MAYER·BROWN

Issue 22 | Fall 2015

Business & Technology Sourcing
REVIEW

About Our Practice

Mayer Brown's Business & Technology Sourcing (BTS) practice is one of the global industry leaders for Business Process and IT Outsourcing as ranked by Chambers & Partners, The Legal500 and the International Association of Outsourcing Professionals (IAOP). With more than 50 dedicated lawyers—many having previous experience with leading outsourcing providers and technology companies—the practice has advised on nearly 300 transactions worldwide with a total value of more than $100 billion.

Editors' Note

Kevin A. Rang
Chicago
+1 312 701 8798
krang@mayerbrown.com

Derek J. Schaffner
Washington DC
+1 202 263 3732
dschaffner@mayerbrown.com

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

Welcome to the Fall 2015 edition of the Mayer Brown *Business & Technology Sourcing Review*.

Our goal is to bring you smart, practical solutions to your complex sourcing matters in information technology and business processes. We monitor the sourcing and technology market on an ongoing basis, and this Review is our way of keeping you informed about trends that will affect your sourcing strategies today and tomorrow.

In this issue, we cover a range of topics, including:

- Innovation in Outsourcing Arrangements
- Service Levels for SAAS
- Trade Payables (Receivables) Monetization Techniques
- The New EU General Data Protection Regulation
- Internet of Things
- Growing Trends in Sourcing

You can depend on Mayer Brown to address your sourcing matters with our global platform. We have served clients in a range of sourcing and technology arrangements across multiple jurisdictions for more than a decade.

We'd like to hear from you. If you have any suggestions for future articles or comments on our current compilation, or if you would like to receive a printed version, please email us at BTS@mayerbrown.com.

If you would like to contact any of the authors featured in this publication with questions or comments, we welcome your interest to reach out to them directly. If you are not currently on our mailing list, or would like a colleague to receive this publication, please email contact edits@mayerbrown.com with full details. ◆

Securing the Benefit of Innovation in Outsourcing Arrangements

Mark A. Prinsley
Brad L. Peterson
Derek J. Schaffner

Mark A. Prinsley
London
+44 20 3130 3900
mprinsley@mayerbrown.com

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

Derek J. Schaffner
Washington DC
+1 202 263 3732
dschaffner@mayerbrown.com

Innovation is a high-value topic now. In some sense, the customer in an outsourcing arrangement is always looking for innovation. In response, suppliers both innovate and adopt innovations made by other companies. Often, the "innovation" will be the ability to provide more economic, useful or resilient service than was originally promised. In exceptional cases, innovation creates opportunities to deliver entirely new insights, products or services.

Cloud computing has spawned a burst of innovation relevant to outsourcing. For example, cloud computing provides the processing power for innovations such as big data, cognitive computing, robotic process automation, the Internet of Things and "as a Service" products. Many of the innovations spawned by cloud computing can be applied to improve outsourced functions in ways that reduce cost while holding steady or even improving service performance. In addition, increasing amounts of second-stage outsourcing means that customers are seeking productivity gains beyond those that can easily be anticipated from the consolidation, sourcing or offshoring of a function.

So, the question becomes, how can customers secure the benefits of innovation?

Traditional Outsourcing Models

Traditional outsourcing pricing models do not naturally drive the benefits of innovation to customers. Where the customer pays for inputs such as FTEs or machines, the supplier has an incentive to avoid innovations that would reduce the quantity of those inputs. Where the customer pays based on the number of activities performed, the supplier captures all reductions in its cost of performance. In each case, there is a chance that the supplier could improve its profitability through innovations that reduce its cost but increase risks for customers.

In addition, the traditional outsourcing model tends to involve a promise to deliver services at standards that are being attained or are clearly attainable at the signing. Thus, the supplier has the ability to win the lion's share of the benefit of any innovation by offering improvements only at an additional charge. Some outsourcing agreements include glide paths or other automatic mechanisms, but those generally provide customers only what was foreseeable in an earlier competitive bidding process, not what is delivered in the burst of innovation that we are seeing today.

Suppliers often claim that market forces drive them to continuously innovate and improve.

However, in the traditional outsourcing model, early termination fees create barriers to switching suppliers. This reduces the incentive for a supplier to provide innovations to existing customers on the theory that doing so would cannibalize existing committed revenue (although the supplier might offer innovations to win new customers).

General Innovation Covenants

It is quite common for outsourcing arrangements to include an express commitment by the supplier to deliver innovation. Similarly, customers often have rights to "roadmap" briefings and to be offered a chance to be an early adopter of innovations. Frequently, a customer will negotiate the right to participate in development forums and the like to help influence developments by the supplier that could benefit the customer.

Whether these mechanisms ensure that the customer gets "enough" innovation or a "fair" share of any resulting innovation is something of a mystery. The supplier certainly acquires know-how from the customer (and other customers), and it develops its skills in delivering its services at the customer's expense.

Bespoke innovation reliably produces innovations that conform to agreed specifications. The challenge, however, is that the customer may share little or none of the value that the innovation brings to the supplier.

Quite often, the customer makes further, specific investment to participate in the supplier's development process. The customer's "benefit" is in getting a service that may be more specifically tailored to its developing needs. The customer may also benefit from having the supplier's investment in innovation being spread across its entire customer base. In the absence of a gain-sharing methodology, though, it is not easy to see how the customer gets a direct financial benefit from the gains the supplier makes as a result of innovation reducing the cost of delivery of services in the traditional service level and input-based changing model. These gains might well be material.

Outcome-based pricing models work by aligning the interests of the customer and the supplier. If structured well, this model can incentivize a supplier to drive gains through innovation over an extended period.

Somewhat paradoxically, customers often seek a share of gains from innovation through covenants that prohibit innovation. For example, outsourcing arrangements commonly prohibit suppliers from subcontracting work without consent. While these covenants can reduce the risk that cost-reducing innovations for the supplier will increase customer risk, they also allow the customer to negotiate for some share of the benefits of approved innovations. The roundabout nature of the protection is unlikely to provide a full or fair share of the benefits to the customer.

Bespoke Innovation

There are also difficulties in assessing whether the customer gets a fair share of the gain that the supplier derives from bespoke innovation, that is, innovation made specifically for an individual customer at that customer's cost. Bespoke innovation reliably produces innovations that conform to agreed specifications. The challenge, however, is that the customer may share little or none of the value that the innovation brings *to the supplier*. Often, the customer contributes not only funding but a great deal of market, technical and operational information.

The customer will often negotiate some form of exclusivity in bespoke innovations. While the customer still may not receive much of the benefit that the supplier receives, the exclusivity can protect

the customer from having competitors benefit from cloning the innovation in their own operations. It seems unlikely that the supplier and the customer will negotiate a deal at the time the innovation is ordered that fairly reflects the benefit each party might derive from the innovation. While this is a common problem in any innovation arrangement, the long-term relationship between the customer and the supplier does raise the question of whether there are alternative models that might reward each party more equitably for their respective investment in the innovation by referencing the benefit in fact derived from the innovation. One such alternative model is outcome-based pricing.

