GLOBAL SOURCING

TRENDS IN 2016

INSIDE

KEY CONTACTS

LONDON

Alistair Maughan
+44 20 79204066

Susan McLean
+44 20 79204045

NEW YORK

John F. Delaney
+1 212 468 8040

Vivian L. Hanson
+1 212 506 7393

WASHINGTON, D.C. / NORTHERN VIRGINIA

Christopher D. Ford
+1 202 887 1512

Thomas J. Knox
+1 703 760 7317

Scott W. Stevenson
+1 202 887 1549

SAN FRANCISCO

Paul E. Jahn
+1 415 268 6387

Aaron P. Rubin
+1 415 268 6809

William I. Schwartz
+1 415 268 7449

TOKYO

Masato Hayakawa
+81 3 3214 6522

HONG KONG

Gordon A. Milner
+85 2 2585 0808

MORRISON FOERSTER

At the beginning of the year, we surveyed Morrison & Foerster's Global Sourcing Group lawyers from around the world to create a snapshot of the current state of the global outsourcing market and to identify emerging trends that are likely to shape the market over the next 12 months. This year, our lawyers comment on the role of cloud computing in outsourcing transactions, the increased reliance on robotic process automation, the impact of the *Browning-Ferris* decision and the recent developments in European privacy law.

This report is based on our lawyers' views and experiences over the last year, as well as their conversations with service providers, outsourcing consultants and clients. Our thanks to industry observers from other organizations who participated in this report.

CONTINUED RISE OF CLOUD COMPUTING

As anticipated in our last Global Sourcing Trends advisory, we continued to see a steady – and ongoing – increase in the role of cloud computing in outsourcing transactions.

The benefits of cloud computing – including rapid deployment, scalability, lower costs and operational flexibility – are now well known to enterprise consumers of IT services and to the sourcing professionals that advise them. With most major IT providers now offering variations of cloud services, many of which have matured and have been tested in recent years through smaller deployments, larger enterprise customers are more confidently exploring the possibility of using cloud services in conjunction with their outsourcing strategies. We expect that momentum to continue to build in 2016 and for cloud computing to appear in outsourcing transactions in an increasing variety of forms.

In some cases, cloud services will be included as a component of multi-sourced solutions where customers seek best-in-breed solutions from a panel of providers. For example, a customer might obtain the storage capabilities of its multi-sourced solution from a cloud provider while obtaining other services from non-cloud solutions. Increased use of this approach will advantage providers with expertise at integrating and managing cloud services as a component of a multi-provider solution.

More significantly from the standpoint of a market trend, we increasingly see outsourcing providers package offerings of "traditional" data center-centric outsourcing solutions with options for customers to convert to cloud solutions during the term of the contract. The lengthy duration of many outsourcing relationships warrants structuring contracts to accommodate shifts to new technologies (particularly when the new technology is emerging with the apparent dominance of cloud services) without requiring a wholesale renegotiation.

This approach allows customers to transition to cloud solutions over time as offerings mature and internal stakeholders buy-in, which would alleviate some of the risk to the provider that it will lose the deal to lower rates offered by pure-play cloud providers. Of course, the economic benefits that customers experience with a move to a cloud option will likely come at some cost in terms of contractual protection.

Accordingly, customers negotiating outsourcing contracts can expect to be presented with addenda that modify select terms of the outsourcing contract as applicable to cloud offerings. For example, providers may seek to alter certain data security and business continuity commitments, service level obligations, change control procedures, subcontracting limitations, audit rights and termination for convenience rights with respect to cloud services. In most cases, this means customers will have to relinquish some degree of flexibility and control. We expect, however, that customers will seek to leverage the larger overall outsourcing transaction in order to improve on the terms typically available in the market for one-off contracts for cloud services.[1]

The inclusion of a cloud option in outsourcing contracts may remind sourcing professionals of the earlier trend of "transformational outsourcing," where the value proposition of the transaction depended on implementation of a future "transformed" solution. As with that trend, the ability of customers to realize the anticipated benefits of cloud solutions as part of their outsourcing agreements will depend on many factors, including proper structuring of the contract and effective transition planning.

