label and co-branded card programmes, and banking platforms. Cecilia has been recognised for her practical and tailored approach to advising her clients and for her depth of market understanding.

Hunton Andrews Kurth LLP

200 Park Avenue
New York, NY 10166
USA

Tel: +1 212 309 1000
Fax: +1 212 309 1100
Email: info@hunton.com
Web: www.huntonAK.com

HUNTON
ANDREWS KURTH

Trends and Developments

Contributed by:
Randy Parks, Jeff Harvey, Andy Geyer and Cecilia Oh
Hunton Andrews Kurth LLP see p.21

Introduction

In the US outsourcing industry, developments have been largely incremental in 2021 with three super-trends continuing their trajectories:

- migration to digital operating models to capture new opportunities and savings;
- massive and increasing investment in data protection, cybersecurity, and compliance resources in response to threats to digital infrastructure; and
- reworking of contracting models to increase agility and prioritise results.

These super-trends manifest themselves in nine key long-term strategic evolutions:

- a shift to "as a service" offerings;
- migration to the cloud;
- increasing adopting of automation;
- the digital transformation of traditional business models and the conversion of data flows into revenue-generating products and analytical tools;
- evolving security services and cybersecurity/data protection requirements;
- increasing industry and process-specific compliance challenges;
- a shift to "outcome based" commercial models;
- continuing swings in emphasis between value/innovation and cost savings, driven by industry-specific economic conditions and opportunities; and
- a bias towards shorter contract durations.

Key short-term, tactical developments in 2021 include:

- the effects of the COVID-19 pandemic; and
- continuing evolution of US state laws addressing data protection.

Digital Operating Models

Evolutions in technology over the past decade have dramatically changed the way information technology services are delivered and consumed and how firms go to market. "As a service" and cloud-based offerings continue to multiply and take market share from legacy models. These products appeal to customers who prefer to buy more-or-less standardised functionality delivered through a web browser, rather than procure and manage a complicated network of hardware, software, employees, and contractors. The delivery and pricing models for these services assume that there is little variation in the services, service levels and the related risk allocations and contract terms. Accordingly, the service agreements are standardised and the providers are reluctant to negotiate terms.

Providers also are increasingly integrating into their offerings robotic process automation (RPA), machine learning, and, to a lesser extent, artificial intelligence (AI). Most outsourcing transactions now include some form of these tools. RPA typically is delivered through a software platform and customised "bots" capable of performing tasks often handled by lower-cost human operators. The legal issues raised by these implementations are not new and usually revolve around ownership of intellectual property in the bots, pricing of additional bots (both new development and cloning) avoiding proprietary automa-

tion platform lock-in, data protection and ownership, sharing of savings, and displacement of workers.

"Internet of Things" (IoT) transactions are accelerating, as provider offerings mature and buyers seek the benefits of sensor- and data-heavy product offerings.

Machine learning and AI

Implementations that deploy more capable machine learning and AI solutions raise far more interesting questions. For example, what disclosure and warranties will the vendor provide regarding what the AI is doing and what it must not do? Will the customer be permitted to audit the AI and is the customer even capable of doing so effectively? These questions are particularly acute when the AI is integrated into decision-making processes that carry the potential for legal liability.

Legislators and regulators have taken notice of the potential for misuse of AI with encoded bias. For example, in 2019, Illinois adopted the Artificial Intelligence Video Interview Act, which prohibits an Illinois employer from using AI to evaluate job interview videos in certain circumstances. Similar bills have been introduced or enacted in Colorado, California, Massachusetts, Maryland, New Jersey, Washington, and New York City, some of which would impose bias auditing and other compliance requirements on AI users, enforced through civil penalties. As of September 2021, the National Conference of State Legislatures was tracking legislation addressing AI generally in 17 states and legislation specifically addressing autonomous vehicles in 26 states.

Intellectual property and AI

Also important is the question of who owns the intellectual property in the AI and its outputs? This question particularly concerns buyers of "expert" AI systems, who deploy them to optimise business processes that they view as key competitive advantages. To maximise the value of the AI, the customer must disclose its trade secret processes and historical data to "train" the system. While this raises conventional issues of confidentiality and ownership of the disclosed IP, the customer must also consider who owns the insights generated by the AI in processing the customer's data and how the vendor is permitted to use and profit from the AI that the customer has helped to train.