Traditional outsourcing models are not well-suited to delivering the benefits of innovation to customers. In this time of rapid innovation in technology that delivers outsourced services, customers who are willing to make the initial investment in structuring outcome-based pricing strategies can secure more of the benefits of an increased flow of innovations.

Outcome-based Pricing

In an outcome-based pricing model, the supplier is paid based on the benefit that the customer derives from use of the supplier's services. For example, a supplier of accounts receivable administration services might be paid based on how quickly it collects amounts due (that is, on days sales outstanding) instead of on the number of FTEs administering receivables or the number of invoices sent. A supplier of procurement services might be paid a "gain share" based on a share of savings achieved. A supplier of bespoke innovations might be paid a share of the revenues from reuse of the innovation.

Outcome-based pricing models work by aligning the interests of the customer and the supplier. The supplier gets paid by reference to gains made by the customer. If the supplier is more efficient at delivering the outsourced service, then, in theory, the customer's business would be more profitable. If structured well, this model can incentivize a supplier to drive gains through innovation over an extended period. In addition, if the incentives are well-aligned, the contract needs fewer restrictive covenants and requires less control-oriented governance.

Outcome-based pricing benefits greatly from an initial investment in deal structuring. This investment is larger than that required to merely replace one set of inputs with another set of inputs. The challenge is to define measurable outcomes that can be attributed to successful innovation. In doing so, the parties work to exclude the effects of factors outside of supplier's control. For example, a customer might use days sales outstanding *compared to an industry average* instead of the customer's historical days sales outstanding so that the supplier's compensation is based on its efforts, not changes in general economic conditions or improvement measured from an inefficient internal metric.

There are, of course, risks in outcome-based pricing. The supplier may impose unanticipated costs and risks on the customer as it pursues the selected outcomes or may be compensated for lucky results instead of genuine effort. The customer's strategies may shift, making the outcomes less valuable. The supplier's scope might need to be expanded to give the supplier adequate control over an outcome. However, balanced against a likely lack of fairness in the division of benefits from innovation in conventional input-based pricing, the risks in outcome-based pricing for elements of a deal that involve innovation commitments do not look insurmountable.

Conclusion

Traditional outsourcing models are not well-suited to delivering the benefits of innovation to customers. In this time of rapid innovation in technology that delivers outsourced services, customers who are willing to make the initial investment in structuring outcome-based pricing strategies can secure more of the benefits of an increased flow of innovations. ◆

Service Levels for SAAS

Linda L. Rhodes

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

Customers are rapidly increasing their use of software-as-a-service ("SAAS") solutions and other cloud services as part of their sourcing strategy. Cloud solutions offer the flexibility to quickly ramp services up and down, with typically little or no exit costs. However, cloud providers are able to offer flexible and cost-effective solutions because their offerings are standardized. Accordingly, customers find that providers of SAAS solutions are less likely than traditional outsource providers to negotiate services levels (as well as other contract terms) to meet the customer's particular business needs. Accordingly, customers should understand the limited negotiating flexibility with cloud providers and how to mitigate the service level limitations, where possible.

In a traditional outsourcing transaction, a customer typically has the flexibility to negotiate the service levels it needs to meet its business requirements. The customer can usually negotiate a reasonably expansive set of metrics, with desired target performance levels within a reasonable range. By contrast, cloud providers typically have a standard set of metrics and performance levels, with little negotiability. Typically, the number and type of service levels offered are quite limited. Cloud providers may offer customers the choice of platinum, gold or silver service levels, but all are based upon pre-set standards determined by the provider.

Traditional outsourcing transactions include a service level methodology pursuant to which the provider will put a certain percentage of its monthly charges at risk, typically in the range of 10 to 15 percent of the monthly charges. The customer has the right to over-allocate the at-risk amount across service levels, typically in the range of 150 to 200 percent. Such a methodology allows the customer to impose higher credits for individual service level failures.

Cloud solutions offer the flexibility to quickly ramp services up and down, with typically little or no exit costs. However, cloud providers are able to offer flexible and cost-effective solutions because their offerings are standardized.

Further, in traditional outsourcing, the customer can add and delete service levels, promote key performance indicators to critical service levels and reallocate the percentages of the at-risk amount assigned to individual service levels. Often, credits increase following a specified number of consecutive failures of the same critical service level to incentivize the provider to resolve underlying systemic issues. Credits are not the sole and exclusive

remedy, thus allowing the customer to seek damages and terminate for material service level failures. These tools allow the customer to focus the provider's attention on those service levels most important to the customer and incentivize suppliers to quickly resolve performance deficiencies.

By contrast, these tools are typically unavailable to customers in cloud transactions. Cloud providers give nominal credits for service level failures. The customer has no flexibility to add, delete or promote service levels or reallocate credits. Providers will push hard to make service level credits the exclusive remedy. In addition, service levels are often set forth in service offerings that are incorporated by reference into the services agreement. Providers reserve the right to change the terms of their service offerings from time to time without the customer's consent.

In traditional sourcing transactions, service levels set forth clear guidelines as to when a provider is or is not in compliance with its service obligations. Nevertheless, because service levels cannot possibly cover every aspect of a provider's performance, the outsourcing agreement will contain additional representations and warranties as to the quality and performance of the services. In public cloud agreements, services are often described at a high level with little detail. Providers are reluctant to give general performance warranties, which limit the customer's ability to bring claims for damages for deficient services.

What is a customer to do? First, be thoughtful in selecting what services you put on the cloud. Understand your business's needs and the provider's ability to meet those needs through its cloud offering. A customer can often protect itself against deficient performance through its right to terminate the services with little to no exit costs. However, whether or not a termination right is an effective remedy for deficient performance depends in large part on how critical the services are to the customer's business and how disruptive a change in providers will be.

Further, the lack of flexibility in cloud contract terms and conditions does not mean a client should not push for the tools available in traditional outsourcing transactions. Cloud providers have different levels of flexibility, depending upon the size and negotiating leverage of the provider. The customer should continue to push for the agreement to provide, among other things, that service level credits are not the sole and exclusive remedy for service level failures.

Cloud providers may offer customers the choice of platinum, gold or silver service levels, but all are based upon pre-set standards determined by the provider.

Include warranties about general performance standards in the services agreement, at least with respect to core features and functionality. Then, if the provider's services are deficient, the customer can use those warranties to hold the provider accountable for breach of contract in cases where there is no service level to cover the deficient performance. Unilateral changes to service offerings by providers should not have a materially adverse impact on customers. Even if service level credits are the sole and exclusive remedy, it is important to make clear that such credits will not affect any right of the customer to claim damages arising from the provider's failure to meet its other obligations under the agreement.