While we anticipate that outsourcing providers will increasingly offer and promote these cloud solutions, we expect that the pace of adoption by global enterprises will be measured as these sophisticated buyers of IT services continue to exercise caution when moving to cloud-based offerings. This will particularly be the case with companies that operate in industries in which meeting regulatory requirements remains a key concern[2] and for global enterprises concerned about the changing compliance framework for cross-border data transfers.[3] As regulatory guidance emerges, compliance mechanisms are validated and solutions mature (including further development of private and hybrid cloud offerings as viable alternatives to the public cloud), we expect the implementation of cloud services as a core element of outsourcing solutions to accelerate.

1 For a discussion of negotiating cloud contracts, *see* "Negotiating Cloud Contracts," December 18, 2014.

2 For an overview of recent guidance issued by the Financial Conduct Authority (FCA) for UK-regulated financial services firms, *see* "Cloud Computing in the Financial Services Sector – the UK FCA Gets On-Message," November 25, 2015.

3 *See*, "Cloud Data Security Standards Reach New Heights?" March 26, 2015.

INCREASED RELIANCE ON ROBOTIC PROCESS AUTOMATION

Outsourcing service providers are increasingly seeking to rely on robotic process automation (RPA) as a way to reduce costs and error rates, improve regulatory compliance, provide services more efficiently and increase profits.

RPA has matured rapidly and, while the scale of savings and efficiencies is hard to state definitively, there is clear evidence in the outsourcing market of RPA's practical application and its increasing importance to both service providers and their customers. RPA is clearly well advanced on the journey through to mainstream acceptance.

RPA is the use of software with machine-learning capabilities and artificial intelligence to manipulate data and perform repetitive, rules-based tasks that were previously performed by service providers' employees. RPA "robots" can perform anything from basic tasks, such as data gathering, to sophisticated analysis using artificial intelligence to understand meaning and context of unstructured data.

If used appropriately, RPA enables businesses to perform tasks:

- **At a lower cost:** According to data from KPMG, for example, a 40 to 75 percent cost reduction can be delivered by the adoption of RPA, and approximately 100 million workers may be replaced by RPA robots over the next 10 years;
- **More quickly and efficiently:** RPA-based processes can be run non-stop for 24 hours a day, every day of the year. According to data from technology company Xchanging, robots processing insurance-related tasks can process over 30,000 cases per month and have reduced the processing time from 5 minutes to under 10 seconds. Similarly, mobile phone company Telefónica O2 deployed more than 160 robots to process between 400,000 and 500,000 transactions each month, yielding a three-year return on investment of over 650 percent; and
- **More accurately:** RPA robots, if programmed correctly, are less likely to make errors and will apply rules and logic consistently when performing tasks—thus improving regulatory compliance, for example. RPA also delivers a basis of service provision that is more scalable to volumetric changes in an organization's demand.

- Despite the headline-grabbing success stories, little discussion has taken place on the impact of RPA on the terms of outsourcing contracts. Most commentary has focused on the typical benefits of RPA and on advising customers to ensure they receive a reduction in costs when their service provider is using RPA to streamline and improve the services. The adoption and application of RPA does not merely affect cost, however. Other issues include:
- Who is responsible—and liable if the robot fails to perform as envisaged—for mapping the various systems and processes to be replaced by the robots?
- Who is responsible—and liable if the robot fails to perform as envisaged—for developing the decision-making parameters and exceptions to be applied by the robots? Who would be liable if a recommended course of treatment does not result in a successful outcome for a patient? Who would be liable if a mortgage application was incorrectly rejected?
- How does an RPA-based solution fit within an organization's enterprise level security? There will understandably be nervousness about the creation of new automated systems and the impact that they will have on security of the enterprise.
- Will the traditional definition of key employees, such as account managers, remain applicable? Arguably, the employees who have programmed the robots (both those who write the code and those who "train" the robot to do the right thing) are more important to the success of the project, so both customers and service providers will want to ensure that appropriate processes are in place to ensure that the loss of the employees who program the robots does not adversely affect their continued operation.
- How does RPA sit with existing value for money mechanisms? Unless contract terms are properly constructed, customers risk relinquishing to service providers the majority of the benefits of RPA advances. Contractual benefits-sharing mechanisms will become increasingly important.
- How should "ownership" of the robot/RPA engine be determined? Who owns the IP rights in the software or rules engine, the service provider

or the customer? On what terms can a service provider leverage its solution for one particular customer on behalf of other customers?

