MAYER·BROWN

Issue 17 | Winter 2012

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

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

David J. Messerschmitt
Chicago
+1 312 701 8902
dmesserschmitt@mayerbrown.com

Welcome to the Winter 2012 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:

- Estimating the value for contact terms in sourcing agreements;
- Contracting for the private cloud;
- Cross-border privacy issues related to the US Patriot Act;
- The ever evolving product sourcing value chain in China; and
- Preparing for eDiscovery in outsourcing contracts.

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

We'd like to hear from you with suggestions for future articles and 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. ◆

Estimating the Value of Contract Terms in Sourcing Agreements

Brad L. Peterson

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

Although estimates of economic value in sourcing agreements generally focus on the pricing schedule and the products or services to be delivered, sourcing agreements also provide value by securing commitments, obtaining options, aligning incentives and supporting a successful relationship. Those commitments, options, incentives and support for a successful relationship—referred to in this article as contract terms—clearly have economic value. However, customers generally do not make formal estimates of the economic value of contract terms. Instead, customers generally rely on impressions of the importance of "risks" or "key terms." In this article, I endeavor to describe the benefit of estimating the economic value of contract terms and approaches to doing so.

The Benefit of Estimating the Value of Contract Terms

Estimating the economic value of the contract terms in a sourcing agreement allows customers to:

- Make smarter choices between lower prices and better contract terms.
- Balance the desire to "get it done now" against the value of "doing it right."
- Invest appropriate time and resources in drafting and negotiating contract terms.
- Focus negotiating energy on the high-value contract issues.
- Recognize contracting teams and souring professionals for the value they create by crafting and negotiating superior contract terms.
- Achieve desired business outcomes.

Contract terms can help to secure a commitment to provide specified products and services at firm prices.

Estimating the Economic Value of Commitments

Contract terms can help to *secure a commitment to provide specified products and services at firm prices*. That commitment may include contract terms such as sweep clauses, service warranties, rights to make immaterial changes without additional charges, continuous improvement obligations, "all-in" pricing, first-priority access to scare resources, reliable disaster recovery commitments, audit rights, defined direct damages, reasonable amounts at risk and a clear and complete definition of scope.

To estimate how much a contract commitment is worth, you can estimate the additional cost of the likely outcome without the commitment.

To estimate how much a contract commitment is worth, you can estimate the additional cost of the likely outcome without the commitment. If the likely outcome is incurring additional charges, you could estimate the value of that commitment based on the likely additional amount that the supplier would charge absent that commitment.

If the likely outcome is alternative sourcing, you could estimate the value of that commitment based on the cost of the best alternative available without that commitment. For example, if the contract in essence exchanges a long-term commitment for a 10 percent reduction in cost compared to spot market prices, that 10 percent could be the estimate the value of failing to secure the commitment. In situations where there may not be comparable products or services available on the spot market, the best estimate might be the expected cost of a workaround or supply interruption.

Estimating the Economic Value of Options

Contract terms can *provide options* to the customer, such as an option to obtain out-of-scope services at reasonable prices, in-source or re-source, change technical or operational requirements, impose reasonable rules and restrictions, relocate customer facilities, change customer technology, adjust prices through benchmarking, have services provided to related companies (including divested companies), terminate the agreement or obtain additional services such as M&A support or termination assistance services.

A straightforward approach for calculating the direct economic benefit of an option is to estimate the probability of exercising the option and to multiply that figure by an estimate of the economic benefit achieved by exercising the option.

Options such as these are valuable because they reduce the amount and likelihood of change-related charges. Customers' financial models tend to overlook the value of options because they assume that all will go as planned—an increasingly unrealistic assumption in our fast-changing world.

A straightforward approach for calculating the direct economic benefit of an option is to estimate the probability of exercising the option and to multiply that figure by an estimate of the economic benefit achieved by exercising the option. For example, if the supplier agrees that a termination-for-convenience charge will be reduced by $1 million if related to a change of control, and if you estimate a 5 percent probability that the customer will terminate related to a change of control, you could estimate the value of that provision as 0.05 x $1,000,000 = $50,000. If you can obtain that provision for less than $50,000, then it will add value to the contract.

Contract terms can increase incentives for the supplier to act in the customer's best interest.

That is, of course, a straightforward example. You may need to use more judgment to estimate the value of options that provide agility, flexibility and adaptability in achieving desired business goals. These are undeniably important. Even though the value of these options cannot be estimated with precision, an estimate based on the collected best judgment of your team will be superior to ignoring their value.

Estimating the Economic Value of Aligning Incentives

Contract terms can increase *incentives for the supplier to act in the customer's best interest*. Contract terms such as service level credits, deliverable credits, holdbacks, gain sharing, obligations for the supplier to correct its errors at its cost, and indemnities against harm caused by the supplier support a successful relationship by helping to aligning the interests of the supplier and the customer. These incentive provisions can also mitigate potential customer risk by requiring the supplier to pay some of the customer's losses. These incentives can balance the perverse incentives created by the primary pricing structure, such as the incentive to do only what is required at minimum cost created by a fixed-price arrangement.

You can estimate the value of an incentive clause by subtracting the economic value you expect to derive without the incentive from the economic value you expect to derive if you have the incentive. The value you place on incentives depends on your estimates of (i) the value of achieving your desired business outcome, (ii) the supplier's ability to help to achieve that outcome and (iii) the strength of the incentive.

The strength of the incentive depends on its size relative to the supplier's cost of achieving the desired result.

The strength of the incentive depends on its size relative to the supplier's cost of achieving the desired result. Like the customer, the supplier is looking at the cost-versus-risk calculation. For every dollar that the customer wants the supplier to invest in reducing a risk by 1 percent, the supplier should have at least $100 at risk. Any smaller sum at risk would make the potential liability more of a cost of doing business than an incentive.

Estimating the Economic Value of Supporting a Successful Relationship

Contract terms can also *support a successful outsourcing relationship* by:

- **Building trust.** Trust increases when companies are willing to translate their communications into enforceable legal obligations. It is further increased when the contract terms make the two companies, to a degree, accountable to each other as "partners" in sharing the risks and rewards of operating the outsourced scope. Trust allows companies to work together seamlessly.
- **Creating alignment on how to work together.** Sourcing contracts create complex, multi- faceted relationships. Agreeing on how to work together allows these relationships to succeed across company boundaries. For example, specifying reporting, governance and information-rights simplifies the communication process; agreeing on how work will be added or removed reduces friction at important points in the relationship; and issue management and escalation provisions make it easier to resolve disputes.

The purpose of these provisions is to make the contract easier and less expensive to govern. Thus, customers might estimate the value of these provisions based on the amount of additional spending that will be required to make up for not having them. In addition, the customer might consider the additional value created by a well-functioning relationship, such as innovative ideas and rapid response to needs for change.

Importance of Data

The accuracy of the estimate of course relies on the quality of the data. Customers often gather or create useful data as part of analyzing the overall business case. For example, if the value of the desired business outcome is estimated, that estimate can be used to value any change in the probability of achieving that desired business outcome. Deciding how the value of contract terms will be estimated generally allows a customer to more easily identify the key data and gather it during the initial due diligence phase and save it for future reference after a contract is complete.

Thus, the value of contract terms should be estimated based on their effect on desired business results, taken as whole, not as individual terms.

The contract terms are a key data point and require careful analysis. First, the strength of individual contract terms depends the limitations, exclusions and other precise language of those contract terms. Second, just as a chain is only as strong as its weakest link, an individual contract term may only be effective if related contract terms are also effective. For example, a strong commitment is of little value without an adequate remedy for breach. Thus, the value of contract terms should be estimated based on their effect on desired business results, taken as whole, not as individual terms.

However, even a simple estimate based on rough data can provide better guidance for economic decisions than ignoring the economic effect of contract terms in financial analyses or merely listing contract terms or risks. Ignoring the contract terms is equivalent to valuing them at zero, yielding a more wrong answer than a simple

estimate on rough data. Valuing contract terms at zero will result in agreeing to poor contract terms with results such as surprise charges, lack of control, inability to exit, compliance failures and responsibility for the supplier's failures. Merely listing contract terms or risks forces the decision makers to guess at the terms' importance in maximizing shareholder value.

Contract terms provide value by securing the supplier's commitment to defined services for a fixed price, providing options, aligning incentives and supporting a successful relationship.