You can successfully use cloud solutions if you make informed decisions about the services you decide to place on the cloud and the cloud solution selected and if you seek to minimize the limitations of cloud contract terms to the extent possible. ◆

Alternatives for Monetizing Trade Payables (or Receivables)

Massimo Capretta

Massimo Capretta
Chicago
+1 312 701 8152
mcapretta@mayerbrown.com

This article was published previously in *Treasury & Risk Magazine*.

Here's how to distinguish between the three primary approaches to supply chain finance—and when to leverage each one.

As anyone who regularly deals with supply chain issues knows, buyers and suppliers of goods and services usually have conflicting interests. Supply chain managers at most companies are under pressure to improve the company's cash efficiency, usually by extending payment terms to their suppliers. But many suppliers lack the financial strength or flexibility to adjust to longer payment terms. For example, if a supplier already has a highly leveraged balance sheet, increasing bank borrowing to finance short-term working capital may be prohibitively expensive. Extended payment terms may also expose suppliers to increased commodity or foreign exchange risk.

When a large, well-capitalized company is buying goods or services from a small or highly leveraged supplier, it may be in a position to use its own balance sheet to support the supplier. A number of strategies have emerged in recent years to help buyers and suppliers leverage the buyer's stronger financial position to help the supplier access lower-cost liquidity, often so that the supplier can then offer the buyer extended payment terms. Most of these strategies involve monetization of the supplier's trade accounts receivable.

A negotiable-instrument–based program is similar in many respects to an open-account program. However, the supplier or buyer also creates a "draft," a "bill of exchange," a "negotiable promissory note," or another form of negotiable instrument.

The most common forms of trade receivables monetization include open-account–based supply chain finance and negotiable-instrument–based supply chain finance. Together, these two strategies are often referred to as "structured vendor-payables finance" or "reverse factoring." A third, related strategy is non-recourse receivables purchase, which is often incorrectly referred to as "factoring."

How Open-Account Supply Chain Finance Works

An open-account structured vendor-payables program involves the sale of receivables owned by various suppliers and owed by one particular buyer. The suppliers sign up to negotiate and sell their receivables

to investors via a bank or another company running an Internet-based platform. To maximize economies of scale, a buyer usually wants to have a number of suppliers taking part in its open-account program.

A number of strategies have emerged in recent years to help buyers and suppliers leverage the buyer's stronger financial position to help the supplier access lower-cost liquidity, often so that the supplier can then offer the buyer extended payment terms. Most of these strategies involve monetization of the supplier's trade accounts receivable.

Depending on the size of the supplier base, the investors purchasing the receivables generally consist of a single bank or a small group of banks, although receivables are sometimes sold on a blind trading platform, in which case they may be purchased by any number of investors. The universe of possible investors is usually made up of the relationship banks of the buyer, but this is not always the case. In recent years, a number of alternative investors such as hedge funds and insurance companies have also appeared in the market.

The platforms on which receivables are submitted, approved, and sold tend to be similar across most open-account structured vendor-payables programs. A supplier will sell goods or services to the buyer, generating an invoice that it posts on the supply chain finance platform for the buyer's confirmation. Once the buyer confirms the invoice as valid, the related receivable becomes eligible for purchase by an investor. Only confirmed invoices are eligible for purchase, so a specific transaction can be sold only if both the supplier and the buyer agree to have it sold.

In confirming the invoice, the original transaction's buyer agrees that it will pay the investor the full amount of the invoice on its due date without any claim, abatement, deduction, reduction, or offset of any kind. This confirmation enables the investor to look directly to the buyer for payment. The buyer may still request deductions and make similar claims against the supplier, with those offsets potentially applying to future invoices, but the buyer will not be permitted to challenge the amount owed on the receivable sold to the investor.

The investor's agreement with the supplier sets out a formula for determining the purchase price on all offered invoices. Typically the price is equal to the face value of the invoice minus a discount calculated based on the credit profile of the buyer—not the supplier—as well as the number of days to maturity of the receivable. If the supplier and investor elect to consummate the sale of a particular invoice, then the receivable represented by the invoice is sold on a non-recourse basis to the investor in a legal "true sale." By utilizing a true sale, the investor can generally focus its underwriting on the underlying credit profile of the buyer and ignore the credit of the supplier.

When the sale of a receivable closes, the buyer will be notified. Then on the scheduled maturity date of the invoice, the buyer will owe the investor the full face amount of the invoice. The difference between the buyer's payment to the investor and the investor's discounted payment to the supplier constitutes the investor's fee for participating in the transaction. This is often the only fee that the investor charges; the buyer usually pays no fee on this type of transaction. Also, if the investor is the buyer's cash management bank, the buyer may not have to modify its cash disbursement operations to pay the investor rather than the supplier. In many cases, the investor simply debits a pre-agreed bank account for the amount of each sold receivable on the invoice maturity date.

An open-account structured vendor-payables program involves the sale of receivables owned by various suppliers and owed by one particular buyer.

Using Negotiable Instruments Instead of Receivables

An open-account vendor-payables program is not the ideal supply chain finance solution for every buyer. Open-account programs rely on the sale of accounts receivable under Article 9 of the Uniform Commercial Code (UCC). The UCC provides an easy and predictable way to finance or sell intangible assets like receivables in the United States. However, in some non-U.S. jurisdictions, selling intangibles can be cumbersome and may expose the investor to additional legal risks, such as risks associated with fraud and insolvency.

Even in the United States, an investor purchasing a receivable needs to record that purchase under the UCC filing system in one or more states. Depending on the supplier's existing credit arrangements, the investor may also need to obtain lien releases from the supplier's lenders before the receivable can be sold.

To bypass these challenges, buyers sometimes opt to implement an alternative structure that utilizes negotiable instruments instead of accounts receivable. A negotiable-instrument–based program is similar in many respects to an open-account program. The supplier submits invoices, which the buyer approves. However, the supplier or buyer also creates a "draft," a "bill of exchange," a "negotiable promissory note," or another form of negotiable instrument. These instruments are governed by U.S. law.

Once created, the instrument is then sold by the supplier to an investor using a process similar to that of open-account receivables sales, but it usually involves a physical embodiment of the negotiable instrument. The investor takes physical possession of the instrument upon purchase, then presents the instrument to the buyer for payment on the invoice maturity date. In some cases, the creation, acceptance, assignment, and presentment of the instrument are handled entirely by the investor, with no need for the supplier and buyer to exchange a physical document.

Because these instruments are governed by U.S. law and owed by a U.S. buyer, they are free of most foreign-law constraints, even if the supplier is a non-U.S. company. Thus, negotiable instruments allow an investor working with a U.S.-based buyer to purchase receivables from a wider universe of suppliers than it could under an open-account program.

