Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Technology & Outsourcing 2023

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

USA: Law & Practice and Trends & Developments

Jeffrey Harvey, Randall Parks,
Andrew Geyer and Cecilia Oh
Hunton Andrews Kurth LLP

USA

Law and Practice

Contributed by:
Jeffrey Harvey, Randall Parks, Andrew Geyer and Cecilia Oh
Hunton Andrews Kurth LLP

Contents

Hunton Andrews Kurth LLP has more than 15 lawyers working in the outsourcing, technology and commercial contracting practice group and another 30 in its closely related privacy and cybersecurity practice. The practice has a global reach, with key office locations in Richmond, Washington, DC, New York, London and Brussels. Related practice areas include enterprise IT, contract life cycle management, digital commerce, blockchain/crypto, and corporate transition and integration services, where they have support from outsourcing subject-matter experts in employment, IP, and tax. The firm's lawyers are highly experienced in negotiating outsourcing transactions, having negotiated extensively with all the major service providers and built strong relationships with all the major sourcing consultancies. The team has significant experience of IT outsourcing and business process outsourcing transactions of all types, including IT infrastructure and applications support, HR outsourcing, finance and accounting outsourcing, R&D, and facilities management.

Authors

Jeffrey Harvey is a partner at Hunton Andrews Kurth LLP, where he chairs the global technology and outsourcing practice group. His practice focuses on IT, business processes, sourcing and system integration/implementation, e-commerce, and various commercial contracting. He also focuses on the implementation and integration of social media, mobile technologies, analytics and cloud computing services (SMAC), along with emerging technologies such as AI and the metaverse. Jeffrey has negotiated, documented and assisted with significant sourcing, e-commerce and other IT transactions valued at several billion dollars across the globe, as well as assisting his clients with the post-execution management of those transactions.

Randall Parks is a partner at Hunton Andrews Kurth LLP and chairs the firm's executive committee. With more than 20 years of experience, he has negotiated and documented dozens of large-scale, complex commercial and technology transactions worth billions of US dollars for multinational companies. Randy has consistently been recognised for his work in IT and corporate law. His practice focuses on complex commercial transactions, particularly business process and IT outsourcing, e-commerce, licensing, systems acquisition, development and integration agreements, manufacturing, supply, distribution, and complex services agreements and multi-country joint ventures.

Andrew Geyer is a partner at Hunton Andrews Kurth LLP, where 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 business process and IT outsourcing, procurement, licensing, commercial contracting and general corporate matters, and is highly regarded for his strength in IT outsourcing and overall IT contract negotiation. Andy's extensive knowledge of the field and industry also enables him to counsel clients successfully on software audits and licensing, IP, and data management issues.

Cecilia Oh is a partner at Hunton Andrews Kurth LLP, with extensive experience of business process/IT outsourcing and complex technology transactions involving technology licensing, software as a service (SaaS), fintech, application development, systems integration and e-commerce. She represents a wide spectrum of clients, ranging from industry leaders to start-ups, in the financial services, retail, healthcare, hospitality and transportation industries. She also 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 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

1. Market Conditions

1.1 IT Outsourcing

Key market developments in IT outsourcing include:

- the continued shift of physical IT assets to cloud environments and from software programs to software as a service (SaaS) environments;
- the provision of services and solutions that are supported by AI and robotics;
- the provision of customer-usable tools and technologies that are powered by AI; and
- the digital transformation of traditional business data flows into revenue-generating products and analytical tools, as 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 traditional sole-source agreements into a multitude of different agreements. More providers are competing for and providing smaller chunks of services, with more demands being placed on client procurement departments.

Of the above-mentioned factors, generative AI is currently the trendiest and is also likely to have the most significant near-term impact on providers and customers. The following are among the other issues arising in this context.

- IP ownership in generative AI outputs is currently somewhat of a "hot button" issue, as many cases litigating ownership of the various outputs continue to work their way through the courts.
- AI models may have been trained on "biased" models or models that are overly reliant on data without additional context, thereby increasing the potential for discriminatory hiring practices.
- Privacy concerns are also front-of-mind as concerns grow over the potential of AI models to "scrape" personal information and use it in a manner not intended by the data subject.
- Given the potential for these technologies to remove the "human" element from the workforce, there may be personnel issues for HR to review.