Summary

Contract terms provide value by securing the supplier's commitment to defined services for a fixed price, providing options, aligning incentives and supporting a successful relationship. Customers can estimate the economic value of contract terms. Although an uncertain future makes that value difficult to estimate accurately, customers can make better decisions and achieve better business outcomes by working with available data to derive their best estimates of the value created by contract terms. ◆

▲ Return to Table of Contents

Contracting for Private Cloud Services

Paul J. N. Roy
Kavi C. Grace

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

Kavi C. Grace
Chicago
+1 312 701 8218
kgrace@mayerbrown.com

The drumbeat of cloud computing is getting ever louder with regular testimonials about the cost-savings and agility benefits it provides. Yet large corporations have made only limited use of cloud computing. They have typically limited cloud services to peripheral, non-core functions, due to technical, legal and security concerns.

Today, many companies are discovering the growing number of offerings for a breed of private cloud services that deliver the benefits of public cloud computing, while providing more of the protections that large corporations seek.

Today, many companies are discovering the growing number of offerings for a breed of private cloud services that deliver the benefits of public cloud computing, while providing more of the protections that large corporations seek. This growth in corporate-friendly offerings is being fueled by the goal of cloud service providers to expand their reach into the corporate market and by the desire of traditional outsourcing providers to protect their share of that market.

Private Cloud Computing Defined

The National Institute of Standards and Technology (NIST) describes the essential characteristics of cloud computing as (i) on-demand self-service, (ii) broad network access, (iii) resource pooling, (iv) rapid elasticity and (v) measured service. It further defines a "private cloud" as a cloud computing infrastructure that "is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units), [which] ... may be owned, managed and operated by the organization, a third party, or some combination of them...."

This definition covers a wide range of private cloud offerings, many of which can have very different consequences for the customer. Some private cloud offerings go a long way toward addressing the privacy, security and compliance issues that companies face, while others pose many of the same risks as public clouds. The fact that a service is a private cloud offering does not necessarily solve all these issues. Customers must carefully consider the attributes of each service and the corresponding contractual protections that it can obtain.

From a customer's perspective, a well-constructed private cloud contract will adhere to many of the customer protections found in traditional outsourcing contracts.

Contract Terms for Private Services

From a customer's perspective, a well-constructed private cloud contract will adhere to many of the customer protections found in traditional outsourcing contracts. It will also allow the service provider the flexibility needed to achieve the structural efficiencies inherent in cloud computing. The following is a brief review of some of the key terms that customers should obtain when contracting for private cloud services to support core functions.

A key contractual term for private cloud services that support core functions is the customer's ability to specify the locations where data will reside.

Location Commitments. A key contractual term for private cloud services that support core functions is the customer's ability to specify the locations where data will reside. This requirement arises principally from the customer's need to comply with data privacy and security regulations enacted around the globe. This term is standard in outsourcing contracts but not in public cloud contracts, which enable the provider to change locations at will and without notice to or consent by the customer.

Architectural Control. In contrast to traditional outsourcing arrangements, the standardized nature of the service provider's private cloud environment means that the customer must accept some loss of architectural control. A customer can take steps to ensure that its systems are compatible with the cloud systems at the start, but this is not a complete protection, since the provider can make changes over time.

There are risks that the customer may incur uncertain costs to make modifications to its systems or that it could suffer disruption, neither of which is tenable when core functions are involved. If the customer cannot be protected against a disruptive change, the contract must at least include rights that give the customer the legal and practical ability to terminate the cloud services and provide a reasonable time to transition its functions to an alternate provider before the change takes effect. One additional provision that can help the customer to avoid burden or disruption is a requirement that the provider must give the customer advance notice of its architectural plans and ensure opportunity to comment on those plans.

Technology Currency and Technology Advances. In traditional outsourcing contracts, customers often require providers to keep pace with current technology and to share their advances with the customer. Cloud service providers may resist this requirement on the grounds that they must maintain consistent architecture, which, for technical or strategic reasons may not be current in every respect.

The need for this protection is less compelling in cloud services, however, because the cloud provider is already motivated by competitive pressures to keep its shared environment current. Nevertheless, customers that rely heavily on cloud services for core functions may want some general commitment in this regard, particularly given the potential time and effort required to shift a core function to another provider.

Data Security Commitments. Cloud contracts generally do not permit customers to impose their unique security requirements on the provider. This is not significantly different from traditional outsourcing arrangements in which providers press to use their own security protocols when delivering services from their environments (e.g., a provider's data center or call center).

In private cloud arrangements, as in traditional outsourcing, the customer should have the right to require the provider to confirm that its security protections equal or exceed the customer's standards and that it will not diminish those protections.

The difference comes in how the potential gap is bridged. In public cloud offerings, the customer is usually obliged to satisfy itself that security protections disclosed by the provider are adequate. In private cloud arrangements, as in traditional outsourcing, the customer should have the right to require the provider to confirm that its security protections equal or exceed the customer's standards and that it will not diminish those protections. This difference is important, since the provider is clearly better-positioned than is the customer to interpret the security-related capabilities of its own systems and procedures.

Termination Charges and Residual Costs. Given the standardized nature of the cloud infrastructure and the deployment of that infrastructure to support multiple customers, contracts for private cloud services should not require the customer to pay termination charges for stranded systems costs. There may be termination costs in some cases, particularly if the customer has required the provider to assist with transition of the customer's systems to the cloud environment (i.e., data conversion, transfer and testing) without full, up-front compensation for those services. Flexibility is one of the inherent benefits of cloud computing, however, so any provider request for termination charges should be carefully scrutinized.

Building customer confidence in using private clouds to support critical functions will, no doubt, require a strong connection to the provider organization.

Post-Termination Rights to Technology. One of the protections that customers often obtain in traditional outsourcing agreements is the right to acquire equipment and software used by the provider to support the customer. This protection is not available in private cloud arrangements for the obvious reason that the supplier cannot hand over part of its cloud infrastructure. As a result, it is important that customers of private cloud services include contract protections, similar in terms to traditional outsourcing contracts, that ensure the customer will have the time and information necessary to in-source or re-source the services when necessary, regardless of the reason for termination.

Post-Termination Rights to Personnel. In traditional outsourcing contracts, the customer often has the right to hire provider personnel who are substantially dedicated to the customer's account. This helps ensure transfer of knowledge relevant to the supported function.

Because private cloud services, by definition, do not rely on personnel dedicated to the customer, this protection is not available to customers of those services. The absence of this protection further underscores the importance to customers of exit-planning and associated contract rights.

Limitations on Key Personnel. Contractual assurances relating to the quality and continuity of key provider personnel are mainstays of traditional outsourcing contracts. The success of an outsourcing relationship depends heavily on effective governance of the relationship. While private cloud services rely less on individual management, the reality is that even in those arrangements, there is need for effective governance to answer questions, advise on strategy and resolve problems.

Building customer confidence in using private clouds to support critical functions will, no doubt, require a strong connection to the provider organization. Consequently, many of the same key personnel protections found in traditional outsourcing contracts should apply, as well, to private cloud arrangements.

Audit Rights. Customers in traditional outsourcing arrangements typically have broad audit rights, while customers in public cloud arrangements have few, if any. Audit rights in private cloud contracts generally fall somewhere in between.

Since private cloud services utilize leveraged systems, private cloud providers want to limit a customer's operational audit rights to protect the security and the integrity of those systems. This may limit the extent of a customer's right to directly access the provider's systems and may well prevent the customer from being able to test the integrity of those systems. Nevertheless, private cloud customers should have the right to obtain all the information and data they need to satisfy their control requirements. In addition, customers should require SSAE 16 or equivalent audit reports for the provider's systems and processes used to support the customer.

An essential characteristic of cloud computing is price elasticity, which results from broad leveraging of the cloud systems across multiple customers.

Change in Volumes. Pricing structures under traditional outsourcing contracts often contain volume ranges beyond which unit pricing must be renegotiated. This constraint is based on the changing proportion of the provider's fixed and variable costs that comes with volume changes.

An essential characteristic of cloud computing is price elasticity, which results from broad leveraging of the cloud systems across multiple customers. Volume-pricing discounts may still be used by cloud providers wishing to encourage broader use of their systems.

Another factor that may influence variable pricing, at least for some initial period, is cost recovery. This becomes especially relevant when a provider incurs up-front costs in assisting the customer to initially transition to a cloud environment.