- What happens after termination of the outsourcing contract? Is the service provider entitled to retain the robot/rules engine or does the customer have the right to obtain the source code/rules and prevent the service provider from continuing to use it?
- How can interoperability be ensured? The customer and the service provider will need to ensure that the robots are compatible with the customer's present and likely future systems. In general, the evolution of automation standards will be a key gating factor to determine the speed of mainstream implementation of RPA.
- How will data collection ensure privacy? The customer will need to ensure that it has appropriate consents in place from individuals whose personal information is processed by robots and that it imposes appropriate contractual obligations on the service provider with respect to the storage, access and processing of that information. This is particularly the case where robots may be used to process sensitive personal information (e.g., health insurance claims, differential analysis of symptoms, the diagnosis of illnesses and treatment planning—the last of which is not as far away as one might think; currently, IBM's Watson supercomputer can, among a myriad of other skills, analyze a patient's medical information against an array of data to make treatment recommendations for cancer patients).
- Will the adoption of RPA result in the early termination of existing outsourcing contracts? Unlike traditional outsourced services, RPA can be deployed in-house if the correct skills are available. Given that RPA can be programmed to perform specific tasks for a particular business, customers may be less likely to purchase commoditized off-shore outsourcing services that may not be "quite right" and that may result in the payment of substantial set-up and customization costs to the service provider. Customers may also repatriate work from off-shore locations if the level of service provided by the robots is better and more consistent than what is currently offered by its service provider.

RPA will remain a hot topic and key consideration for businesses in 2016 and beyond. We expect more companies to look at the potential applications and benefits of RPA. While the information available to date supports the view that RPA can be very beneficial to certain businesses, we would urge companies to consider the broader legal, technical, security, cost and staffing implications of any proposed RPA solution. The timing of RPA's evolution from its growth stage to maturity depends on many factors, and that includes the degree of pragmatism and realism of the claims that service providers make for the benefits that RPA can deliver.

BROWNING-FERRIS DECISION'S AFFECT ON OUTSOURCING TRANSACTIONS

It is no surprise that how well a Service Provider's employees perform is an important factor in the success of any outsourcing arrangement. As a result, most outsourcing contracts contain numerous provisions regarding employee-related issues. Such provisions include: requirements that Service Providers perform background checks on their employees; the ability to remove Service Provider employees from the performance of the services if the customer believes that having those persons working on the account is not in the best interest of customer; and requirements that certain key persons remain on the account for a designated period of time and cannot work on the accounts of competitors for a period of time after they cease working on the customer's account. Depending on the kind of deal and the needs of the customer, the agreement may place many other restrictions on the Service Provider and the use of its employees.

Because of these restrictions, customers have always been concerned about co-employment issues in outsourcing contracts. In a nutshell, co-employment refers to the situation where two employers *retain and exercise* control over a single employee's work. The more restrictions on the Service Provider relating to the use of its employees, the more risk that the customer could face co-employment issues. If deemed to be co-employed, the Service Provider employee could claim that the customer owes such person the same rights and privileges that it gives to similarly situated employees of the customer, as well as that the customer is obligated to treat that person as an employee, including meeting statutory and tax requirements associated with that person.

As a result of the concern of customers, certain practices have become customary to avoid co-employment. For example, customer personnel would not directly give direction to a Service Provider

to direct the worker's activities through his or her supervisor – an employee of Service Provider; customers would not provide working tools (e.g., laptops) to Service Provider employees; customers would restrict Service Provider employees' access to privileges provided to employees (e.g., access to the company gym); and customers would ensure that Service Provider employees would not be invited to employee-related functions (e.g., parties and picnics). All of these actions would be taken as indicia that the person was not an employee of the customer, but was solely employed by the Service Provider.