1.2 Business Process Outsourcing (BPO)

Key market developments in BPO include:

- an increased focus on social media, including the metaverse, as the primary tool for communicating with customers;
- the provision of services and solutions that are supported by robotics, AI 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 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 in the following ways.

- 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.

- 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 AI in the BPO market presents similar issues to those noted in respect of IT outsourcing market developments (see **1.1 IT Outsourcing**). As firms lean into outbound communications through social media, compliance with applicable regulatory regimes (eg, the Telephone Consumer Protection Act) and exposure to a robust plaintiffs' bar become key issues.

Companies with a presence in the metaverse must consider legal implications as though they are operating in the outside world, even if only interacting with avatars and cryptocurrency.

1.3 New Technology

The impact of new technology (eg, AI, robotics, blockchain, smart contracts and the metaverse) is most evident in the IT 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 more cheaply, without sick days, without raises and without vacations. Low-skilled workers are feeling the brunt of these new technologies, in addition to more restrictive immigration policies being used to prevent lower-skilled workers from entering the USA. However, higher-skilled workers tasked with the development and management of such technologies (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 IP 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. There does not currently appear to be a "one-size-fits-all" solution to managing AI risk. Instead, most advisors are advising clients to analyse each AI offering on a case-by-case basis and in the unique context in which it will be deployed.

The current debate pertaining to the metaverse concerns whether or not it is dead. Application of the metaverse has been wildly successful in the gaming industry, as "free" games such as Fortnite, Roblox and Minecraft have earned billions of dollars in a relatively short period of time. However, transitioning the metaverse into an online environment for adults to interact with each other – and, importantly, interact with businesses – has proven far more challenging. While the metaverse is hardly dead, it has yet to take hold to the extent most analysts predicted and its heyday is likely several years away.

1.4 Outsourced Services

The most commonly outsourced services in the USA are:

- IT;
- HR;
- call centre;
- service desk;
- accounting;
- security;
- facilities management;
- logistics;

• social media design/marketing; and
• web design/development.

"IT" encompasses a broad range of services, including application development/maintenance, data centre outsourcing, and SaaS/cloud/hosting services.

2. Regulatory Environment

2.1 Restrictions on Technology Transactions or Outsourcing

Private Sector

Despite state and federal law-makers' 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 **2.2 Industry-Specific Restrictions**, 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 Sector

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 and offshore resources, 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 are often subject to scrutiny by elected officials, watchdog organisations, consumer groups and the media, which can complicate and delay negotiations.

Offshore Restrictions

In addition, offshore outsourcing may be limited or restricted under certain government-sponsored programmes. By way of an example, the Main Street Lending Program – a federal programme established under the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") to offer loans to SMEs 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

Financial Services

In the USA, various state and federal regulators oversee financial institutions through a system of functional regulations. 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 extends not only to the bank's own activities but also to 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 origi-

nators 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 inter-agency guidance – which is largely based on the OCC's existing guidance – would replace and harmonise:

- the Federal Reserve's *Guidance on Managing Outsourcing Risk*, issued in 2013;
- the OCC's *Third-Party Relationships: Risk Management Guidance*, issued in 2013 and supplemented with FAQs in 2020; and
- the FDIC's *Guidance for Managing Third-Party Risk*, issued in 2008.

The proposed guidance provides a multidisciplinary 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 and implementing of strategies and policies to address third-party risks, thereby 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 – ending third-party relationships in an efficient matter, including consideration of appropriate transition services.

Similar to the existing guidance from 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, including compliance with HIPAA's Privacy and Security Rules, 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 entities.