Conclusion

Many of the benefits of private cloud services come from the provider's standardization of its services across multiple customers, including standardization of its architecture, currency, security controls and quality measures. Standardization in this context requires certain customer compromises and risks that must be carefully managed, particularly when the private cloud is used to support core customer functions.

The transition of large corporations to widespread use of cloud services for core functions is likely to be slow and evolutionary because of these risks and compromises. However, the persistent cost pressures and agility demands on companies and their need to remain competitive, together with competitive pressures among service providers, make this evolution inevitable.

Lawyers representing these companies must find contract solutions that balance customer needs against the essential features of cloud computing. They must also aim to develop outsourcing contracts that not only keep pace with changing customer issues, but that also advance the evolution of the cloud computing industry. ◆

▲ Return to Table of Contents

The USA Patriot Act and the Privacy of Data Stored in the Cloud

Alex C. Lakatos

Alex C. Lakatos
Washington, DC
+1 202 263 3312
alakatos@mayerbrown.com

European consumers have expressed concern that the USA Patriot Act (the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" or "Patriot Act") will afford the US government undue and unfettered access to their data if they choose to store it on the cloud servers of US providers (e.g., Microsoft or IBM). A recent survey found that 70 percent of Europeans have concerns about their online data and how well it is secured. For many, these fears were exacerbated by an announcement by Gordon Frazer, the managing director of Microsoft UK, that he could not guarantee that data stored on Microsoft servers, wherever located, would not end up in the hands of the US government, because Microsoft, a company based in the United States, is subject to US laws, including the Patriot Act. Aware of these concerns, some EU data centers have gone so far as to advertise that they provide "a safe haven from the reaches of the Patriot Act."

To evaluate the validity of these concerns, several questions must be considered. First, exactly what information does the Patriot Act reach? Second, how likely is it, as a practical matter, that the Patriot Act will ever be used to reach a European company's data stored in the cloud? Finally, how does that risk compare with exposure that European companies already face, such as the prospect of their home-country governments accessing their cloud-stored data? As Ambassador Phillip Verveer, the US State Department's Coordinator for International Communications and Information Policy, explains, "[t]he PATRIOT Act has come to be a kind of label for [privacy] concerns.... We think, to some extent, it's taking advantage of a misperception, and we'd like to clear up that misperception."

"[t]he PATRIOT Act has come to be a kind of label for [privacy] concerns.... We think, to some extent, it's taking advantage of a misperception, and we'd like to clear up that misperception."

This article seeks to dispel some of the myths shrouding the Patriot Act, and to provide an assessment of the risks the Patriot Act poses to data stored in the cloud, particularly where the data, or its owner, are based outside of the United States.

Patriot Act Discovery Tools for Law Enforcement

Contrary to a common misconception, the Patriot Act did not create entirely new procedural mechanisms for US law enforcement to use to

obtain data in furtherance of its investigations. However, the Patriot Act *did* expand certain discovery mechanisms already available to US law enforcement. Two of these expanded mechanisms that US law enforcement could use to access data in the cloud that warrant discussion are FISA Orders and National Security Letters.

Contrary to a common misconception, the Patriot Act did not create entirely new procedural mechanisms for US law enforcement to use to obtain data in furtherance of its investigations. However, the Patriot Act *did* expand certain discovery mechanisms already available to US law enforcement.

FISA ORDERS

Prior to enactment of the Patriot Act, the Foreign Intelligence Surveillance Act permitted the FBI to apply to a special court, the Foreign Intelligence Surveillance Court, for a FISA Order to obtain the business records of third parties for the purpose of foreign intelligence and international terrorism investigations. Originally, however, such business records were limited to car rental, hotel, storage locker, and common-carrier records.

Title II of the Patriot Act, "Enhanced Surveillance Procedures," expanded the reach of FISA Orders to allow the FBI to obtain "an order requiring the production of any tangible things (including books, records, papers, documents and other items) for an investigation to protect against international terrorism and clandestine intelligence activities." This includes data in the cloud. To obtain a FISA Order, the FBI must specify that the tangible things sought are for an authorized investigation either to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

FISA Orders, particularly as expanded under Section 215 of the Patriot Act, have given rise to privacy concerns for several reasons. First, such orders may be granted *ex parte*, meaning with only the FBI presenting evidence to the court. Second, Section 215 includes a "gag" provision that prohibits the party that receives a FISA Order from disclosing that fact. This typically would prevent a cloud service provider from informing its customers that the service provider had shared their data with the FBI in response to a FISA Order. Third, the fact that Section 215 allows the FBI to obtain a person's library records sparked significant protests that the provision was invasive of reader privacy. Finally, the American Civil Liberties Union objects that "[t]he FBI need not show probable cause, nor even reasonable grounds to believe, that the person whose records it seeks is engaged in criminal activity."

In the USA Patriot Act Improvement and Reauthorization Act of 2005, enacted March 9, 2006, Congress took several steps to address these concerns, including adding provisions to allow the recipient of a FISA Order to oppose it before the Foreign Intelligence Surveillance Court and also, after a one-year hiatus, to contest the gag provision. Congress also required the US Attorney General to promulgate regulations to "minimize the retention, and prohibit the dissemination, of non-publicly available information." Notwithstanding these efforts, privacy and civil liberties advocates remain deeply troubled by Section 215.

What is the practical effect of FISA Orders on users of US cloud services? The answer is that the FBI rarely uses FISA orders. In 2010, the US government made only 96 applications to the Foreign Intelligence Surveillance Courts for FISA Orders granting access to business records. There are several reasons why the FBI may be reluctant to use FISA Orders: public outcry; internal FBI politics necessary to obtain approval to seek FISA Orders; and the availability of other, less controversial mechanisms, with greater due process protections, to seek data that the FBI wants to access. As a result, this Patriot Act tool poses little risk for cloud users.

NATIONAL SECURITY LETTERS

The National Security Letter (NSL) is a form of administrative subpoena that the FBI and other US government agencies can use to obtain certain records and data pertaining to various types of government investigations.

When the Patriot Act was enacted, there were already four federal statutes authorizing enumerated government authorities (chiefly the FBI) to issue NSLs. First, under the Right to Financial Privacy Act (RFPA), the FBI and the Secret Service may obtain financial records from financial institutions such as banks, securities brokerages, car dealers, pawn brokers, casinos, and real estate agents (accountants and auditors, however, are not included).

Second, under the Fair Credit Reporting Act, the FBI may use a NSL to obtain from a consumer reporting agency (e.g., the three major credit bureaus: TransUnion, Equifax, Experian) the names and addresses of all financial institutions at which a consumer maintains or has maintained an account, plus consumer-identifying information such as name, address and employment history.

Third, under the Electronic Communications Privacy Act, the FBI may request, from wire or electronic service providers (including Internet service providers), subscriber information, toll-billing records information, and electronic communication transactions records. The US Department of Justice takes the position that this includes, with regard to email accounts, the name, address, and length of service of a person, as well as email addresses associated with an account and screen names.

Fourth, under the National Security Act, an authorized government investigative agency may request any of the types of information described above, from any of the sources described above, when necessary to conduct security checks of government employees or investigate US government employees believed to be spying for foreign powers.

Title V of the Patriot Act, Removing Obstacles to Investigating Terrorism, expanded the FBI's authority to make NSL requests beyond its headquarters, to its 56 field offices; eliminated the requirement that the information sought relate to a foreign power, instead requiring that the NSL request be relevant to international terrorism or foreign spying; and allowed the FBI to obtain full consumer credit reports. The Patriot Act also added another NSL section to the Fair Credit Reporting Act, this one allowing not just the FBI, but any government agency, to obtain information from a consumer-reporting agency in connection with international terrorism or intelligence activities.

After the Patriot Act expanded the scope of NSLs as described above, their use began to rise. The Department of Justice reported to Congress that in 2010 the FBI made 24,287 NSL requests (excluding requests for subscriber information only).

NSLs give rise to privacy concerns and, according to critics, the potential for abuse, for several reasons. First, the FBI may issue NSLs on its own initiative, without the authorization of any court. (This was true even before the Patriot Act.) Nothing in the Patriot Act provides for any judicial review of the FBI's decision to issue an NSL. Second, the NSL statutes impose a gag requirement on persons receiving an NSL. In addition, the Attorney General Guidelines and various information-sharing agreements require the FBI to share NSL information with other federal agencies and the US intelligence community.