The other key advantage of an instrument-based program is what's known as the "holder in due course" doctrine. Section 3-302 of the UCC defines a "holder in due course" as one who takes an instrument for value in good faith, absent any notice that it is overdue, has been dishonored, or is subject to any defense against it or claim to it by any other person. If the purchaser of a negotiable instrument is a holder in due course, the purchaser may not be subject to many of the defenses available to creditors under Article 9 of the UCC. This means that, unlike with open-account programs, invoices sold as negotiable instruments will give the investor priority against claims of the supplier's other creditors, including in a bankruptcy proceeding. Investors should take note, however, that while these programs are built on solid legal foundations, there is little or no case law on the issue of whether an investor in this type of supply chain program would qualify as a holder in due course. In addition, investors often do not need to deal with the UCC recording system when purchasing negotiable instruments.

On the other hand, this type of program is more cumbersome than an open-account program and may be unfamiliar to many U.S. suppliers.

Key Considerations in Structured Vendor-Payables Programs

Buyers considering implementing a structured vendor-payables program will want to consider a few key issues. The first, and perhaps the most obvious, is that these programs require close coordination among the buyer's treasury, legal, and purchasing functions.

The initial negotiation with prospective investors is usually led by a company's treasury and legal teams, but the purchasing function is generally responsible for on-boarding suppliers and maintaining the program. A lack of coordination among these departments can easily lead to implementation of a suboptimal program and underutilization of the program by the company's suppliers.

The second key issue concerns the accounting treatment of a structured vendor-payables program. For the buyer, the chief accounting priority is usually to avoid having to reclassify the affected payables as short-term indebtedness on its balance sheet. Such reclassification is usually unfavorable because it increases the company's balance sheet leverage, which may affect financial covenants and ratios contained in loan agreements, indentures, and employee compensation agreements, among other contracts.

These programs require close coordination among the buyer's treasury, legal, and purchasing functions. A lack of coordination among these departments can easily lead to implementation of a suboptimal program and underutilization of the program by the company's suppliers.

Unfortunately, no specific U.S. GAAP guidance addresses the accounting for structured vendor-payables arrangements. In 2003 and 2004, Securities and Exchange Commission (SEC) staff made conference presentations outlining general guidance for companies that report to the SEC1. They noted that in specific situations, certain characteristics of structured vendor-payables arrangements may cause supplier payables to be reclassified on the balance sheet of the buyer as short-term indebtedness. Lacking specific GAAP guidance, most auditors use these comments as a guide in making determinations regarding balance sheet treatment.

Auditors are more likely to require indebtedness treatment when a structured vendor-payables arrangement has any of the following characteristics:

- The economic terms and character of the obligations owed to the investor are different from the obligations the buyer previously owed to the supplier.
- The buyer agrees to cover the supplier's financing costs or other obligations to the investor.
- Supplier participation in the program is mandatory.
- The buyer has excessive control in the negotiation of documentation between the supplier and the investor.

Most legal documentation used by sophisticated investors in structured vendor-payables programs is designed to address these concerns. However, buyers should be sure to discuss the implementation of any supply chain finance solution with their internal and external auditors well before they start rolling out a program.

1. *SEC Staff Speeches: 2003 and 2004 AICPA National Conference on Current SEC and PCAOB Developments. Robert Comerford: "Classification and disclosure of certain trade accounts payable transactions involving an intermediary."*

An Alternative: Non-Recourse Receivables Purchase

A close relative of structured vendor-payables programs is a non-recourse receivables-purchase solution. This is often described as a "factoring" arrangement, but that's a misleading designation because these facilities have little in common with the small-scale financing mechanism traditionally provided by factoring companies in the United States.

Much like an open-account payables transaction, a receivables-purchase facility entails a supplier selling one or more investors its rights to certain accounts receivable owed by a particular buyer. A big difference

is that the buyer's involvement is minimal beyond introducing the investor to its supplier base. The buyer does not have to confirm each invoice before the receivable can be sold. In fact, an investor might provide these types of facilities to suppliers without the buyer even knowing about it. Another benefit for the buyer is that a receivables-purchase facility generally does not have any accounting complications for the buyer.

A close relative of structured vendor-payables programs is a non-recourse receivables-purchase solution. This is often described as a "factoring" arrangement.

For suppliers, these facilities can provide much higher advance rates and lower overall costs compared with more traditional asset-based loan facilities. They can also assist suppliers in monetizing excess customer concentrations that would be excluded by the borrowing-base funding formulas found in most asset-based loan (ABL) agreements or accounts receivable securitizations. Traditional ABL and securitization facilities will often contain strict concentration limits on the percentage of receivables of a particular obligor which may be used to generate funding availability. These limits can often be as low as a few percentage points. For many suppliers to industries with a small number of dominant buyers (e.g., retail, auto) these limitations can result in the supplier being unable to monetize a large percentage of its outstanding receivables.

Finally, unlike a structured vendor-payables program, which will usually require a great deal of work at the buyer to implement and roll out among its supplier base, these types of transactions can be executed quickly and sometimes even on a one-off basis.

The downside of these facilities for the investor is that there is no direct confirmation from the buyer that it will pay the investor. Thus, investors in these facilities are very keen to make sure that what they are acquiring from the supplier is a valid and enforceable claim against the buyer. The investor usually conducts significantly more due diligence on suppliers before entering these transactions, and it pays close attention to making sure that the supplier is transferring the receivables via a legal true sale.

The Future of Trade Receivables Monetization

All three of these types of arrangements help suppliers access improved liquidity, whether or not their buyer is looking for extended payment terms. Most of these strategies can be implemented with few, if any, direct expenses to the buyer.

Trade receivables monetization is particularly popular in the consumer retail, automotive and other manufacturing, chemical, and pharmaceutical sectors. Buyers in these industries tend to have extensive supply chains that are global in scope, and generally the buyers are larger, with a more favorable credit profile, than most of their suppliers. However, the benefits of monetizing trade receivables aren't limited to a few business sectors. These strategies may be utilized by any buyer with a solid credit rating and a diverse supplier base, or by any supplier whose buyers have high credit quality.

A lot is happening in supply chain finance, and it seems likely that the recent growth in popularity of these programs will continue well into the future. Based on our own pipeline of projects at Mayer Brown, we expect to be talking about structured trade receivables solutions for a long time. Stay tuned. ◆

The General Data Protection Regulation: The Status of the Negotiations to Implement a New Data Protection Law throughout Europe

Oliver Yaros

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

Significant progress has been made to finalize the European Commission's 2012 proposal to completely reform the European Union's data protection laws—the new General Data Protection Regulation (GDPR or Regulation). The current EU data protection regime, the EU Data Protection Directive 95/46, is widely considered to be inadequate in light of advances in technology that rely on the use of personal data such as big data analytics. Reform is needed to "future-proof" data protection law while simultaneously protecting the rights of individuals and allowing businesses to utilise personal data.

