MAYER·BROWN

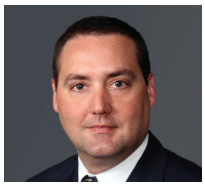
Issue 20 | Spring 2014

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

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

Welcome to the Spring 2014 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:

- Lessons Learned from Outsourcing Disputes
- Alternatives to Benchmarking and Cost Transparency
- Legal Issues in Contracting for SMAC Services
- Privacy Updates
- A Recap of 2013 by the Privacy Commissioner of Hong Kong and Strategic Focus for 2014
- Best Practices on NFC Mobile Payments Issued in Hong Kong

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. 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. ◆

Lessons Learned from Outsourcing Disputes

Peter Dickinson
Rani Mina

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

Rani Mina
London
+44 20 3130 3903
rmina@mayerbrown.com

This article was previously published on Feb 14th in *Supply Chain Europe* magazine.

The New Norm

The current challenging economic conditions are driving additional outsourcing activities. However, the need for companies to achieve greater efficiencies and reduce budgets means that customers are being forced to do more with less. In addition, the pace of technological change is accelerating and companies need to be able to swiftly react to unanticipated changes in the marketplace or otherwise fall behind the competition.

With outsourcing contracts historically having terms ranging from five to ten years, the industry has reached a point where there are examples of high profile failures — and the hidden risks and causes of these failures can be identified more easily. Recent examples of cases that have ended up in court include the dispute between Ericsson and H3G, arising out of the termination by H3G of an IT outsourcing contract, and the well-publicised case between BSkyB and EDS/HP, where EDS/HP paid BSkyB a reported £318 million in damages.

For every example of a failed outsourcing deal that is taken to court or reported in the media, our experience shows that there will be several more troubled deals in which the issues are resolved quietly between the parties behind closed doors.

The purpose of this article is to consider what lessons can be learned from some of those troubled sourcing deals.

Improving the Chances of Success from the Outset

When many of the long-term sourcing transactions now reaching maturity were entered into, the economic backdrop was very different: no one had foreseen the global downturn or the pace of technological change. Although most contracts provided for a limited degree of change without the parties having to renegotiate the contract (e.g., by use of the ARCs and RRCs model), they were not sufficiently flexible — in terms of their operating or charging models — to cope with the degree of change required.

It is essential that customers and suppliers need to recognise that through the lifecycle of any contract, unanticipated macroeconomic events or significant technological changes may arise which could materially impact the demand for services (both in terms of nature and volume).

One obvious way to mitigate this risk is to have shorter contract terms. Over the last few years, terms of between three and five years have become the norm. As a consequence, if and when unforeseen events do arise, the parties are more likely to be

able to find a solution to address them. However, that is by no means the only potential mitigation.

When entering into an outsourcing contract, a key issue for the customer will be whether the value of the deal is greater than the value of the alternatives that the outsourcing arrangement will preclude. It is common to undertake financial modelling when making these assessments, but companies will not properly understand the real value unless risk is factored in. If not, it is easy for the up-front financial value to be eroded quickly and for disputes to arise.

In recognition that the environment to be supported will almost inevitably change, and, therefore, so will demand for the services (both in terms of nature and volume), the contract should be designed to give much greater flexibility than was historically the case. The charging model underpinning the deal should recognise this fact also. For example, securing a lower unit cost by giving a minimum revenue commitment may make economic sense at the outset, but if the demand for services subsequently falls below the minimum revenue commitment, it becomes unsustainable.

When entering into an outsourcing contract, a key issue for the customer will be whether the value of the deal is greater than the value of the alternatives that the outsourcing arrangement will preclude.

A financial model which requires the payment of a partial termination fee if the consumption of services falls below a prescribed level could also become problematic at a time of unpredictable demand.

Solutions that include "financial engineering" (giving lower charges in the early years, in exchange for less competitive charges in the later years) are also best avoided, as they can limit flexibility.

Historically, the change control procedures contained in contracts simply provided that if one party wanted to materially change the nature or volume of the services, the agreement of the other party was required, often leading to disputes. Having predictability as to the cost of change should be a key objective. An agreed cost standard should be incorporated in the contract, making clear which changes will be at no cost (e.g. re-deploying a particular resource to another task which requires the same amount of effort) and which changes will be chargeable (e.g. an increase in scope) and setting out the basis upon which changes to the charges will be determined (and an expedited dispute resolution process if agreement cannot be reached).