When entering into outsourcing arrangements with business associates, covered entities are required to enter into written agreements (in the form of business associate agreements) 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. Although 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, as well as implement emerging technologies that 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 (and its subsidiary regional entities) and overseen and backstopped by the Federal Energy Regulatory Commission. The CIP standards are designed to protect and secure cyber-assets associated with critical assets that support North America's power grid, the Bulk Electric System. All owners, operators and users of the bulk power system (which may include both public and investor-owned utilities, generation and transmission co-operatives, 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 those business processes that involve 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 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 laws at the state, federal and local levels. 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, the different privacy and data security requirements tend to be sectoral in nature and apply to different industry sectors or particular data-processing activities. By way of an 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 HIPAA, which was enacted to help ensure the privacy and security of PHI, as discussed in **2.2 Industry-Specific Restrictions**. Industry standards are also relevant, although they generally do not have the force of law. By way of an example, the Payment Card Industry Association's Data Security Standard specifies requirements for relationships between companies and their vendors that process cardholder data.

State Requirements

In addition to federal requirements, a number of states have enacted laws requiring organisations that maintain personal information about state residents to adhere to general information security requirements. 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 more prescriptive requirements on organisations with regard to the processing of personal information.

All 50 states, plus DC, Guam, Puerto Rico and the Virgin Islands, have adopted legislation requiring notice to data subjects of certain security breaches involving personally identifiable information. Companies that have outsourced data-processing tasks to vendors 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 – as the providers control and secure the IT and other infrastructure that is attacked – 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 custom-

ers have sought their own insurance coverage for these risks.

The California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020, requires covered businesses to provide a number of rights to California consumers with regard to:

- accessing, deleting, correcting and opting out of the sale of personal information; or
- sharing personal information for purposes of cross-context behavioural advertising.

As discussed in **4.5 Data Protection and Cybersecurity**, the CCPA also includes requirements for different types of contracting parties, including "service providers" and "contractors".

In addition, Virginia's Consumer Data Protection Act (VCDPA), Colorado's Privacy Act (CPA), Utah's Consumer Privacy Act (UCPA), and Connecticut's Data Privacy Act (CTDPA) all came into effect in 2023. These laws provide rights to residents of their respective states, including as to access, deletion, and opting out of sale and targeted advertising relating to personal information. These laws all 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, whereas a processor is the party that processes the personal information on behalf of the controller. Notably, the CCPA, CPA, UCPA and CTDPA also include requirements when sharing de-identified data. A growing number of states have enacted comprehensive privacy laws with similar requirements that go into effect in 2024 and beyond.

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.

3. Model Outsourcing Contracts

3.1 Standard Contract 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 IT outsourcing services to one-off consulting projects. It usually includes a basic service-level methodology, security and data protection provisions, and 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.

Agreements Covering Multiple Jurisdictions

Where multiple jurisdictions are involved, the master agreement typically provides a framework for local country agreements to be entered into between local affiliates. This may take into account payment using local currencies (including associated allocation of currency risk), unique IP or labour provisions, specific compliance issues involving local laws, and any country-specific enforcement requirements. 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 ser-

vices agreements coupled with separately priced and separately negotiated software licences.

3.2 Alternative Contract Models

Multi-sourcing

While highly consolidated "mega" deals (ie, a single contract with a single vendor who provides the full suite of IT services to the customer) are still frequently negotiated, multi-sourcing remains the primary contracting model for most customers. Under a multi-sourcing model, customers engage multiple vendors (through individual contracts) to collectively provide the full suite of IT services desired by the customer. The multi-sourcing model permits customers to mix and match "best of" technologies provided by unrelated vendors in order to achieve a more optimal IT environment. This model is not without problems, however, as successfully integrating products offered by different vendors can be a challenge and more cooks in the kitchen can result in finger-pointing if there is an issue.

Shared Service and Global Business Services Models

Research also indicates that customers have generally increased their investments in various shared services and global business services (GBS) models. This trend reflects broader trends in the outsourcing and IT 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 in 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 continues to increase.

This particular trend is down 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 areas. 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 be 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.

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 be made aware of the legal risks and transaction costs

associated with the adoption of this model upfront.

Other Approaches

Unique situations are sometimes addressed with alternative structures, such as joint ventures (often in the form of contractual joint ventures, but sometimes involving equity investments) and "build operate transfer" (BOT) arrangements. These are highly negotiated responses to special commercial circumstances and are much less common in the market – although there has been a very recent uptick in BOT arrangements.