The proposal is also an opportunity to harmonise data protection law across the European Union. As the current EU data protection regime was drafted as a Directive, each Member State enacted the rules in its own way; the end result being a patchwork of data protection regimes throughout Europe that sometimes conflict with each other. The GDPR will be directly applicable in the same form in all Member States and will, hopefully, reduce the need for specific local advice in each Member State.

In March 2014, the European Parliament published its proposed text of the Regulation following extensive amendments to the Commission's original draft. The European Council of Ministers then published its full draft of the Regulation on June 15, 2015, having debated the Parliament's draft in a piecemeal fashion since March 2014. While agreeing on some key data protection proposals, the Parliament and the Council are in disagreement over others. The Parliament's prescriptive approach reflects the concern over data protection raised by the Snowden revelations during the Parliament's review. The Council, composed of government representatives for each Member State, has adopted a more "risk based" approach, which allows organisations to judge the impact of their data processing activities for themselves. The EU institutions are continuing negotiations to decide upon a final draft which is hoped to be approved by the end of this year.

Significant progress has been made to finalize the European Commission's 2012 proposal to completely reform the European Union's data protection laws—the new General Data Protection Regulation (GDPR or Regulation).

This article highlights a number of key changes proposed by the various drafts of the Regulation, both those changes where the Council and the Parliament have adopted a similar approach and those where there is a high degree of discrepancy between the EU institutions, all of which will affect organisations which process personal data.

The Regulation introduces the concept of "privacy by design," whereby appropriate levels of security are built into an organisation's data processing procedure.

Privacy by Design

The Regulation introduces the concept of "privacy by design," whereby appropriate levels of security are built into an organisation's data processing procedure. Data controllers are required to take a proactive approach, ensuring that an appropriate standard of data protection is the default position for all data controllers to take.

The Parliament's draft details the obligations of organisations here to a greater extent than the Commission's draft, for example, by requiring controllers to take account of the state of current technical knowledge and international best practice when implementing technical and organisational measures. The Parliament text extends the obligation to data processors. The Council's draft is closer to the Commission's approach, which allows the controller to take account of the cost of implementing the required measures. The Council's draft requires controllers to consider the risks posed to individuals by the processing instead of setting precise benchmarks for compliance, and makes suggestions about how to minimise risk, for example by encrypting personal data or using pseudonymisation.

The current The current Directive has no equivalent concept of privacy by design, so a legal requirement for organisations to change their overall approach to data processing would be a fundamental adjustment for controllers.

Governance

Under the GDPR, data controllers could be required to appoint a Data Protection Officer (DPO) to carry out relevant assessments of an organisation's data processing, although this proposal has been the topic of much debate among the EU institutions. The drafts proposed by both the Commission and the Parliament would obligate data controllers to designate a DPO when their processing reaches certain thresholds. However, the appointment of a DPO is not mandatory under the Council's draft (unless otherwise required by national law).

The Regulation introduces an express obligation for controllers to notify breaches of security relating to personal data to the relevant data authority where the breach is likely to cause a degree of risk to the data subject.

Data controllers will be required to undertake impact assessments for higher-risk processing. These assessments would generally include an evaluation of the risk posed to the data subject as well as the measures envisaged to address the risk. The Council's draft suggests that only "high-risk" situations would necessitate a mandatory impact assessment, whereas a "specific risk" would trigger an assessment in the Parliament's text. The Parliament also suggests carrying out general impact assessments in relation to the processing of data protection once every two years.

It remains to be seen whether organisations will be able to carry out these relevant assessments without the designation of a DPO, whether such appointment is mandatory or not.

Processor Liability

Processors will have direct obligations to comply with the GDPR under certain circumstances. They also will be liable to sanctions for breaching the GDPR, whereas under current legislation (at least in the UK), all responsibility to comply with the law falls on the data controller. The exact obligations are yet to be agreed upon by the Parliament and the Council, but it is clear that processors will be held accountable for their own level of appropriate security and must document their processing to the same extent required by controllers under the new Regulation. Processors must obtain the prior consent of the controller to employ sub-processors, while controllers must only use processors which provide sufficient guarantees to implement appropriate measures to meet the requirements of the Regulation.

Contracts with third parties will need to be amended to address the shift in responsibilities for processors.

Notification Obligations

The Regulation introduces an express obligation for controllers to notify breaches of security relating to personal data to the relevant data authority where the breach is likely to cause a degree of risk to the data subject. The Council's and the Parliament's drafts require a detailed notification to be made to the data authority promptly. Data controllers must notify the authority within 72 hours of the breach and processors must notify the relevant data controller of the same without undue delay. Controllers must also communicate the fact that there has been a personal data breach to the data subject promptly where there is a high risk to the individual's rights and freedoms.

Policies of controllers and processors that relate to responding to security breaches will need to be amended and tested ahead of the implementation of the Regulation.

The Data Subject's Rights

Individuals will have the right to have their personal data removed from a controller or processor's system or online content (the "right to be forgotten"). The Council has clarified that this right is not absolute and will always be subject to the legitimate interests of the public. Controllers will need to judge whether freedom of expression and information prevails over the protection of personal data.

Data subjects' right to data portability (the right have a person's data transferred to another service provider) has been endorsed by the Council. However, the Council has restricted the application of this right to personal data provided by the individual.

Processors will have direct obligations to comply with the GDPR under certain circumstances. They also will be liable to sanctions for breaching the GDPR, whereas under current legislation (at least in the UK), all responsibility to comply with the law falls on the data controller.

Individuals will also have the right not to be subject to automated data profiling (where this would produce a "legal effect"). The Council's draft allows profiling in specific circumstances (such as tax evasion monitoring) and where data subjects have provided explicit consent. The practical difficulties of obtaining this consent to carry out "big data" analytics projects may be difficult to achieve and profiling may be hard to justify under alternative grounds.

International Application of the Regulation

The Council has retained the extended territorial scope of the GDPR, with the legislation applying depending on the type of data processing being undertaken, not where that processing is being

carried out. Data controllers located outside the European Union that process personal data in relation to offering goods or services to individuals within the European Union, or as a result of monitoring individuals within the European Union, will be subject to the Regulation. Non-EU organisations will need to consider whether their activities are caught by the Regulation and whether they must appoint a European representative to take responsibility for their actions.

Individuals will have the right to have their personal data removed from a controller or processor's system or online content (the "right to be forgotten").

Harmonisation

The Commission and the Parliament originally envisaged that the GDPR would ensure that one data protection law would be applicable to all EU Member States under the banner of "One Continent, One Law." However, the Council's draft provides more than 40 exceptions to the application of the GDPR, which are dependent upon additional factors—largely the national laws of the Member States. If these exceptions survive to the final draft, there will continue to be a discrepancy in the national data protection laws throughout the European Union and local advice on data protection laws will still be required on a number of issues.