While the use of NSLs is not uncommon, the types of data that US authorities can gather from cloud service providers via an NSL is limited. In particular, the FBI cannot properly insist via a NSL that Internet service providers share the content of communications or other underlying data.

The Reauthorization Act tried to redress some of these concerns. It provided a right to judicial review of NSLs and a right to petition a court to lift the gag order. The Reauthorization Act also provided criminal penalties for violating gag obligations with the intent to obstruct an investigation.

So where does this complex statutory scheme leave cloud users? While the use of NSLs is not uncommon, the types of data that US authorities can gather from cloud service providers via an NSL is limited. In particular, the FBI cannot properly insist via a NSL that Internet service providers share the content of communications or other underlying data. Rather, as set forth above, the statutory provisions authorizing NSLs allow the FBI to obtain "envelope" information from Internet service providers. Indeed, the information that is specifically listed in the relevant statute is limited to a customer's name, address, and length of service.

The FBI often seeks more, such as who sent and received emails and what websites customers visited. But, more recently, many service providers receiving NSLs have limited the information they give to customers' names, addresses, length of service and phone billing records. "Beginning in late 2009, certain electronic communications service providers no longer honored" more expansive requests, FBI officials wrote in August 2011, in response to questions from the Senate Judiciary Committee.

Although cloud users should expect their service providers that have a US presence to comply with US law, users also can reasonably ask that their cloud service providers limit what they share in response to an NSL to the minimum required by law.

Although cloud users should expect their service providers that have a US presence to comply with US law, users also can reasonably ask that their cloud service providers limit what they share in response to an NSL to the minimum required by law. If cloud service providers do so, then their customers' data should typically face only minimal exposure due to NSLs.

Other Law Enforcement Tools

As discussed above, the two law enforcement tools for discovery of third-party data that were most significantly enhanced by the Patriot Act and that have given rise to significant concerns by European critics of the Patriot Act—FISA Orders and NSLs—should not, as a practical matter, pose a significant risk to European data on the servers of US-based cloud providers. But it would be a mistake to end the analysis there.

SEARCH WARRANTS AND GRAND JURY SUBPOENAS

US federal law enforcement has other, more traditional mechanisms for obtaining information it deems necessary to support its investigative efforts, such as search warrants (which must be approved by a US court upon a showing of probable cause) and grand jury subpoenas, which are issued by a US federal prosecutor in support of an ongoing grand jury investigation (and which a recipient may move to quash in court). These mechanisms also can be used to obtain data stored in the cloud. Should the risks these tools pose cause European companies to eschew US cloud services?

At the outset, consider that search warrants and grand jury subpoenas are hardly new. Search warrants trace their roots in the United States back at least to the Bill of Rights (ratified in 1791): the Fourth Amendment provides for protection against searches and seizures in the absence of a properly obtained warrant. Similarly, the grand jury has been functioning as an institution for receiving evidence of criminal activity since the Magna Carta and also has been incorporated into the US Constitution.

Moreover, Europeans (and others) have comparable discovery mechanisms in their home countries. For example, in France, the Police Nationale and the Gendarmerie Nationale both can execute search warrants. Article 13 of Germany's Basic Law similarly recognizes judicially ordered search warrants. And, of course, US search warrants have their roots in English law. Accordingly, to the extent European consumers wish to avoid any risk that any government will access their cloud data, merely avoiding US service providers is unlikely to help.

MLATS

Sequestering data on European cloud servers may be an ineffective prophylactic against US government access for another reason. The United States and most European governments have entered into bilateral Mutual Legal Assistance Treaties (MLATs). In a typical MLAT, the two countries commit to provide one another with "the widest measure of mutual assistance in investigations or proceedings in respect of criminal offenses…."

In 2003, the United States and the European Union entered into an MLAT with a provision addressing data protection. That provision governs MLAT requests made pursuant to prior bilateral MLATs between EU Member States and the United States. The comments to the EUUS MLAT explain that this provision was "meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases." Accordingly, US MLAT requests, particularly

those concerning terrorism investigations, are seldom denied for data protection reasons.

US Jurisdictional Limitations

In the United States, only a party amenable to what is known as "personal jurisdiction" can be subject to a search warrant, grand jury subpoena, NSL, FISA Order or other enforceable request for documents or data. The fundamental requirements for exercising personal jurisdiction over an individual or corporation are grounded in the Constitution, and the Patriot Act did not alter those principles (nor did it purport to do so).

In the context of personal jurisdiction, due process considerations prohibit courts from exercising jurisdiction over a witness who lacks minimum contacts with the forum. In the case of a corporation, this means that any corporation based in the United States will be subject to US jurisdiction and, thus, can be subject to FISA Orders, NSLs, search warrants, or grand jury subpoenas. The same is generally true for a non-US corporation that has a location in the United States or that conducts continuous and systematic business in the United States.

US law enforcement authorities may serve FISA Orders, NSLs, warrants or subpoenas on any cloud service provider that is US-based, has a US office, or conducts systematic or continuous US business—even if the data is stored outside the United States. Thus, merely choosing a European cloud service provider is not enough to ensure that data is beyond the reach of US jurisdiction and the Patriot Act.

Furthermore, an entity that is subject to US jurisdiction and is served with a valid subpoena must produce any documents within its "possession, custody, or control." That means that an entity that is subject to US jurisdiction must produce not only materials located within the United States, but any data or materials it maintains in its branches or offices anywhere in the world. The entity even may be required to produce data stored at a non-US subsidiary.

What does this mean for non-US consumers of cloud services? First, US law enforcement authorities may serve FISA Orders, NSLs, warrants or subpoenas on any cloud service provider that is US-based, has a US office, or conducts systematic or continuous US business—even if the data is stored outside the United States. Thus, merely choosing a European cloud service provider is not enough to ensure that data is beyond the reach of US jurisdiction and the Patriot Act.

Second, US law enforcement authorities may serve FISA Orders, NSLs, warrants or subpoenas on any cloud service customer that is US-based, has a US branch, *or* conducts systematic or continuous US business—even if the data is stored outside the United States. Many European entities have a US presence, and their US presence will allow them to be subject directly to the authority of US law enforcement, regardless of what company they use for cloud storage.

The new legislation might, among other things, replace EU/US Safe Harbor regulations with a new approach that would make it illegal for the US government to invoke the Patriot Act on a cloud-based or data processing company, in efforts to acquire data held in the European Union.

The Patriot Act and European Data Protection

The European Commission's Directive on Data Protection generally prohibits the transfer of personal data to non-European Union countries that do not meet the EU "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy. To bridge these different privacy approaches, the Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor" framework. By joining and adhering to the EU-US Safe Harbor Agreement, US companies can demonstrate that their data protection practices meet EU data protection requirements. European companies then can share data with US participants in the Safe Harbor agreement without violating their home country data protection laws.

The Safe Harbor Agreement contains a provision that allows US companies to comply with applicable US laws compelling the production of data, including the Patriot Act. It is anticipated, however, that at the World Economic Forum in January 2012, the European Commission will announce legislation to repeal the existing EU data protection directive and replace it with more a robust framework. The new legislation might, among other things, replace EU/US Safe Harbor regulations with a new approach that would make it illegal for the US government to invoke the Patriot Act on a cloud-based or data processing company in efforts to acquire data held in the European Union. The Member States' data protection agency with authority over the company's European headquarters would have to agree to the data transfer.

Consumers of cloud services are wise to consider all types of risk to their data, whether from their home country's government or another country's government. Merely avoiding US cloud service providers based on concerns about the Patriot Act does not solve the problem.

The foregoing developments may significantly affect the legal landscape for protection of data on the cloud servers in the cross-border context and, thus, should be monitored closely. However, it may be years before the new legislation is enacted (the current EU Data Protection Directive took three years to be enacted). By that time, changes in technology may present entirely new challenges and considerations.

Conclusion

Consumers of cloud services are wise to consider all types of risk to their data, whether from their home country's government or another country's government. Merely avoiding US cloud service providers based on concerns about the Patriot Act does not solve the problem. That choice alone provides no assurance that cloud data is beyond the reach of the Patriot Act, nor does it provide protection against the risk that non-US governments will access the cloud-stored data, either on their own initiative or in response to a MLAT request from the United States.