3.3 Digital Transformation

In response to the COVID-19 pandemic, 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 models discussed in **3.2 Alternative Contract Models**, using each to complement the other. There has been an increase across the board (albeit less so with captives) in companies returning to outsourced service models complemented by a shared services centre (often using third-party providers) or a GBS model, where on-site employees are no longer necessary or desirable, and where remote delivery is preferred.

As a result, providers are restructuring their commoditised outsourcing offerings to be delivered "as a service". In such 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.

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 (eg, performance, malware/disabling code, and services not to be withheld ("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 are often the subject of intense negotiations. 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, although 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 typically remedied through breach of contract actions.

Remedies

Remedies for breaches of representations and warranties are typically in the form of defect remediation and damages – although 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 are not generally exclusive remedies and can sometimes be "earned back" by the provider) and termination rights.

Cost-Related Protections and Scope

"Market currency" provisions (eg, benchmarking) generally 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 usually allow the customer to withhold payment for invoicing errors or deficient performance of services. "Additional services" provisions typically require the provider to perform out-of-scope but related services at a commercially reasonable price. "Cover services" provisions tend to 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 tend to be the best defence against misunderstandings over the work to be done. "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 reasons 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). The provider, on the other hand, may usually only terminate for non-payment of material amounts.

Customers also require robust exit protections. These protections generally take the form of termination assistance, which often 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 an outsourcing agreement is often limited both by type and amount. Agreements typically provide that damages are limited to, among other things, actual "direct" damages (ie, no consequential or indirect damages). The amount that can be recovered – as well as whether such amount will serve as an aggregate cap on liability – tends to be heavily negotiated. The limit is usually defined as a multiple of monthly charges ranging from 12 to 36 months. In those agreements where the liability cap is not a per claim cap, a liability cap reset concept is generally included. These can take many forms – the most common of which are annual/biannual liability caps and the inclusion of a termination right in favour of the customer if the provider refuses to reset back to zero the damages that have contributed to the cap after

the damages sustained by the customer have reached a certain percentage of the cap.

Exceptions to the consequential/indirect damages waiver and liability 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 (eg, services not to be withheld, compliance with the 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, owing to the enormous potential liability exposure related to data breaches involving personal information, many providers will not agree to unlimited liability for such breaches. Instead, they will propose a "super-cap" for such damages, which is usually 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.

4.5 Data Protection and Cybersecurity

In addition to required content that must be included in contracts pursuant to the CCPA and similar state privacy laws, businesses also are generally required to provide reasonable oversight and management of their service providers that process personal information.

Federal Level

At the federal level, 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 regard to PHI are dictated by contracts with covered entities, known as "business associate agreements" (BAAs). BAAs must impose certain requirements on business associates - for example, 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 to contractually 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, under the CCPA, businesses must enter into contracts with service providers that include a number of restrictions and obligations. By way of an example, the contract must prohibit the service provider from:

- selling or sharing the personal information;
- combining the personal information that the service provider receives from (or on behalf of) the business with personal information that it receives from (or on behalf) of another person or persons – or personal information that the service provider collects from its own

interaction with the consumer - except for limited permitted purposes; and
- retaining, using, or disclosing the personal information either:
  (a) outside the direct business relationship between the service provider and the business; or
  (b) for any purpose other than for the business purposes specified in the contract, including retaining, using or disclosing the personal information for a commercial purpose other than as specified in the contract or as otherwise permitted by the CCPA.

The CCPA also includes requirements for contracts with "contractors" and "third parties" (each as defined in the CCPA). Also, as noted in **2.3 Restrictions on Data Processing or Data Security**, other state comprehensive privacy laws require contracts between "controllers" and "processors". 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 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.

4.6 Performance Measurement and Management

In the USA, there are no common contractual clauses that help the customer manage and measure the supplier's performance in technology transactions and outsourcing.

4.7 Digital Transformation

Although several of the contract terms mentioned throughout **4. Contract Terms** arerelevant in cloud-based offerings, the customer's ability to obtain concessions from a cloud provider on such contract terms is more challenging, owing to the commodity nature of such offerings. Cloud-based deals are also generally for a shorter term than traditional outsourcing agreements and more narrow in scope, which reduces the need for certain terms (eg, market currency and sweeps clauses).