Historically, these indicia would be sufficient to show that no employment relationship existed between the customer and the employees of the Service Provider. In fact, the Internal Revenue Service created a 20-factor test to determine whether a person engaged to perform functions by an entity is an independent contractor or an employee of that entity. That 20-point test was designed to evaluate whether the customer controls how the employee's work is performed.[4] Outsourcing customers have customarily relied upon the 20-point test to gauge their actions in avoiding co-employment situations.

Then came the National Labor Relations Board (NLRB) decision in *Browning-Ferris Industries of California, Inc.*[5] Said case involved the issue of whether employees of a staffing agency (Leadpoint) hired by Browning-Ferris (BFI) could be represented by a union that represented BFI employees. The union named BFI and Leadpoint as employers of such workers. *Browning-Ferris* changed the landscape of what determines a co-employment relationship. In addition to the determining factor being whether the customer *exercised direct* control over the Service Provider employees, additional determining factors could be whether the customer *reserved* authority to control such person's terms and conditions of employment or whether the customer exercised *indirect* – such as through an intermediary – control over such person's employment. Accordingly, the test no longer is only whether the customer exerted direct and immediate control over the Service Provider personnel, but also whether the customer either retained the ability to exert such control or exerted control indirectly through the Service Provider.

The NLRB found that BFI and Browning-Ferris were co-employers and cited a number of factors to support that finding.

> ***Hiring, Firing, and Discipline.*** The NLRB not only found that BFI had and exercised significant control over hiring and firing (e.g., requiring Leadpoint employees to pass drug tests and barring the hiring of individuals who previously had worked for BFI but who BFI had deemed ineligible for rehire), but also retained such indirect hiring and firing rights as: (a) requiring that Leadpoint employees satisfy certain standard BFI selection procedures and tests, (b) rejecting any worker that Leadpoint referred to its facility "for any reason or no reason," and (c) "discontinuing the use of any personnel" that Leadpoint had assigned.

> ***Supervision, Direction of Work, and Hours.*** The NLRB also found that BFI exercised direct control over "the processes that shape" the day-to-day work of Leadpoint's employees. It noted as being of "particular importance" BFI's unilateral control over the speed of [the work] and specific productivity standards. The NLRB noted that BFI managers told Leadpoint employees to work "faster and smarter" and frequently counseled them against stopping [workflow]. Further, while communicating to Leadpoint employees through Leadpoint supervisors (i.e., exercising indirect control), BFI assigned specific tasks that needed to be completed, specified where Leadpoint employees were to be

4 The 20-point test included such factors as level of instruction given by the customer to the worker, degree that the workers are integrated into the business operations, length of continuous relationship of the company and the worker, provision of tools and materials, control over discharge or termination, etc.

5 *Browning-Ferris Industries of California, Inc., d/b/a BFI Newby Island Recyclery, and FPR-II LLC, d/b/a Leadpoint Business Services, and Sanitary Truck Drivers and Helpers Local 350, International Brotherhood of Teamsters, Petitioner*, 2015 NLRB LEXIS 672; 204 L.R.R.M. 1154; 2014-15 NLRB Dec. (CCH) P16,006; 362 NLRB No. 186 ("*Browning-Ferris*").

positioned and provided near-constant oversight of employee work performance. Additionally, the NLRB found that BFI specified the number of workers that it required, dictated the timing of work shifts and decided when overtime would be necessary. And while BFI did not select the specific Leadpoint employees who would perform the work on any given shift, those employees were required to obtain the signature of an authorized BFI representative for their hours each week in order to get paid.

Wages. In addition, the NLRB found that BFI played a significant role in determining Leadpoint employee wages. Under the parties' contract, Leadpoint determined employee pay rates, administered payments, retained payroll records and was responsible for employee benefits. However, Leadpoint was contractually barred from paying its employees more than any BFI employees performing the same work.