Rather than making a selection based solely on the home country of competing cloud providers, informed consumers of cloud services should (i) consult legal counsel in their home country, in any jurisdiction where their data may be stored, and in any jurisdiction where their cloud service provider does business; (ii) closely review their cloud services contracts and ask their providers questions; and (iii) carefully consider all the relevant risks before making a decision. ◆

▲ Return to Table of Contents

Resolving Small Sourcing Disputes

Robert J. Kriss
Brad L. Peterson

Robert J. Kriss
Chicago
+1 312 701 7165
rkriss@mayerbrown.com

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

Resolving small disputes is daily fare for people who govern sourcing relationships. In the best relationships, it proceeds well, with each party feeling comfortable that they are being treated fairly. However, in other relationships, small disputes remain unresolved and fester. In some cases, a customer will find itself forced to accept an unfair resolution in order to obtain critical products or services. For example, a customer might agree that a task is out of scope, despite being described in the Statement of Work, because there is less business harm in paying twice for that task than in not having the task performed.

The problem, we believe, is the lack of a quick, fair and reasonably inexpensive way to resolve small disputes. Escalation to higher-level executives uses valuable management time to perform tasks that those executives may not be well suited to perform and can increase the number of people who are unhappy instead of actually resolving a dispute. Also, escalation often favors the provider as an expert in the particular type of contract. Courts provide neutral dispute resolution, providing an outcome that even the losing party can see as fair, but lawsuits are generally slow and expensive. Traditional arbitration may be somewhat faster, but the cost and time requirements are often out of proportion to the value of small disputes.

This solution provides the benefit of a neutral third party at a cost suitable for small disputes at speeds reflecting the business imperatives to quickly arrive at a decision.

A solution, we believe, is a form of what is sometimes called "daytime baseball arbitration." This solution provides the benefit of a neutral third party at a cost suitable for small disputes at speeds reflecting the business imperatives to quickly arrive at a decision. This solution would work as follows:

- **Initiation.** A party having a claim within the defined scope (say $250,000 or less for illustrative purposes) would have the right to initiate the process by sending a written statement to the other party describing the basis of the claim and making a monetary demand. The written statement would be subject to a strict word limit (say 3,000 words).
- **Response.** Within a short time frame (say five business days), the other party must respond with a written statement of its position within the same word limit and make a written settlement offer.

There is no formal discovery, although each side could demand information under the terms of the outsourcing contract before or after the process is commenced and may comment in its brief if it does not receive what it has requested. The arbitrator may consider unreasonable responses to discovery requests as a factor in reaching his/her decision in the dispute.

- **Arbitration.** The parties then would have a short period (say five business days) to attempt to settle the dispute without arbitration. If they fail to do so, a single arbitrator would be selected by the parties or a predetermined alternative dispute resolution service to resolve the dispute. The arbitrator must pick either the initiating party's demand or the other party's offer as set forth in their written submissions, whichever number the arbitrator concludes is more reasonable based upon the written submissions and oral argument. The hearing would be short (say one hour per side).
- **Resolution.** The arbitrator would be required to issue the award within a short period (say five business days). The arbitrator would not have to issue a written opinion supporting the award unless both parties request a reasoned opinion by the conclusion of the hearing. The award is final and non-appealable. The losing party pays the arbitrator's fees and costs and the prevailing party's attorneys' fees and costs.

Why do we think this process will be effective? First, since the arbitrator can award only one of the two figures presented by the parties at the outset of the dispute, there will be substantial pressure on the initiating party to present a reasonable demand and the responding party to present a reasonable offer. Often these numbers will be relatively close, which will facilitate reaching a negotiated resolution before arbitration begins. Second, since the parties understand that they will have limited opportunities to present their case and the arbitrator will simply choose whichever figure appears to be more reasonable, the parties will want to control their destinies and reach a settlement on their own before arbitration begins. Third, the "loser-pays-all" aspect of the procedure imposes additional pressure to settle. Although the cost of the proceeding should not be great, the symbolic significance of losing and paying all costs will encourage settlements. Finally, strict limits on schedule, length of briefs and duration of the hearing will expedite the process and control costs.

We believe that it can work equally well for resolving this fundamental problem in outsourcing relationships, resulting in better relationships and better business outcomes.

Baseball arbitration has worked in a number of settings, including, of course, baseball salary disputes where it originated. We believe that it can work equally well for resolving this fundamental problem in outsourcing relationships, resulting in better relationships and better business outcomes. In most cases it should result in the parties' reaching a settlement without arbitration. If the parties are unable to settle, it will resolve disputes before they can accumulate and become a bigger problem for the relationship. ◆

▲ Return to Table of Contents

The Evolving Product Sourcing Value Chain in China

Thomas J. Keenan
Geofrey L. Master

Thomas J. Keenan
Hong Kong
+852 2843 2589
thomas.keenan@
mayerbrownjsm.com

Geofrey L. Master
Hong Kong
+852 2843 4320
geofrey.master@
mayerbrownjsm.com

The product supply chain from China is not what it used to be. Over the past 20 years, Chinese consumer-product manufacturers have become increasingly sophisticated and capable of taking on more "value-adding" tasks or segments of the product creation supply chain and have moved from mere manufacturers to multifunctional suppliers. In doing so, they have changed the game, taking on an array of production functions traditionally handled within 'shop-by-product" companies.

However, unless there is evolution in the contracting model that takes these changes into account, product marketing (brand) companies will increasingly face threats to their core roles and functions.

This deconstruction of the manufacturing and product-development process has opened up new possibilities for product companies. However, unless there is evolution in the contracting model that takes these changes into account, product marketing (brand) companies will increasingly face threats to their core roles and functions. For some companies, the evolution of their value chain has been subtle, while for others, the changes have been dramatic and obvious and these companies have come to well appreciate the value and the leverage that the multifunctional supplier brings to the table.

The product value chain is fundamentally comprised of three players (represented in Table 1 below):

- **Manufacturers** — historically focused on the hard aspects of actual manufacture, taking orders from the product marketing companies and manufacturing the products.
- **Product Marketing Companies** — historically focused on the more intangible upstream and downstream aspects of production, such as conceiving, cultivating and launching product and Brand lines.
- **Product Distributors** — historically focused on the last step in the product value cycle, retail or wholesale (i.e., pushing product in the last mile to end-consumers).

In fact, rather than clearly delineated players, each of these players really represent a collection of functions — of value-add activities that all combine to form the product supply chain. In one of the most significant recent developments, the roles of Chinese product manufacturers have expanded, as these manufacturers have taken on more important roles in the supply chain, even becoming potential competitors to both product marketing companies and retailers.

It is important now to look at Chinese suppliers as providers of bundles of value-adding services that must be managed through a contractual framework that effectively addresses the unique attributes of product sourcing and the Chinese manufacturing landscape—a challenge well-suited to the outsourcing contractual model. This article will look at the evolution of the Chinese supply base in the provision of Original Engineering Manufacturing (OEM) (suppliers that manufacture to designs given to them), and Original Design Manufacturing (ODM) (suppliers that develop products and designs on their own) and the new world of issues that sourcing customers around the world face with their service contracts.