Life Cycle Management (Including Resolving Outsourcing Disputes)

Getting the contract right at the outset is of critical importance. However, managing the arrangements and the risks carefully and effectively throughout the lifecycle of the contract is of equal importance.

Outsourcing disputes can be extremely difficult to resolve. Suppliers provide critical services, become embedded in a customer's business and are expected to deliver transformational change and savings to the customer. As a result, outsourcing disputes tend to be high value and highly significant for the customer and supplier.

The key to avoiding this situation is a clear understanding of the reasons why outsourcing relationships run into difficulties, and a realistic assessment by businesses of the benefits and risks of entering into large scale, long term outsourcing arrangements. Our experience of outsourcing disputes across a wide range of sectors and industries suggests that there are some common root causes:

- There is a tension between the desire of the customer to generate cost savings, and do so quickly, and the desire of the supplier to "win the deal" and protect profitability over the life of the deal. Pushing too hard at the outset on price may be attractive but counterproductive.
- Failure to define the scope of services. Vagueness in this area, or an agreement to agree the details later, is often a recipe for later disputes.

- Failure to allow for market developments in areas (such as IT outsourcing) where technology can develop rapidly over the course of an agreement spanning several years. This can leave a customer with no option but to pay for additional or different services in order to maintain efficiencies.
- The complex nature of many outsourcing deals means that, even in the best drafted agreements, it is impossible to anticipate every situation that may occur in a contract that could last for many years.

A key consideration in resolving any disputes which do arise is whether to litigate. For every outsourcing dispute that is litigated, numerous others are resolved by a private renegotiation.

A key consideration in resolving any disputes which do arise is whether to litigate. For every outsourcing dispute that is litigated, numerous others are resolved by a private renegotiation. There are good reasons for this "behind the scenes" approach, other than a healthy fear of litigation:

- Reputation — other than in extreme circumstances, suppliers do not want to be seen to be in dispute with their customers;
- There are other business drivers to continue the arrangement — this is often a long term contract, with most of the economic benefit derived from the later years;
- There is a real risk of business disruption if it were necessary to end the relationship;
- Where staff have transferred across to the supplier, it may be difficult to take the outsourced service in-house or set up new arrangements; and
- The complexity of many outsourcing relationships, and the interdependencies required from both parties to make it work, means that establishing where fault lies is costly and challenging in itself.

A good contract will provide many alternatives to legal action, gradually escalating from informal dispute resolution procedures, through formal exit provisions and all the way to litigation or arbitration.

At the outset of any dispute, it's important to identify the legal remedy that is available and to take steps to preserve this and ensure it is not prejudiced by any of the other steps taken, should it eventually become necessary to take legal action. The usual legal remedies to be considered are:

- Mandatory injunctions;
- Order for specific performance;
- Termination of the contract; and
- Claim for damages.

Potential Claim for Economic Duress

Supply- and service-level threats are a common negotiating tactic, which can leave the customer with little choice but to give in to the supplier's immediate demands.

A customer might also contemplate withholding payment under the contract in the event of a dispute, however, this would not be sensible unless the contract expressly allowed for this as part of the dispute resolution mechanism.

If a supplier were to use such threats to extract more money from a customer, the customer could potentially have a claim for economic duress. This claim might be available under English law if:

- as a result of an illegitimate position taken by the supplier;
- the customer pays money to the supplier or incurs loss or expense; and
- for commercial and economic reasons, the customer had no other option.

Factors that the court will consider are whether the supplier's conduct was an actual or threatened breach of contract, whether the supplier acted in bad faith, whether the customer had any realistic practical alternative and the customer protested at the time and confirmed or sought to rely on the contract.

Managing Outsourcing Disputes

In the event a dispute were to arise, certain steps should be considered at the outset to preserve the usual remedies:

- Expressly reserving the right to terminate, so that any steps taken in the meantime cannot be construed as a waiver or affirmation;
- Preserving documents/data needed to prove the claim;
- Setting up a paper trail showing the evolution of the dispute, while at the same time, avoiding the creation of sensitive documents that may need to be disclosed;
- Ensuring access to witnesses, a concern where key personnel leave during the course of the dispute or where witnesses are consultants who are under no obligation to cooperate;
- Recording costs incurred in connection with the dispute, including management time; and
- Taking sensible steps to mitigate losses.