Many, if not most, outsourcing agreements contain the kinds of protections and abilities for customers to exercise control, directly or indirectly, over Service Providers that were contained in the BFI/Leadpoint arrangement. Customers argue that they require these provisions in the agreement in order to ensure quality over their environment and the products they create. Based on the *Browning-Ferris* decision, however, just the inclusion of these provisions (regardless of whether the rights are exercised) significantly increases the risk of co-employer liability. The outsourcing customer is left with the choice of retaining the operational control (managing quality control with the ability to exert control over the Service Provider's employees) while increasing its risk of joint employer liability, or minimizing the risk of joint employer liability but risking that its operation may not be run in an optimal way.

The question is whether the goals of exercising reasonable control and avoiding joint employer liability are mutually exclusive. The answer is no, but certain precautions must be taken.

- First, remove all unnecessary control factors from the outsourcing agreement. Some easy examples include:
    - Removing any requirement that the Service Provider employee meets the standards set forth in customer's background check policy. Instead, review the Service Provider's background check policy for sufficiency and require a covenant that Service Provider will not place anyone on the account that does not meet those standards, or require a representation that all persons on the account meet those standards. Either way, it does not appear as if the Service Provider employee must meet customer's employment standards;
    - Removing any requirement that Service Provider personnel be pre-approved by customer, other than perhaps certain enumerated Key or Critical Persons;
    - Limiting customer's ability to remove Service Provider personnel from the account. Instead of customer requesting removal and Service Provider being obligated to conform, create a governance structure to allow performance issues to be raised (which would address issues related to employees), and allow Service Provider's internal policies to determine whether removal is appropriate. Customer should be provided a copy of those policies; and
    - Ensuring that the contract contains no provisions that could be construed as affecting Service Provider employees' payment, including not tying bonuses or increases to customer satisfaction surveys or reports.
- Second, the customer must be careful to not overstep its bounds. It is often easy for customers to use their leverage to direct Service Provider employee activities and work structure, even if such rights do not exist in the agreement. Such direction should not occur directly with the worker or indirectly through the Service Provider.
- Finally, include in the agreement provisions whereby the Service Provider must indemnify the customer against any claims brought by a Service Provider employee claiming that such individual is entitled to any salary, benefits or other perquisites to which an employee of the customer would be entitled. A similar indemnification should be included that protects the customer against claims relating to co-employment made by a governmental authority.

In conclusion, the *Browning-Ferris* decision has made it far easier for employees of Service Providers, temporary agencies and similar organizations to

claim that they are employees of the entity with which its actual employer contracted. No longer must a buyer of services exert actual and immediate control over its contracting party's employees to create an employer-employee relationship, but that relationship can also be created where the buyer retains the right through contract (without exercising the right) to exert control, or actually exerts control, indirectly through the contracting party. The outsourcing customer must be vigilant and take the proper precautions to ensure that it avoids the criteria that would make it an unintended employer.

RECENT DEVELOPMENTS IN EUROPEAN PRIVACY LAW AND HOW THEY AFFECT OUTSOURCING PROJECTS

The last months of 2015 and the early months of 2016 have been turbulent in the European data privacy field. A number of very notable developments—each with a potentially significant impact on cross-border outsourcing projects—have followed each other in a short period of time.

Invalidation of U.S.-EU Safe Harbor

First, in October 2015, the European Court of Justice (ECJ) struck down the U.S.-EU Safe Harbor Framework that had been in effect since 2000. Many U.S. companies, including U.S.-based outsourcing service providers, relied on the protection of Safe Harbor Framework in order to safely transfer personal information from customers in Europe to the United States.

The ECJ ruled that the Safe Harbor mechanism does not prevent U.S. companies from sharing data with the U.S. government, nor does it allow European individuals the ability to obtain judicial redress in the United States against such sharing. As a result, the Framework did not meet the requirements of "adequacy" as required under EU law, and thus was invalid (*see* our client alert of October 6, 2015).

The effect of the ruling was that outsourcing service providers (and their outsourcing customers whose data was being processed) faced the need to seek and implement alternative transfer mechanisms, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), or rely on the consent of the respective individuals.