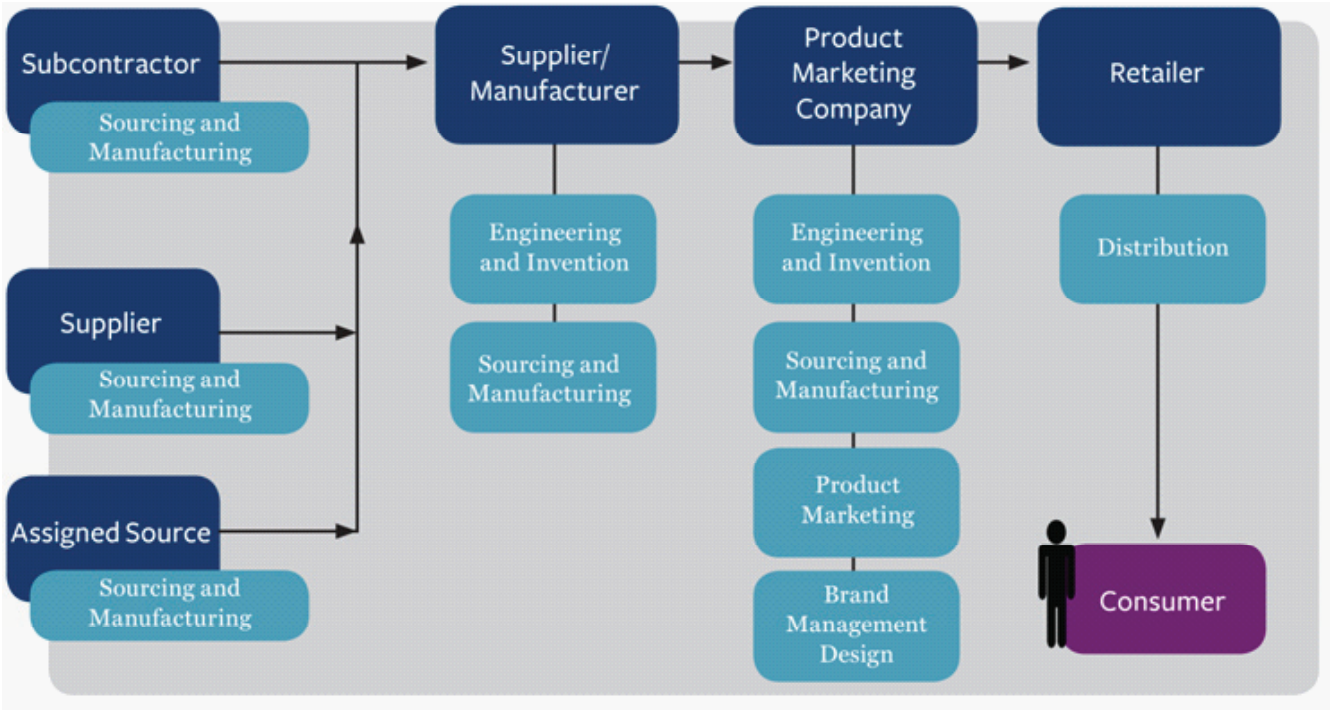
It is important now to look at Chinese suppliers as providers of bundles of value-adding services that must be managed through a contractual framework that effectively addresses the unique attributes of product sourcing and the Chinese manufacturing landscape—a challenge well-suited to the outsourcing contractual model.

The Evolving Value Chain 1990

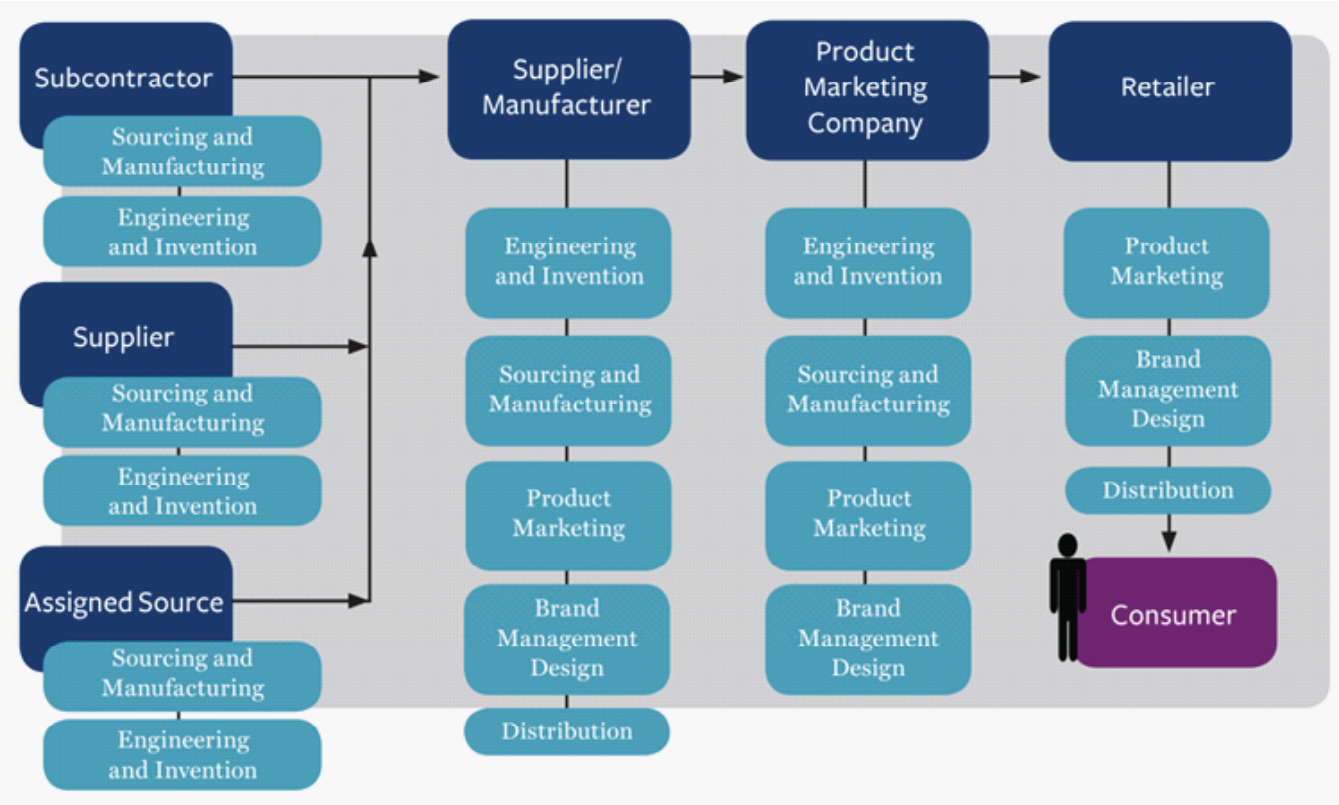
It is helpful to explain the evolution in the value chain through a comparison of the roles of each of the key players in the consumer-product value chain over the last 20 years.

In 1990, brand companies were the key drivers of product innovation as they actively cultivated their connections with retailers and consumers to develop each new generation of product. Key functions, such as marketing, product management, product design, design engineering and manufacturing, were deemed "mission critical" strategic functions that were naturally controlled internally. Manufacturers in China did little more than fabricate toolings, inject plastic parts, source components and assemble product for their customers. The relative added-value of the manufacturer was limited, and, as a result, their margins were thin. Retailers were primarily responsible for end-distribution and interfacing with the consumer.

"House Brands" were few and far between and were limited to opportunistic products at lower price points sourced off-the-shelf from suppliers. In summary, there was relatively little overlap in the roles and responsibilities of the different supply chain players.



The Evolving Value Chain 2010



Today, product marketing companies involve their manufacturers significantly earlier in the new product development process in order to save engineering costs and time and to provide for a more seamless transition to manufacturing. Chinese suppliers have risen to the opportunity, investing in product development engineering resources required to help their customers get products off the ground—motivated by the ability to raise their margins, notably through the avoidance of competitive bidding for new products. By getting involved earlier, Chinese suppliers "lock-in" their customers, avoid the risk of having to compete on mere lowest-cost manufacturing and improve their margins by using their new-found leverage to quote on a "value-base" rather than "cost-plus" basis. The integration of manufacturing suppliers into the process has helped to shorten development lead times, but early integration has left purchasing professionals without the ability to source the product with the best cost supplier.

Over the last 20 years, the confluence of three important factors has shaped the current value chain and shifted leverage away from the brand company to the supplier: (i) consolidation of the retail sector, (ii) the need for brand companies to be more cost-competitive through low-cost country manufacturing, and (iii) the push by Chinese suppliers to increase their margins and protect their manufacturing through the creation of more ODM products that cannot be ported to other suppliers.

The integration of manufacturing suppliers into the process has helped to shorten development lead times, but early integration has left purchasing professionals without the ability to source the product with the best cost supplier.

First, consolidation of the retail sector in both North America and Europe has allowed retailers to increase their own margins through the develop-

ment of "house brands" to supplement their own supplier's (brand companies') offerings. While initially undertaken on an opportunistic basis, the trend has become prevalent in hard lines (hardware, electronics), soft lines (clothing) and fast-moving consumer goods (groceries) product offerings, while squeezing the price points where many brand companies operate. As a result of their increased leverage through consolidation, retailers presented an attractive alternative customer base for Chinese manufacturers, allowing both the retailer and manufacturer to greatly increase their margins through the removal of the brand company intermediary.