5. Employment Matters

5.1 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. They must also 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 (see **5.2 Role of Trade Unions or Workers Councils**) – can be terminated at any time for any reason,

without notice and without severance or redundancy pay.

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

5.2 Role of Trade Unions or Workers Councils

The Worker Adjustment and Retraining Notification Act (the "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 Offshore, Nearshore and Onshore

One of the principle drivers for customers in all outsourcing transactions is reduced costs. Providers are generally more capable of achieving these cost reduction goals when they employ their offshore resources. Accordingly, a significant portion of the provider's delivery centres continue to be located offshore. Additionally, given global inflation rates, there may have been a slight uptick in "onshoring".

However, on the whole, the USA is experiencing roughly the same allocation of deals among offshore, nearshore and onshore vendors as in previous years. Customer preferences that pertain to geographical considerations continue to be:

- whether sensitive personal information is in-scope;
- level of geography-specific risk;
- whether a particular service is customer-facing;
- talent of resources;
- cost savings; and
- criticality of services.

5.4 Remote Working

If employees are working remotely from a state other than the state where the employer-company has office locations, the company must evaluate the need to comply with the state laws of the states where the employees are working. This includes (but is not limited to) state leave, workers' compensation, and unemployment compensation laws. The company should also evaluate whether employee presence in those states triggers an obligation to register to do business in those states and whether the employer would be subject to corporate tax obligations in those states due to the presence of employees in the states.

Trends and Developments

Contributed by:
Jeffrey Harvey, Randall Parks, Andrew Geyer and Cecilia Oh
Hunton Andrews Kurth LLP

Hunton Andrews Kurth LLP has more than 15 lawyers working in the outsourcing, technology and commercial contracting practice group and another 30 in its closely related privacy and cybersecurity practice. The practice has a global reach, with key office locations in Richmond, Washington, DC, New York, London and Brussels. Related practice areas include enterprise IT, contract life cycle management, digital commerce, blockchain/crypto, and corporate transition and integration services, where they have support from outsourcing subject-matter experts in employment, IP, and tax. The firm's lawyers are highly experienced in negotiating outsourcing transactions, having negotiated extensively with all the major service providers and built strong relationships with all the major sourcing consultancies. The team has significant experience of business process and IT outsourcing transactions of all types, including IT infrastructure and applications support, HR outsourcing, finance and accounting outsourcing, R&D, and facilities management.

Authors

Jeffrey Harvey is a partner at Hunton Andrews Kurth LLP, where he chairs the global technology and outsourcing practice group. His practice focuses on IT, business processes, sourcing and system integration/implementation, e-commerce, and various commercial contracting. He also focuses on the implementation and integration of social media, mobile technologies, analytics and cloud computing services (SMAC), along with emerging technologies such as AI and the metaverse. Jeffrey has negotiated, documented and assisted with significant sourcing, e-commerce and other IT transactions valued at several billion dollars across the globe, as well as assisting his clients with the post-execution management of those transactions.

Randall Parks is a partner at Hunton Andrews Kurth LLP and chairs the firm's executive committee. With more than 20 years of experience, he has negotiated and documented dozens of large-scale, complex commercial and technology transactions worth billions of US dollars for multinational companies. Randall has consistently been recognised for his work in IT and corporate law. His practice focuses on complex commercial transactions, particularly business process and IT outsourcing, e-commerce, licensing, systems acquisition, development and integration agreements, manufacturing, supply, distribution, and complex services agreements and multi-country joint ventures.