The nightmare for the category-leading customer is that the vendor takes the AI-generated insights and newly-trained AI and turns them into a category-killing product in which the customer has no financial participation. Savvy vendors recognise this concern and are willing to address it effectively.

Critically, customers must consider how the AI system and related projects and data uses will comply with applicable data protection laws. In the United States, various state and sector-specific laws require businesses to enter into written agreements with service providers that limit the service provider's ability to process the data for any purpose other than to perform the services and to employ reasonable safeguards to protect the data. A key consideration when entering into a contract with a vendor is to ensure that the vendor's access to and use of such data does not run afoul of representations the business owner has made to data subjects whose personal information is being processed in connection with the AI model.

With the recent enactment of the California Consumer Privacy Act of 2018 (CCPA), the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act (2021, effective 2023), and the Colorado Privacy Act (2021, effective 2023), the US legal regime is beginning to shift

to one that offers individuals certain rights with respect to their data (ie, access, deletion, and opt out of sale), moving away from the notion that businesses that collect the data are "owners" of such information with the autonomy to use the data indefinitely and without question as long as appropriate notice and choice were offered at the outset.

Vendors and customers are leveraging the confluence of efficient technologies, capable automation, and cheap, ubiquitous sensors and consumer technologies to transform their existing business processes and deploy new ones. Examples include business collaboration tools with robust social-media style functionality, smart-manufacturing tools to optimise production, business "internet of things" implementations allowing continuous communication with products while in use, and consumer subscription models for security, entertainment, health and fitness, finance, and education.

Each of these models generate specific questions of compliance, liability management, cyber-risk, and a host of other legal issues typical of information technology transactions. However, for large buyers, the sheer volume and pace of evolution of these models creates a new set of more strategic concerns, including: how to efficiently procure solutions at speed; how to manage cybersecurity, data protection, and compliance risks across a rapidly multiplying vendor population; and how to manage a vendor population that may include under-capitalised start-ups that cannot possibly satisfy claims against them, but which offer a must-have business solution.

Cybersecurity, Data Protection and Compliance

As the trend to digitisation accelerates and data flows expand, vendors and customers are making increasing investments in cybersecurity, data protection, and compliance in response to increased threats from bad actors, increased regulatory scrutiny, and an increasingly active plaintiff's bar. Data breaches, ransomware attacks, and other cyber-attacks are announced almost daily and law enforcement and private security firms regularly warn of new threat agents (including nation states and organised crime) and attack vectors.

Legislators, regulators, and trade organisations are considering and adopting a range of cybersecurity and data protection requirements, including: the California, Virginia and Colorado laws noted above, and other state and local laws; new security standards for federal government contractors; at least 23 federal bills in the 117th Congress addressing data; and evolutions of regulations and guidance for industry sectors, such as New York's Cybersecurity Regulations for financial institutions, potential changes by the FTC to the Safeguards Rule under the Graham-Leach-Bliley Act, and updates to the Payment Card Industry's Data Security Standard.

As threats and regulations multiply, firms are relying more heavily on managed security services, and "security as a service" offerings to replace or augment their in-house capabilities. Given the sensitive subject matter and potentially catastrophic consequences of a service failure, these transactions often are heavily negotiated and require a holistic liability management structure, supplementing contractual liability allocations with vendor and buyer insurance coverages and operational changes (such as broad-scale encryption) to manage risks.

Reworking of Contracting Models

The shift in buyer preference to procuring functionality rather than assets is mirrored in contracting models. Strategic buyers prefer contracts that prioritise and incentivise delivery of services that are tightly tied to positive business

outcomes. For example, instead of charges based on a build-up of hardware, software, and labour costs, a customer might prefer to pay by the transaction or even based on its revenue in the business line supported by the vendor. Similarly, service credits (or performance bonuses) might be linked to metrics that correspond to business success, rather than an abstract measure of system performance.

The pace of change also continues to put pressure on contact durations. Since technologies, delivery models, and costs evolve so rapidly, both vendors and customers are reluctant to lock themselves into long-term agreements. This reluctance manifests itself in "as a service" agreements that permit the vendor to change or discontinue the service on a few months' notice and in three to five-year terms for more complex outsourcing agreements, possibly with renewal terms that are subject to price escalators. Sectoral economic conditions continue to drive shifts in transaction volume and to influence the balance between transactions focused on value/innovation and cost savings.