Furthermore, the Commission's proposal for any national data protection authority to act as a "one-stop-shop" for an organisation's compliance with data protection law throughout Europe has been significantly diluted. The Council's draft still requires organisations to liaise with the supervisory authorities from different Member States where there is an international data protection issue as opposed to dealing with just one authority as proposed by the Commission and the Parliament. If this position remains, the GDPR will be seen as a missed opportunity to harmonise European data protection laws.

Sanctions

The GDPR will see fines imposed on organisations that breach EU data protection law rise well above the current maximum fine that could be imposed by the Information Commissioner Office in the United Kingdom (currently £500,000), for example. The Council's draft supports the Commission's proposal to limit maximum fines for a breach of the GDPR to 2 percent of an enterprise's worldwide turnover, or €1 million, whichever is higher. These levels are significantly lower than the Parliament's suggested maximum fines of up to €100 million or 5 percent of the entity's turnover.

What Next?

The three institutions have now entered a closed door series of negotiations to agree to the final text. Given the informal nature of these negotiations, there is no clear deadline for the parties to come to a consensus on the final version of the GDPR. Tough negotiations will be required to bridge the disparities between the Parliament and the Council, so a final draft is unlikely to be concluded before the end of this year.

Once the legislation is finalised, there is likely to be a two-year transition period to adhere to the new rules. Therefore, the GDPR could be in force throughout the European Union by the end of 2017. Organisations (both inside and outside Europe) should examine the new rules very carefully to identify the changes that they need to make to ensure that they are compliant with the GDPR before it comes into force, particularly in light of the enhanced sanctions. ◆

The Internet of Things: Promises and Perils for Traditional Product Makers

Paul J. N. Roy
Julian Dibbell

Paul J. N. Roy
Chicago
+1 312 701 7370
proy@mayerbrown.com

Julian M. Dibbell
Chicago
+1 312 701 8237
jdibbell@mayerbrown.com

According to some reports, the Internet of Things originated in 1982, when computer scientists at Carnegie Mellon University added sensors to a campus Coke machine and connected it to the local network so they could check how many Cokes were left without leaving their workstations. Primitive though it was, that experiment offered a glimpse of the efficiencies that a world of similarly connected devices—an Internet of Things (IoT)—might someday bring. Today, the world's economies are brimming with Internet-connected devices, some 5 to 10 billion of them, growing toward a predicted total of 40 billion by the year 2020. At scales like these, the promise of IoT comes into sharp focus: Combining massive connectivity with the big data that flows from it, those billions of connected devices are sending constant updates on their use, and their users, back to businesses for analysis, with the potential for vast savings and profits to result.

The FTC outlined three main categories of measures that businesses should take to protect against privacy and security risks in connected devices: (i) security by design, (ii) data minimization and (iii) notice and consent.

In short, the Internet of Things is not just for computer scientists anymore. Nor, for that matter, is it just for technology companies. If anything, the IoT holds its greatest promise for businesses selling the kinds of relatively low-tech products—automobiles, manufacturing tools, home appliances, hospitality services—that are most likely to be transformed by an injection of smart, connected technology. But if the Internet of Things is a particularly compelling proposition for these types of businesses, it also exposes them to a peculiar set of risks.

Generally speaking, the perils of Internet of Things technology stem from the same core issues that create its promise: connectivity and data. Connected devices can be remotely hacked and turned against their legitimate users. Additionally, the massive collection of data invites misuse of that data, both by hackers and by the businesses that collect it. While these threats face any business that chooses to adopt IoT technology, the makers of traditional, mass-produced goods are in some ways particularly vulnerable to them. For one thing, such businesses are typically larger and more established than tech companies, with high

profiles and broad consumer bases that make them especially attractive targets for hackers. At the same time, however, they typically lack the tech companies' native capacity to assess and defend against cybersecurity and data risks and lack experience dealing directly with consumers who normally purchase their products through third parties. Borrowing some of that expertise, whether by partnering with or hiring technology vendors, will often make sense for a conventional product maker venturing into IoT. But doing that in turn creates the potential for complications—cultural frictions, misallocated risks—that comes with any such relationship.

None of which is to say that conventional product makers should resist exploring the Internet of Things. But to make the most of its promise, they should take care to understand its perils—and how best to guard against them.

Knowing the Risks

Connecting products to the Internet of Things creates an array of legal risks, including enforcement actions by regulators like the Federal Trade Commission (FTC), lawsuits by other businesses and class actions by consumers. As varied as these risks may be, however, they all essentially revolve around the two core issues of connectivity and data.

CONNECTIVITY RISKS

The chief risk created by connecting a product to the Internet is that a third party—neither the authorized user of the device nor the business that produced and still communicates with the device—will use that connection to gain unauthorized access to the device.

The consequences of such an attack can be drastic. The intruder may gain not just access but control of the product, in which case the potential damage to life and property may be limited only by the nature of the product. Among threats to consumers, vulnerabilities in connected automobiles have lately made dramatic headlines, focusing on the ability of hackers to remotely cut the brakes or the power on some late-model cars. But there is evidence to suggest that the threats to business and manufacturing (where more than 40 percent of connected devices are deployed) are at least as formidable. Famously, for example, the first cyberattack to physically damage a connected device was the Israeli government's alleged deployment of the so-called Stuxnet computer worm to incapacitate an Iranian nuclear reactor. And last year, hackers managed to gain control of a German steel plant's blast furnace, doing serious damage to it in the process.

Generally speaking, the perils of Internet of Things technology stem from the same core issues that create its promise: connectivity and data. Connected devices can be remotely hacked and turned against their legitimate users.

Moreover, physical damage is not the only kind of damage a cyberattack on a connected device can inflict. Sensitive personal data can be stolen directly from connected devices used by consumers. Trade secrets and other sensitive commercial data can be lifted from devices used by businesses.

Nor does the damage have to be done by third parties, or even with intent to do harm. Manufactured products have always been subject to dangerous malfunctions. In connected devices, the complexity of embedded software creates an added layer of susceptibility to malfunction. The fact that such software can be updated remotely creates further opportunities for things to go unintentionally wrong.

DATA RISKS

Seeking to maximize the value of the personal or commercial data collected from connected devices, businesses may collect kinds or amounts of data that the data subjects did not consent to share, or did not expect to share given the vagueness or generality of the language they did consent to. Businesses may also put the collected data to uses the data subjects do not

believe they agreed to. Overstepping the bounds of consent in any of these ways can give rise to privacy violations (for personal data) or to breaches of trade secrecy or confidentiality (for commercial data).

Conversely, if data collected by a business shows ways to improve the safety or reliability of the product, and the business fails to perceive or to act on that evidence, that failure could be held against it in a later product liability suit.

