Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Outsourcing

USA
Hunton Andrews Kurth LLP

chambers.com

2019

Law and Practice

Contributed by Hunton Andrews Kurth LLP

Contents

Hunton Andrews Kurth LLP (New York - HQ) as a firm has 1,000 attorneys, and its Outsourcing, Technology and Commercial Contracting group has 21. The practice has a global reach, and key office locations include Richmond, Washington DC and London. Related practice areas include: outsourcing, commercial contracting and contract lifecycle management, information technology, digital commerce, corporate transition and integration services, and privacy and cybersecurity. Outsourcing transactions are critical to the ongoing operations of an organisation and involve many complex issues that require subject-matter experience from a wide variety of practice areas. The Hunton Andrews Kurth team includes outsourcing-savvy lawyers from our tax, privacy and data security, intellectual property, immigration, benefits, and labour and employment practices.

Authors

Randy Parks is a partner and chair of the global technology and outsourcing practice group, co-chair of the firm's corporate team, co-chair of its retail and consumer products industry practice group and serves on the firm's executive committee. He has negotiated and documented dozens of large-scale, complex commercial and technology transactions worth billions of dollars for multinational companies, including retailers, manufacturers and consumer products companies. Randy has been consistently recognised for his work on information technology, corporate law and mergers and acquisitions. 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. His practice focuses on global outsourcing, technology, e-commerce and commercial contracting transactions. He also focuses on information technology, business processes, sourcing and system integration/implementation, e-commerce, commercial contracting and various intellectual property matters. He also focuses on the implementation and integration of social media, mobile technologies, analytics and cloud computing services (SMAC). He has negotiated, documented and assisted with significant sourcing and other information technology transactions valued at several billion dollars.

Andy Geyer is a partner. Highly regarded in the outsourcing space, Andy Geyer 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 (ITO), business process outsourcing (BPO), procurement, licensing, commercial contracting and general corporate matters. Andy is lauded for his strength in IT outsourcing and overall IT contract negotiation. His deep 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 Cecilia Oh is a partner and has deep experience with complex commercial and innovative technology transactions, especially pertaining to e-commerce, outsourcing, payments and FinTech services. She has negotiated and documented several complex, large-scale outsourcing transactions, including for some of the largest financial institutions and retailers in the United States. Cecilia's work often involves providing practical advice to clients on core banking platforms, PCI DSS compliance and emerging payment solutions, such as mobile wallets.

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.

1.2 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
- a shift in focus to value over cost savings.

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 now become much 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.

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 United States), higher-skilled workers tasked with their development and management (eg, developing platforms for the cryptocurrency market) have greater opportunities.

1.4 Other Key Market Trends

With the adoption of newer technologies and more restrictive immigration policies decreasing the need for (and supply of) lower-skilled and lower-wage workers, companies are increasingly moving away from labour arbitrage and toward higher value propositions. Accordingly, lawyers should ensure that contracts governing these services and technologies provide a mechanism for clients to measure, report upon and realise the value provided by the supplier, as outcomes are more important to today's clients than processes.

2. Regulatory and Legal Environment

2.1 Legal and Regulatory Restrictions on Outsourcing

There are no US federal laws that specifically restrict outsourcing in the private sector. As discussed in further detail below, certain regulated industries, such as the financial services 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, watch-dog organisations, consumer groups and media, which can complicate and delay negotiations.

2.2 Industry-Specific Restrictions

Financial Services

In the US, 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. Such guidance effectively requires financial institutions to implement risk-management practices with respect to their third-party relationships that are commensurate with the level of risk involved. In particular, such guidance focuses on:

- the performance of due diligence on such third-party vendors (and their downstream vendors);
- ongoing oversight of third-party and fourth-party vendors;
- business resilience for critical activities;
- adequate assurances relating to liability and other key contract terms in a written agreement; and
- the protection of non-public personal information.

Financial institutions are required to take these considerations into account when formalising outsourcing arrangements with third parties.

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") by regulating 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 preempts any state law that provides less protection for PHI, state laws that are more protective will survive federal preemption.

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

As a general matter, the United States 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 US, 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.

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. Addition-

ally, information security laws in Massachusetts and Nevada impose highly prescriptive requirements on organisations with respect to the processing of personal information.

All 50 states, 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 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 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.

Companies in the United States 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 United States.

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.

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.

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 be considered a "service provider" under the California Consumer Protection Act of 2018, a written contract must prohibit the entity receiving the information from "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business...." Additionally, the New York State Department of Financial Services' cybersecurity regulations require that, by 1 March 2019, 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 US 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 for a range of services, from long-term ITO 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, limitations of liability, indemnity, 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 paying in local currencies. Occasionally, this basic structure is sometimes supplemented by stand-alone licences for software products or side agreements for specific service offerings.

3.2 Alternative Contract Models

Increasingly, providers are restructuring their commoditized 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.

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

Research indicates that customers have generally increased their investments in various shared services 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, 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 likely 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 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 in a transaction involving a third-party provider.

While there has been a small handful of captive deals over the last twelve months, 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.

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.

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.

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 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 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 the requested 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, etc). 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, etc). 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, etc) 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, several 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 United States, 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

Hunton Andrews Kurth LLP
Riverfront Plaza,
East Tower
951 East Byrd Street
Richmond,
VA 23219

HUNTON
ANDREWS KURTH

Tel: +1 804-788-8200
Fax: +1 804-788-8218
Email: info@hunton.com
Web: www.huntonAK.com

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 United States 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.