Sectors under financial stress generally see increases transactions driven by cost savings (eg, retail and healthcare), while high-growth sectors see transactions seeking to leverage vendor capabilities to drive revenues and open new markets (eg, financial services).

Short-Term Developments

Underlying all of the outsourcing industry activity this year have been the effects of the global COVID-19 pandemic. Providers and buyers appear to have reached equilibrium with respect to the tension between work-from-home mandates and the security issues posed by distributed delivery models. Most providers have conceded that COVID-19 is not a force majeure event, since the risks and work-arounds are well understood. However, the Delta variant has made clear that exacerbations of the pandemic might be force majeure and contract language has evolved accordingly. The forced transition to work-from-home has suppliers and customers both thinking about whether the shift – and related cost savings – can or should be made permanent.

Contributed by: *Randy Parks, Jeff Harvey, Andy Geyer and Cecilia Oh,* ***Hunton Andrews Kurth LLP***

Hunton Andrews Kurth LLP has more than 20 lawyers working in the outsourcing, technology and commercial contracting practice group. The practice has a global reach, with key office locations in Richmond, Washington, DC, New York, London and Belgium. Related practice areas include outsourcing, commercial contracting and contract life cycle management, information technology, digital commerce, corporate transition and integration services, and privacy and cybersecurity. The firm's lawyers, highly experienced in negotiating outsourcing transactions, have negotiated with all of the major service providers and cultivated deep relationships with all of the major sourcing consultancies. The team has significant experience with outsourcing transactions of all types, from data centre and infrastructure, business process, to HR, facilities management, and FAO.

AUTHORS

Randy Parks is a partner and chair of the global technology and outsourcing practice group, co-chair of Hunton Andrews Kurth's corporate team, and co-chair of its retail and consumer products industry practice group. He has negotiated and documented dozens of large-scale, complex commercial and technology transactions worth billions of dollars for multinational companies. Randy has been consistently recognised for his work on information technology and corporate law. His practice focuses on complex commercial transactions, particularly business process and information technology outsourcing, e-commerce, licensing, systems acquisition, development and integration agreements, manufacturing, supply, distribution, and complex services agreements and multi-country joint ventures.

Jeff Harvey is a partner at Hunton Andrews Kurth. His practice focuses on global outsourcing and technology transactions, complex e-commerce transactions, software audit management and compliance, IoT adoption and implementation, global ERP system implementation and integration, SMAC (social media, mobile technologies, analytics and cloud) transactions, digital media placement and buys, and cloud/as-a-service transactions across a wide variety of industries. He has negotiated and documented significant sourcing and other information technology transactions valued at several billion dollars across the globe, and assisted his clients with the post-execution management of those transactions.

Andy Geyer is a partner at Hunton Andrews Kurth. Highly regarded in the outsourcing space, he handles complex domestic and international business process and technology-related transactions for clients in a variety of industries. Andy offers clients innovative, value-driven solutions to challenging information technology outsourcing, business process outsourcing, procurement, licensing, commercial contracting and general corporate matters. Andy is lauded for his strength in IT outsourcing and overall IT contract negotiation. His extensive knowledge of the field and industry also enables Andy to counsel clients successfully on software audits and licensing, intellectual property and data management issues.

Cecilia Oh is a partner at Hunton Andrews Kurth with extensive experience with ITO/BPO outsourcing and complex technology transactions, including those involving technology licensing, software-as-a-service, fintech, application development, systems integration and e-commerce. She represents a wide spectrum of clients, including in the financial services, retail, healthcare, hospitality and transportation industries, ranging from industry leaders to start-ups. In addition, Cecilia advises clients on the use of electronic signatures, payment processing, private label and co-branded card programmes, and banking platforms. Cecilia has been recognised for her practical and tailored approach to advising her clients and for her depth of market understanding.

Hunton Andrews Kurth LLP

200 Park Avenue
New York, NY 10166
USA

Tel: +1 212 309 1000
Fax: +1 212 309 1100
Email: info@hunton.com
Web: www.huntonAK.com

HUNTON
ANDREWS KURTH