Mitigating the Risks

In a recent report on the Internet of Things, the FTC outlined three main categories of measures that businesses should take to protect against privacy and security risks in connected devices: (i) security by design, (ii) data minimization and (iii) notice and consent. Taking effective measures across all three categories should weigh in a business's favor in any enforcement action by the FTC. It may also cut short any private claims brought for breaches of privacy or security.

SECURITY BY DESIGN

Businesses should ensure that security measures are built into the device from the outset, and that any outside vendors hired for the purpose can and do build them in.

> The chief risk created by connecting a product to the Internet is that a third party—neither the authorized user of the device nor the business that produced and still communicates with the device—will use that connection to gain unauthorized access to the device.

As part of such built-in security measures, businesses should also ensure that the device's software can be remotely updated for security purposes, and should secure any end-user consents required to do that lawfully throughout the life cycle of the device. That said, however, businesses should recognize the unique challenges involved in implementing remote updates of connected devices. Compared to more conventional computing devices, such as desktop and laptop computers or smartphones, IoT devices may be connected to the Internet sporadically. For connected devices that are particularly durable goods—tractors with product lives of 20 years, for example—the software or associated hardware embedded in the device may eventually become so obsolete that it cannot be updated at all. (Similarly, any outside vendor hired to manage the device's security may become unavailable before the device goes out of service.)

For these reasons, businesses should not rely entirely on the ability to update devices. Rather they should ensure that a device's on-board security is as robust as it can be before shipping, and anticipate the need to offer component retrofits to enable continued updates.

DATA MINIMIZATION

In collecting data through connected devices, businesses should collect and retain only as much of it as the business has an immediate use for. Minimizing the amount of data retained will minimize any risks associated with data retention, including data theft, misuse of data, and failure to act on data.

NOTICE AND CONSENT

Businesses should ensure that a connected device's end users have adequate notice of the uses their data will be put to and that they consent to that use.

This may be easier to do where the end users are other businesses rather than consumers. For one thing, consumers will be more likely to look for any relevant notice on the device itself, which, for devices without conventional interfaces, may not be an opportune place for it. Businesses, on the other hand, will tend to be more attentive to and sophisticated about any terms of use presented. Moreover, to the extent that the terms appear to claim rights not normally retained by the manufacturer of a conventional consumer product, such notice may create reputational costs for the business. Thus, for consumer-facing products, businesses should rely more on data minimization than on notice to offset the risk of exceeding the data subject's consent. ◆

Volume Up, Value Down: A Growing Trend in Sourcing

Peter Dickinson
Megan Paul

Peter Dickinson
London
+44 20 3130 3747
pdickinson@mayerbrown.com

Megan Paul
London
+44 20 3130 3325
mpaul@mayerbrown.com

The second quarter of 2015 saw a record high in the number of sourcing deals, globally. But, while volumes are increasing and the market appears to be growing, the annual contract value and duration of these transactions continues to decline.

Recently released data from ISG, a global technology insights, market intelligence and advisory services company, showed a record high of 451 outsourcing contracts signed in Q2, and a total of 754 agreements in the first half of 2015. However, the ISG Outsourcing Index, which provides a quarterly review of sourcing industry data, also showed that during Q1 of 2015 the annual contract value was down 14 percent from the previous year.

Why are we seeing this increase in deal activity but a decrease in contract value? Is it solely the move toward automation and greater digitization causing a decrease in price? Or are there other factors to consider? Does this trend have the capacity to fundamentally change the way customers contract for third-party services and if so, what can customers expect?

Migration from Traditional Sourcing

While a greater number of smaller deals in the marketplace is not a new trend for 2015, we also have seen greater migration away from the traditional, tower-centric solutions and dedicated data centers. Instead, more customers are opting for application-centric solutions and shared data centers where specialized services are provided by smaller, niche providers. This migration has meant a definite shift away from sole-source environments where large, global suppliers have a function-wide scope, providing the end-to-end environment including management and maintenance of assets. Instead, customers are now separating asset purchases from services and choosing suppliers by service scope rather than by function, leading to a multi-sourced environment within a given function.

The "as-a-service" approach to service delivery is facilitating the movement from traditional methods of service delivery with specialist providers capable of offering XaaS (everything as a service). Traditional hardware and

software offerings no longer allow enterprises sufficient flexibility to evolve and keep pace with technological advancement, data analytics and data storage and intelligent cost control.

New Technologies

Perhaps most relevant in the IT and BPO markets, customers are seeking opportunities to capitalize on technological advancement. Smaller suppliers, with distinct capabilities in disruptive technologies, are ready with specialized expertise to make that expectation a reality. The pace of change is increasing, and customers need to recognize the importance of rationalizing their sourcing portfolios to take advantage of greater automation and digitization.

While a greater number of smaller deals in the marketplace is not a new trend for 2015, we also have seen greater migration away from the traditional, tower-centric solutions and dedicated data centers.

Realizing this need will be a key component to a customer's sourcing strategy. It will give customers the opportunity to assess their current sourcing environment and the scope of their existing agreements and to understand where technology can streamline processes. This will facilitate process efficiencies and cost reduction.

But What Does This Mean for the Marketplace?

Customers expect suppliers to know how to take advantage of the technological advancements to streamline and refine processes and significantly drive down pricing. As a result, a more competitive marketplace with greater importance on technology and intelligent cost control is emerging. Suppliers are being forced to adapt, and differentiation is key—in respect of both pricing and service offering. However, it's not all bad news for suppliers. As a result of the move away from the traditional service delivery model, there is likely to be greater opportunity in the marketplace for the small to medium suppliers, providing they have a unique skill set to offer.

Suppliers may also benefit from the impact this trend is having on the contracting process. In the absence of a very sophisticated customer, we are likely to see an increase in transactions done on supplier terms and conditions with limited bespoke tailoring as a more standardized approach to contracting is adopted; reflective perhaps of a more standardized as-a-service solution.

This increase in the number of lower-value deals is likely to impact how customers view the contracting process as well as the cost and time dedicated to each transaction. Supplier selection may become more of a challenge when contracting on supplier terms as comparisons may be more opaque. A more streamlined approach to tendering will surely need to be adopted to allow a true like-for-like comparison before an intelligent supplier selection can be made. Comprehensive RFPs are likely to become less common as the demand increases for a more agile, immediate form of pre-contracting to keep pace with emerging technologies and changing business requirements.

As a result, the contracting process is likely to become more streamlined with a greater appetite for automated documentation and a "light touch" approach to legal input where services are standardized and contracts are lower in value. However, legal counsel should be mindful of the operational and legal risks associated with these complex relationships and recognize that contracts with a lower value (usually because of a more niche scope) are neither low risk nor of low strategic

importance to the business or IT infrastructure. Costs associated with the contracting process should be kept under control, but they should not be a main consideration during supplier selection when outsourcing critical services or when reviewing the risks associated with contracting on supplier terms and conditions.

The "as-a-service" approach to service delivery is facilitating the movement from traditional methods of service delivery with specialist providers capable of offering XaaS (everything as a service).