Contributed by: Jeffrey Harvey, Randall Parks, Andrew Geyer and Cecilia Oh, **Hunton Andrews Kurth LLP**

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

Cecilia Oh is a partner at Hunton Andrews Kurth LLP, with extensive experience of business process/IT outsourcing and complex technology transactions involving technology licensing, software as a service (SaaS), fintech, application development, systems integration and e-commerce. She represents a wide spectrum of clients, ranging from industry leaders to start-ups, in the financial services, retail, healthcare, hospitality and transportation industries. She also 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 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

Contributed by: Jeffrey Harvey, Randall Parks, Andrew Geyer and Cecilia Oh, **Hunton Andrews Kurth LLP**

Introduction

Developments in the US outsourcing industry have been largely incremental in 2023. Three super-trends continuing their trajectories are:

- migration to digital operating models in order to capture new opportunities and savings, including through the increased use of machine learning and AI-based tools and solutions;
- 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 (although, looking back over the past year, this shift appears to have been in nomenclature only);
- continuing swings in emphasis between value/innovation and cost savings, driven by industry-specific economic conditions and opportunities; and
- a bias towards multi-sourcing and shorter contract durations.

Digital Operating Models

Evolutions in technology during 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. Although the largest cloud and as-a-service providers are reluctant to heavily negotiate and alter the terms of their existing agreements, middle-market providers (who may leverage the services of the larger providers as part of their offerings) are much more likely to do so.

Providers are also increasingly integrating robotic process automation (RPA), machine learning, and AI into their offerings. Most outsourcing transactions now include some form of these tools. RPA is typically delivered through a software platform and customised "bots" capable of performing tasks often handled by lower-cost human operators. Providers sell solutions that are enabled by AI, but there is currently very little transparency when it comes to the solutions themselves. This often leaves customers wondering if the providers are truly leveraging AI or just marketing the latest trend in the technology space. With that being said, providers are beginning to offer generative AI-based tools that are available for use directly by customers – often in the form of virtual assistants, chatbots,

and personalised experience generation. At this juncture, however, it is too early to tell whether these solutions and tools are as revolutionary as the industry claims.

The legal issues raised as a result of the provision and use of these new technologies are not entirely new and usually revolve around:

- ownership of IP in relation to the bots (or, in the case of generative AI, the outputs);
- pricing of additional bots (both new development and cloning);
- avoiding proprietary automation platform lock-in;
- privacy concerns over AI tools "scraping" the Internet;
- biased data (or, biased human intervention in the data) used to develop AI models;
- data protection and ownership;
- sharing of savings; and
- displacement of workers.

Internet of things (IoT) transactions continue to accelerate, as provider offerings mature and buyers seek the benefits of sensor- and data-heavy product offerings.

Machine learning and AI

Machine learning and AI solutions are capable of sorting through massive amounts of data to, in many cases, reach their own conclusions. In the absence of human intervention, there is no room for context or consideration of "soft" factors – hence the solutions reach conclusions based solely on the data they were trained on and subsequently collect. This one-track-mindedness of the solutions poses problems when their output 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. 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 and places particular emphasis on the potential for racial biases resulting from the use of AI. 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.

Additionally, multiple states have enacted AI-targeted amendments to their respective privacy laws. Colorado, Connecticut and Virginia, for example, have enacted laws that:

- give consumers the right to opt out of automated profiling; and
- require a data protection assessment for activities that pose a "heightened risk of harm".

In the 2023 legislative session, Indiana, Montana, Oregon, Tennessee and Texas also passed consumer privacy laws that include provisions governing AI – some of which mirror those passed by Colorado, Connecticut, and Virginia.

As of July 2023, the National Conference of State Legislature was tracking legislation addressing AI in at least 25 states as well as Puerto Rico and Washington, DC. Out of these jurisdictions, 14 states and Puerto Rico have adopted resolutions or enacted legislations.

Intellectual property, traditional AI and generative AI

Also important is the issue of who owns the IP in the AI and its outputs. The answer to this question differs depending on the type of AI solution deployed. Traditional AI systems process data based on a predetermined set of rules and logic, generally performing a specific task to increase efficiency through repetition. Generative AI processes data against a base data set and develops creative or new content as a result.

Buyers of traditional AI systems must disclose their trade secret processes and historical data to establish the aforementioned predetermined set of rules and logic. Although 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 through 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 provider 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 providers recognise this concern and are willing to address it effectively.