Although national European data protection authorities granted a grace period until the end of January 2016 for putting in place alternative transfer mechanisms, both customers and service providers faced a tight squeeze for the alternatives to be finalized in time.

Many in the market hoped that the European Commission and the U.S. Department of Commerce would expedite their efforts of putting in place a "Safe Harbor 2.0," which they had been working on since 2014. However, in the months following the ECJ ruling, updates on a new Safe Harbor Framework were lacking. Instead, some national European data protection authorities took the ECJ ruling to conclude that the considerations that invalidated the Safe Harbor could equally apply to the alternative mechanisms of SCCs and BCRs (*see* our client alert of October 15, 2015).

It wasn't until February 2, 2016, that the European Commission and the U.S. Department of Commerce held a joint press conference announcing that they had reached an agreement on the principles of a Privacy Shield as a successor to the Safe Harbor Framework. The final text of the Privacy Shield was released on February 29, 2016 (*see* our client alert of March 3, 2016).

On April 13, 2016, the Article 29 Working Party (WP29) issued its opinion on the Privacy Shield in which it requested clarifications on a number of what it considered shortcomings of the agreement (such as the complexity of redress mechanisms available to individuals and restrictions on mass surveillance), and urged the EU and the United States to make changes to the Privacy Shield accordingly. The WP29 confirmed that companies can continue to rely on other transfer mechanisms (e.g., SCCs and BCRs).

According to the European Commission, the Privacy Shield should be finalized and take effect by July 2016, but this may be pushed back depending on the progress made on the points that the WP29 has raised.

General Data Protection Regulation

In the meantime, the European Commission, the EU Parliament and the EU Council have been working diligently towards the finalization of another ambitious project, namely the reform of EU privacy legislation.

Privacy legislation in Europe has consisted of national implementations of the EU-wide Privacy Directive, which has been in effect for over 20 years. However, technological developments such as the Cloud, data analytics and Big Data, as well as the increased use of outsourced and managed services, have led EU lawmakers to work on a successor to the Privacy Directive.

In December 2015, the Commission, Parliament and Council concluded their negotiations and agreed on the final text of the General Data Protection Regulation (GDPR) which, once in force, will harmonize European privacy law because of its direct effect in European Union Member States without the need to be separately implemented in national law.

The GDPR was formally adopted in April 2016 and will be published in the Official Journal of the EU in early May (*see* our client alert of April 15, 2016). The GDPR will enter into force 20 days after such publication and will apply after a two-year transition period (i.e., over the course of 2018). Many companies have already initiated preparations to assess and address their new obligations under the GDPR.

Amongst the many changes that the GDPR will bring —the number of articles increased from 34 in the Privacy Directive to 99 in the GDPR—are enhanced contractual requirements that customers (including organizations implementing outsourcing projects) will need to put in place when engaging service providers. These now include, for example, the service provider's promise to only process data via documented instructions from the customer, including for transfers, confidentiality commitments, consent from the customer for enlisting sub-processors, a duty of care in selecting sub-processors and deleting or returning personal information upon the end of the provision of the data processing service.

Other notable changes include the requirement (upon customers) to carry out Privacy Impact Assessments when implementing new systems and processes, as well as the obligation to notify the data protection authority and/or affected individuals of data security breaches. For outsourced services, customers will in both cases require cooperation and input from the service provider and will seek to address this in the agreement.

And, unlike the Privacy Directive, not all obligations are for customers (acting as "data controllers") only. The GDPR will now introduce obligations that apply directly to service providers (acting as "data processors"), where service providers have an establishment in the EU or offer their services transferring data into the EU.

It is expected that, as a result of the increased requirements under the GDPR, customers and service providers will want to (and sometimes need to) put in place more detailed and elaborate contractual provisions to address their respective obligations under the law, as well as their contractual positions towards each other (including their respective liabilities). For a more extensive discussion on the new requirements under the GDPR, *see* our client alerts of December 18, 2015 and of March 23, 2016.