Governance Will Be Key

Service integration and higher levels of governance will become ever more important as the multi-source model becomes more prevalent and the complexity of the relationship between multiple suppliers and retained organizations and functions increase. A multi-source environment with increased IT interfaces, competitive forces and a complexity of roles and responsibilities sounds like a governance disaster waiting to happen. However, complexity associated with multi-sourcing is mitigated and, in fact, capitalized upon by suppliers broadening their service management capabilities to promote governance as a core competency.

However, not all the teams play nicely together and it will be those suppliers that recognize the benefit of providing a specialist service integration offering that will ultimately succeed in this evolving marketplace.

Where such management capability is not offered as a service by a supplier, a customer will have to decide whether it is capable (both operationally and financially) of providing this important governance function itself. In the instances where it is not, there is likely to be an increased opportunity for a new category of IT services professional: the service broker. The service broker might design, source and provide a complete managed service with centralized governance and a heavy emphasis on data analytics to effectively manage a multi-sourced environment as a stand-alone specialist service offering. These contracts can raise their own unique challenges and the complexity of the sourcing relationship will increase for the customer organization. However, contracts with a service integration specialist should provide the customer opportunity to transfer much of these challenges and associated risk to the service integration specialist.

Legal counsel should be mindful of the operational and legal risks associated with these complex relationships and recognize that contracts with a lower value (usually because of a more niche scope) are neither low risk nor of low strategic importance to the business or IT infrastructure.

Conclusion

Regardless of the size or value of the contracts in place, it is critical that customers properly consider the contractual and operational risks associated with a multi-sourced environment. Even with increase in lower value contracts, they must implement a robust governance model to address the growing complexity of their third-party relationships. ◆

MASSIMO CAPRETTA
Counsel

Massimo Capretta is counsel in Mayer Brown's Chicago office and a member of the Banking & Finance practice. Massimo's transactional practice focuses on representing both financial institutions and companies across a broad spectrum of domestic and international financing transactions. Massimo has particular experience with domestic and cross-border trade receivables securitization, asset-based finance, factoring, supply chain/vendor finance, trade finance and other receivables monetization strategies. He regularly advises clients on the creation and management of bespoke receivables finance transactions. Massimo has been a speaker and panelist on a number of presentations to industry participants on topics including receivables finance, asset-based lending and cross-border finance.

JULIAN M. DIBBELL
Associate

Julian Dibbell is an associate in Mayer Brown's Chicago office and a member of the Business & Technology Sourcing practice. Before joining Mayer Brown in 2014, Julian worked as a journalist and author covering the Internet and other digital technologies. Julian received his JD degree in 2014 from the University of Chicago Law School, where he was a staff member of the University of Chicago Law Review and co-founder of the Law and Technology Society.

PETER DICKINSON
Partner

Peter Dickinson is the Co-head of Mayer Brown's Global Business Technology and Sourcing practice. Peter's practice focuses on mergers and acquisitions, joint ventures and other significant commercial transactions including, in particular, large scale multi-jurisdictional outsourcing projects.

MEGAN PAUL
Senior Associate

Megan Paul is a senior associate in the Corporate & Securities practice of the London office. She undertakes a broad spectrum of transactional corporate and commercial work, focusing primarily on international and domestic outsourcing transactions, venture capital transactions and private mergers and acquisitions. Megan has represented clients in multi-jurisdictional and domestic sourcing transactions across a variety of industry sectors including information technology, telecommunications, customer relationship and call centres, human resources, cloud computing and facilities management. Megan also has experience with re-negotiating sourcing transactions, both domestic and international.

BRAD PETERSON
Partner

Brad Peterson, a partner in the Chicago office, focuses on outsourcing, joint ventures, strategic alliances and information technology transactions. Brad has represented customers in dozens of large outsourcing agreements, including outsourcing finance and accounting, procurement, human resources, IT infrastructure, applications development and maintenance and other functions. Brad has also represented information technology buyers in hundreds of technology transactions, including cloud computing, software licensing, software development agreements, hosted services agreements, and ERP implementation agreements. With a background in the IT industry, an MBA from the University of Chicago and a JD from Harvard Law School, he provides practical, business-oriented advice on contracting for technology and services.

MARK A. PRINSLEY
Partner

Mark Prinsley is a partner in the London office and the head of the IP/IT, outsourcing and privacy practice in London. His practice is focused on complex IT and business process transactions which are frequently multi jurisdictional and often involve issues relating to personal data. His practice involves acting for customers at all stages of outsourcing transactions, particularly in the financial services sector.

LINDA RHODES
Partner

Linda Rhodes, partner in the Washington, D.C. office, focuses her practice on complex commercial transactions, with a primary focus on business and technology sourcing. She has represented a wide spectrum of clients, including large multinational corporations, in a variety of industries, such as information technology, telecommunications, pharmaceuticals, health care, financial services, insurance, energy, chemicals and consumer products. She has substantial experience in leading contract negotiations, bringing complex transactions to successful closure and effectively managing the international aspects of global transactions.

PAUL J.N. ROY
Partner

Paul J.N. Roy is a partner in the Business & Technology Sourcing practice in Chicago and represents clients in a broad range of information technology transactions, including technology development, implementation, support. He also regularly advises clients with outsourcing transactions, including outsourcing of IT infrastructure, application development and maintenance, and network management functions, and outsourcing of business process functions, including financial services, securities, and finance and accounting, HR/employee services and CRM services, among other business process functions.

DEREK SCHAFFNER
Counsel

Derek J. Schaffner is counsel in Mayer Brown's Washington DC office and a member of the Business & Technology Sourcing practice. He represents clients in a wide variety of information technology and business process outsourcing transactions and other information technology licensing and development transactions. Derek's representative information technology transactions include the outsourcing of IT infrastructure services and support, managed network services, network security services, application development & maintenance, telecommunications services, and cloud hosting services. His representative business process sourcing transactions include ERP deployments, the outsourcing of finance & accounting functions, human resource/employee services, and international employee relocation services.

OLIVER YAROS
Senior Associate

Oliver Yaros is a senior associate in the Intellectual Property & IT group of the London office, having joined Mayer Brown as a trainee in 2004 and admitted to practice in 2006. He advises clients on TMT, outsourcing, IT, data protection, privacy, e-commerce and IP issues. Oliver acts on global financial industry utility projects, IT and business process outsourcing projects and IT systems procurement transactions as well as advising a range of clients on many e-commerce and data protection issues such as how to comply with data protection laws throughout Europe, the change in the law on cookies, the export of personal data from the EEA, conflicts between privacy compliance and disclosure requirements under foreign law, theft or loss of data and the appropriate organizational and technical measures to take to protect data.

About Mayer Brown

Mayer Brown is a global legal services provider advising clients across the Americas, Asia and Europe. Our geographic strength means we can offer local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.