Buyers of generative AI solutions are less concerned with the development of a category-killing product by the provider than they are with the source and creation of the output itself. Generative AI solutions generally "scrape" publicly available sources of data in order to deliver new output that is responsive to various queries from end users. The data resulting from the query is typically based on any number of other data sources – the origin of which is unknown. By way of an example, a generative AI solution may be trained by using several of a famous artist's greatest works. If an end user then requests that the solution create a brand new image, as if this author painted it, the generative AI solution will fulfil the request. The famous artist neither trained the AI solution nor painted the new image, but the generative AI solution used this author's style of painting and previous works – in combination with other data – to develop the new image. Is the new image a derivative work of the author's images used to train the generative AI solution? Is "training" a generative AI model a "fair use" or a permissive use? Consider the impact on this author's career (and their incentive to produce creative works) if users can obtain works of any image that appears as if the artist painted them.

Similarly, buyers of generative AI solutions must understand the risks associated with treating output as though it is owned by the buyer. If 1,000 separate buyers each ask their own instance of the solution to perform the same task, then the output may be exactly the same or substantially similar for each of the 1,000 buyers. Can any one of the buyers legitimately claim ownership? Providers of generative AI solutions generally make it clear that all risk associated with the use of the output, including any risk of infringement, is borne by the end user.

In reality, many of these issues are not settled and are currently working their way through the courts as of the time of writing (October 2023).

Critically, and in cases of both traditional AI and generative AI, customers must consider how the AI system and related projects and data uses will comply with applicable data protection laws, and whether any data protection laws were violated by the collection of such data. In the USA, various state and sector-specific laws require businesses to:

- enter into written agreements with providers whereby the provider's ability to process the data for any purpose other than performing the services is limited; and
- employ reasonable safeguards to protect the data.

A key consideration when entering into a contract with a provider is to ensure that the provider's access to and use of such data does not run afoul of representations the business owner – whether the customer in a customer/provider relationship or a provider who hosts data online – has made to data subjects whose personal information is being processed in connection with the AI model.

With the recent enactment of almost a dozen state privacy regimes, including the California Consumer Privacy Act of 2018 (CCPA), the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act 2021 (effective 2023), the Colorado Privacy Act 2021 (effective 2023) and the Utah Consumer Privacy Act 2022 (effective 2023), the US legal regime is continuing to shift to one that offers individuals certain rights with regard to their data (ie, access, deletion, and opt-out of sale). This shift represents a move 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 IoT 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 IT transactions. However, for large buyers, the sheer volume and pace of evolution of these models creates a new set of more strategic concerns, such as:

- 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 towards 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 above-mentioned California, Virginia and Colorado laws, as well as other state and local laws;
- new security standards for federal government contractors;
- at least 30 federal bills in the 117th Congress addressing data; and
- evolutions of regulations and guidance for industry sectors, such as:
  (a) New York's Cybersecurity Regulations for financial institutions;
  (b) updates to the Payment Card Industry's Data Security Standard;
  (c) the Biden administration's Executive Order on reproductive health data; and
  (d) continuing rulemaking by the FTC on a wide-range of commercial surveillance, data security, algorithmic decision-making, and digital advertising topics.

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 are often heavily negotiated and require a holistic liability management structure, which supplements contractual liability allocations with vendor and buyer insurance coverages and operational changes (such as broad-scale encryption) in order 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 prioritising and incentivising delivery of services that are tightly tied to positive business outcomes. By way of an 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. Given that 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 update the service without the customer's approval and typically have terms of three to five years, 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 – for example, retail and healthcare – generally see increased transactions driven by cost savings. High-growth sectors such as financial services, however, see transactions seeking to leverage vendor capabilities to drive revenues and open new markets.

Short-Term Developments

The ongoing effects of the global COVID-19 pandemic have continued underlying much of the outsourcing industry activity in 2023. Providers and buyers appear to have reached equilibrium with regard to the tension between managing a remote workforce and the security issues posed by distributed delivery models. Most providers have conceded that COVID-19 is not a force majeure event, given that the risks and workarounds are well understood.

However, the COVID-19 variants have made clear that exacerbations of the pandemic might be force majeure and contract language has evolved accordingly. Customers and providers alike are cautiously optimistic that the worst of the virus is over; however, winter is coming and – along with it – come new virus variants and fresh fears that the virus will experience a resurgence.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com