Second, retailers have pushed their brand company suppliers to offer productivity savings and to lower their prices to consumers with products that are competitively priced against "house brand" products. Competition has further exerted pressure on the same brand companies to increase margins by lowering their manufacturing costs through shifting more and more of their manufacturing to low-cost countries.

The entire value chain for consumer products sourced or manufactured in Asia has become increasingly interconnected and mutually reliant—ownership of physical manufacturing assets and intellectual property rights has become more ambiguous and contentious.

Finally, in order to meet the needs of both retailers and brand companies, manufacturers in China have invested in human capital to increase management skills and English language capabilities, as well as investing in new critical areas such as product marketing, project management, product design and engineering, quality systems and injection-mould manufacturing. To further add value for their customers, these mostly privately held (family-run) companies have the cash to offer other services including injection-mould (production equipment) financing and product inventory and warehousing services. Successful Chinese suppliers have made these investments to stand themselves above their peers and, in the process, have increased their margins and have made themselves indispensable to their customers.

What Does This Mean Today?

The entire value chain for consumer products sourced or manufactured in Asia has become increasingly interconnected and mutually reliant—ownership of physical manufacturing assets and intellectual property rights has become more ambiguous and contentious. With ambiguity over ownership and rights to manufacturing assets, customers lose the key leverage of mobility. While brand companies were able to become more price competitive through lower production cost and reduced overheads within their own organizations by outsourcing their design engineering and manufacturing to Asia, their supply chains became longer and, while some new problems are obvious, others remain latent, only to emerge when the relationship breaks down.

Brand Companies

With greater reliance on suppliers in China to design their products, to finance their tooling and inventory, brand companies have found themselves more and more "married" to their suppliers. As a result, Brand companies find themselves directly and indirectly facing the same challenges as their suppliers: currency and commodity volatility, product quality and labor issues.

Brand companies are using the lowest-cost suppliers who themselves often employ unsophisticated purchasing, finance and management practices. As a result, the brand companies are receiving price increase requests from their suppliers on a monthly and sometimes weekly basis as their suppliers struggle to properly manage these issues. Suppliers that are facing these problems have been known to essentially suspend taking orders unless they get the price increases—bringing the supply chain to a grinding halt. Brand companies have an unenviable dilemma: either take the increases and the hit to their margins, or face the daunting prospects of trying to change suppliers during the product life cycle.

Poor product development processes in place between brand companies and their distant suppliers have given rise to three major problems: unclear responsibility for product quality, delayed product realization and ambiguous ownership of

protectable intellectual property rights. Supplier financing of tools and lack of clear assignment and licensing of intellectual property can make it cost-prohibitive or impossible to change suppliers when things get tough in the relationship.

Because Chinese suppliers make up such a large portion of most brand companies' cost of goods, brand companies are pressured to take into account additional concerns such as their suppliers' environmental and social compliance (ethical) practices.

Finally, corruption continues to be a major issue in China, and brand companies need to be both proactive and vigilant in their management of this issue. Brand companies need to establish clear expectations for their staff and suppliers and adopt policies for doing business with suppliers that engage in corruption, including termination of the business relationship. Brand companies need to structure their affairs with their suppliers so that they can quickly move away from a supplier that engages in untoward business practices.

As a result of increased reliance on manufacturers within the value chain and the investments made by brand companies to improve their manufacturers' capabilities, brand companies have created a new set of their own competitors that, on their own or in collaboration with retailers, are increasingly well-positioned to chip away at the brand company's market share and margins.

Manufacturers

As a result of their enhanced roles and capabilities, manufacturers find that they have new leverage in the relationship as well as a heightened awareness of the need to protect their interests and investments. Manufacturers also realize that Chinese nonlegal dispute resolution solutions do not adequately meet their needs when dealing with overseas customers. As a result, Chinese suppliers are warming to the idea that manufacturing outsourcing services agreements are not just tools for their customers to control them, but with their new-found leverage, are a means to protect their own interests. Many Chinese manufacturers today have further taken on advanced marketing services for their customers, including, in some circumstances, to "category management" ranges of products for their customer's product portfolio. Some suppliers have even greater ambitions—to develop and sell their own brand of products both domestically and abroad.

As a result of increased reliance on manufacturers within the value chain and the investments made by brand companies to improve their manufacturers' capabilities, brand companies have created a new set of their own competitors that, on their own or in collaboration with retailers, are increasingly well-positioned to chip away at the brand company's market share and margins.

Retailers

Retailers (those remaining) have strengthened their positions greatly in the past 20 years. Retailers now have two sets of suppliers to choose from: brand companies and Chinese manufacturers. A growing share of high-volume, low price-point products are being sourced directly from Chinese manufacturers, further putting pressure on product marketing companies.

Conclusion

Dramatic changes have taken place in the supply chain over the past 20 years, and manufacturing and product development services agreements used in today's environment all too often do not adequately contemplate or address either the obvious or the latent issues present in this new highly integrated, mutually reliant value chain. Manufacturing agreements in use today are often based on the 1990s model of distinct responsibilities of the parties with a relatively simple range deliverables of Chinese manufacturers with a narrow focus on the product, rather than the basket of services now on offer (and often provided).

Supply chain contracts need to address the distinct, discrete services performed by the manufacturer and adequately protect brand companies' interests.

Supply chain contracts need to address the distinct, discrete services performed by the manufacturer and adequately protect brand companies' interests.

In the absence of contractual coverage addressing these issues, the current trends tip the balance of control in the supplier's favor and raise an ever-increasing list of issues for brand companies to address without the proper tools.

Low-cost country manufacturing is here to stay. The myriad of issues and challenges that exist will increase, and all players in the supply chain will struggle to adequately control them.

Robust manufacturing and product development outsourcing services agreements should proactively address the new order problems that are emerging in the brand company-Chinese manufacturer relationships. A thorough discussion and agreement addressing key issues and providing flexibility for growth and change can keep the relationship balanced and allow the brand company to maintain reasonable options. ◆

▲ Return to Table of Contents

Preparing for eDiscovery in Outsourcing Contracts

Shawna Doran
Kim A. Leffert
Brad L. Peterson

Shawna Doran
Chicago
+1 312 701 7768
sdoran@mayerbrown.com

Kim A. Leffert
Chicago
+1 312 701 8344
kleffert@mayerbrown.com

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

Parties to litigation are typically required to identify, preserve, retrieve, review and produce electronically stored information (ESI) within their control that is potentially responsive to the matter. The time frames for fulfilling these discovery requirements are often short, and courts have shown little patience for companies that fail to meet their discovery obligations. An excuse that "the data is on an outsourcing provider's systems" will likely fall on deaf ears as courts continue to issue discovery sanctions for noncompliance that range from negligence to willful misconduct.

These sanctions can include monetary fines, adverse inference instructions, dismissal of the suit or default judgment or, sometimes, a combination of penalties. For example, in *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497 (D. Md. 2010), a federal court in Maryland found that the defendant had engaged in a willful bad-faith discovery violation, including the failure to implement a litigation hold, attempted and actual deletion of ESI and misrepresentations regarding the completeness of discovery. The court recommended a default judgment and a permanent injunction as to plaintiff's copyright claim. It also ordered monetary sanctions and that the president of Creative Pipe be jailed for not more than two years unless and until the award of attorneys' fees and costs was paid.

To protect themselves, companies need systematic, reasonable and defensible electronic discovery and records management programs designed to comply with discovery obligations. These programs can reduce the need to conduct costly or inefficient fact-gathering in response to discovery requests and provide defenses to claims of improper destruction, or spoliation, of evidence.

To protect themselves, companies need systematic, reasonable and defensible electronic discovery and records management programs designed to comply with discovery obligations. These programs can reduce the need to conduct costly or inefficient fact-gathering in response to discovery requests and provide defenses to claims of improper destruction, or spoliation, of evidence. Further, having an effective and updated records management policy, program and retention schedule will enhance a company's efforts to achieve proper data management—a key factor in minimizing discovery costs and mitigating the risk of sanctions.

A company that outsources its ESI to a third-party provider generally has the same obligations to preserve and produce relevant data that it would have if that data was on the company's own equipment and premises. In fact, a company may face heightened risk because a subpoena or discovery request may go directly to the third party. This article describes how a company can use contractual provisions to effectively manage its ESI remotely and to ensure compliance with its discovery obligations.

[I]f your service provider has access to data that may fall within the attorney-client or work-product privileges, consider adding specific clauses to the contract to protect any ESI that you have identified as potentially privileged.

Preserve Your Privileges

As a general matter, if your service provider has access to data that may fall within the attorney-client or work-product privileges, consider adding specific clauses to the contract to protect any ESI that you have identified as potentially privileged. For example, the contract could provide for additional restrictions on disclosure, data-tagging or segregation of potentially privileged information.

If you cannot specifically identify privileged information, consider using a broad-brush approach, such as requiring that the provider treat all communications to or from your corporate law department as potentially privileged. Or, if you are not aware of any particular privileged information, consider obtaining an option in your contract to designate information as protected at a later time. You may even agree to accept additional charges for such later-requested additional security.

If your service provider will store ESI that may be subject to preservation or production requests, consider contractually requiring the provider to engage in developing and implementing a joint litigation response plan.

Create a Litigation Response Plan

If your service provider will store ESI that may be subject to preservation or production requests, consider contractually requiring the provider to engage in developing and implementing a joint litigation response plan. Such a plan might involve, for example:

- A list of responsibilities for preserving ESI that can be identified with reasonable certainty, and which might be described in any preservation or production request, and for providing prompt notification of any technical or other limitations that would prevent fulfillment of the preservation or production request.
- Participation in periodic meetings to discuss and update litigation response policies and procedures.
- Appointment of an experienced legal information management representative by the service provider to manage production and preservation activities.

Provide Your Service Provider with a Litigation Requirements Notice

When litigation that has been filed, or is reasonably anticipated, relates to ESI possessed by your service provider, consider sending your provider a copy of the litigation hold notice that describes in reasonable detail all items to be preserved. Ask your provider to promptly contact you with any questions or concerns related to the notice and to provide you with any additional information you or the provider may need to more clearly determine the scope of the request.

Generate Information for Legal Proceedings

As litigation progresses, there are additional activities that you might want your service provider to undertake:

- Cost estimates for the preservation and/or production of data
- Descriptions of systems, data, media and processes utilized by the provider

- Reports, declarations and affidavits from provider personnel
- Explanations of why preservation or production of certain documents is infeasible or impossible in certain circumstances

Regardless of the responsibilities assigned to your service provider—whether related to preservation and production of ESI or to trial proceedings—it is recommended that you request your service provider to document in writing all steps taken to fulfill its obligations.

Regardless of the responsibilities assigned to your service provider—whether related to preservation and production of ESI or to trial proceedings—it is recommended that you request your service provider to document in writing all steps taken to fulfill its obligations. This documentation helps ensure that your company's requests are carried out in full. It also provides evidence of your company's diligent actions to comply with preservation obligations and discovery requests should your efforts come under scrutiny.

Third-Party Data Requests

Opposing parties may request or demand access to your ESI directly from one of your service providers. There is a risk that a provider might provide ESI that should not be delivered to the opposing party. You can reduce that risk by including in your agreement or litigation response plan requirements that the provider:

- Immediately contact a company representative upon receipt of any request or subpoena by third parties for corporate ESI possessed by the provider and, to the extent legally permissible, forward a copy of the request or subpoena to the company;
- Meet and confer with the company prior to responding to the third party(ies);
- Tender responsibility for responding to the request to the company, and assist with any responses; and
- Take all commercially reasonable steps to preserve the company's legal rights in connection with any response in the event the provider is barred from notifying the company of the request.

Having litigation response plans and including contractual obligations in service contracts can allow your company to handle discovery requirements faster, more effectively and with reduced risks and expenses when some or all of your data is managed by outsourced, or cloud computing, providers.

Recommendation

Having litigation response plans and including contractual obligations in service contracts can allow your company to handle discovery requirements faster, more effectively and with reduced risks and expenses when some or all of your data is managed by outsourced, or cloud computing, providers. Companies that do not already have these contractual provisions can attempt to amend their agreements with third-party providers that possess critical ESI. Consider including litigation-readiness provisions as a standard requirement for new contracts and new relationships with outsourcing and cloud computing providers. ◆

▲ Return to Table of Contents

SHAWNA DORAN

Associate

Shawna Doran is an associate in the Business & Technology Sourcing practice of Mayer Brown's Chicago office. Shawna's practice focuses on information technology and business process outsourcing arrangements, privacy and data security issues, and information technology transactions, including software license and implementation agreements. Before joining Mayer Brown, Shawna worked as general counsel for a company specializing in computer forensics and electronic discovery.

ALEX LAKATOS

Partner

Alex Lakatos, a partner in the firm's Washington DC office, practices in complex international litigation, particularly on behalf of non-US financial institutions. He also counsels financial institutions on banking and securities regulatory, enforcement, legislative, and strategic issues. He has significant experience in matters where these areas intersect – for example, the litigation of cross-border disputes in US court in tandem with an SEC or bank enforcement investigation. His matters often include parallel litigation in non-US forums. He is experienced in contesting issues of particular concern to non-US financial institutions, such as financial privacy, multi-jurisdictional discovery, choice-of-law conflicts, and asset forfeiture.

KAVI GRACE

Associate

Kavi Grace is an associate in the Business & Technology Sourcing practice, focusing on the areas of business process, operations and technology outsourcing, consulting, software development, e-commerce and information technology transactions. He regularly drafts and negotiates a broad range of agreements involving outsourcing arrangements, consulting services, software distribution and technology development services.

THOMAS KEENAN

Associate

Thomas Keenan is a lawyer in the Business & Technology Sourcing practice of Mayer Brown's Hong Kong office. He represents clients in product and service transactions, including the full range of supply chain activities. Prior to joining Mayer Brown, Tom was the head of sourcing for US and European multinationals based in Hong Kong and Paris. In addition to his native English, Tom is fluent in Mandarin and French.

ROBERT KRISS

Partner

Robert Kriss has represented some of the world's largest Internet and technology companies in commercial and class-action litigation. He began representing Internet-based companies in the late 1990s when he successfully defended America Online in more than 60 class actions arising from consumers' alleged difficulties connecting to AOL. Since then, Bob has successfully defended numerous consumer class actions involving a wide variety of Internet-based marketing and billing practices and has represented clients such as Accenture, Acxiom, AT&T, Oracle, Mead Johnson and others in commercial and securities litigation involving information technology outsourcing and new system implementation. He also has assisted companies in investigating and remediating data breaches and in establishing privacy policies.

KIM LEFFERT

Counsel

Kim Leffert, counsel in Mayer Brown's Chicago office, has an extensive litigation practice. A significant and growing part of her work involves electronic discovery issues. Kim has substantial experience assisting clients with the preservation, collection, review and production of electronic documents in litigation. She also helps clients prepare document retention policies and procedures and records-management programs, as well as develop electronic discovery programs.

GEOFREY MASTER

Partner

Geofrey Master is a partner in the Business & Technology Sourcing practice of Mayer Brown's Hong Kong office. Geof advises clients in transactions involving the sourcing of products and business functions, including information technology and business processes. Prior to joining Mayer Brown, Geof spent over ten years with Electronic Data Systems (now HP), including five years as international general counsel.

BRAD PETERSON

Partner

Brad Peterson is a partner in the Business & Technology Sourcing practice of Mayer Brown's Chicago office. His practice focuses on business process and IT outsourcing transactions, alliances, and information technology transactions, including software license and 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 technology contracts.

PAUL J. N. ROY

Partner

Paul J.N. Roy is a partner in the Business & Technology Sourcing practice of Mayer Brown's Chicago office and represents clients in a broad range of onshore, nearshore, and offshore information technology and business process outsourcing transactions. He regularly advises clients on the outsourcing of IT infrastructure services and support, application development and maintenance, network management and support and help desk/call center services. Paul also advises clients on the outsourcing of finance and accounting functions, HR/employee services, CRM and financial services operations, among other business process functions.

About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia and Europe. Our presence in the world's leading markets enables us to offer clients access to 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 & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

OFFICE LOCATIONS

AMERICAS
- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- Washington DC

ASIA
- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai
- Singapore

EUROPE
- Brussels
- Cologne
- Frankfurt
- London
- Paris

TAUIL & CHEQUER ADVOGADOS
in association with Mayer Brown LLP
- São Paulo
- Rio de Janeiro

ALLIANCE LAW FIRM
- Spain (Ramón & Cajal)

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