Outsourcing disputes can be costly to resolve and the costs are front loaded to a large extent. Some of the reasons for this are:

- The disputes tend to be complex, with no quick and easy solution;
- Dispute resolution clauses tend to be multi-layered;
- A detailed investigation is needed to identify the cause of the dispute and who is at fault;
- Disputes around interpretation of the contract are inherently uncertain;
- Legal advice is needed to assess the legal merits of the dispute, identify options to resolve the dispute and to formulate a strategy;
- Steps need to be taken to minimise the risk that remedies will be lost or prejudiced and to ensure recovery is maximised;
- Outsourcing projects generate a lot of documentation, much of which will need to be reviewed by lawyers; and
- Technical expert assistance is often needed to assist in the investigation and pursuit of any claim.

A key means of controlling costs is to ensure there is flexibility to use different processes to resolve different issues in dispute. Each process can be tailored to keep the costs incurred to a reasonable level. For example:

- Time limits can be imposed on the parties in terms of making and responding to claims and resolving the dispute informally;
- Limits can be imposed on the length of written submissions; and
- If a form of expert determination is used, a decision could be given on a document only basis or following a very short oral hearing.

Conclusion

In the best relationships, outsourcing proceeds well, with each party feeling comfortable that they are being treated fairly. In other cases, disputes arise that are complex, costly and difficult to resolve. These disputes can put the outsourcing relationship at risk, threaten the customer's business and take up valuable management time.

Both parties have an interest in minimising uncertainty in their relationship and avoiding disputes, or if disputes arise, in rationally resolving them as quickly and as amicably as possible.

If sufficient attention is paid to clarity at the time the contract is entered into, if the risks and potential causes of failure are managed carefully throughout the contract and if potential disputes are addressed when trouble first appears, the chances are that disputes can be avoided altogether or resolved without too much difficulty. ◆

Benchmarking: Alternative Methodologies to Ensure Cost Transparency

David Bates
Megan Paul

David Bates
London
+44 20 3130 3429
dbates@mayerbrown.com

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

Benchmarking is used to compare the performance and pricing of the services provided by one vendor against those provided by other vendors on a like-for-like basis. It provides a customer with the opportunity to determine whether a vendor's charging methodology is in line with market standards and, if not, to seek changes that should ordinarily result in decreased charges to the customer and/or a more efficient, or higher quality, delivery of service.

Benchmarking is often heavily negotiated during the contracting phase, as vendors may be reluctant to agree to such a provision within the contract. Customers want to retain control of spending and ensure that the price they are paying is competitive with that paid by the rest of the market. Vendors, however, may be aware that their pricing is uncompetitive, or may feel that they have a unique and/or an innovative service or manner of delivery that makes it impossible for the customer to find an appropriate like-for-like comparative service. It's where these latter circumstances are genuine that benchmarking may not be suitable and an alternative may need to be considered.

Historically, benchmarking has been negatively perceived. It has been used as an unfair negotiation tool to artificially drive down costs. Critics of the mechanics cite the difficulty in finding a true like-for-like comparative structure and argue that the process should not just focus on costs.

It can also signify "the beginning of the end," to the extent there is (or was) a collaborative working relationship between customer and vendor. A customer is unlikely to invoke a benchmarking procedure where it is satisfied with the pricing charged (as well as the efficiency of the services being received) and, as a result of the level of transparency of charging and information sharing, trusts that it is receiving competitive market pricing and performance from its vendor.

A Transparent Pricing Methodology

A customer-friendly alternative to benchmarking is the inclusion of transparent pricing methodologies. The more information the customer has in relation to the services received, the method of delivery and the associated costs, the better equipped it will be to understand how the services are priced and whether, in fact, it is receiving market-competitive pricing. The use

of consultants can be invaluable in assessing this information, and customers are becoming more accustomed to challenging vendors where the information is not forthcoming, or where other vendors are capable of providing more comprehensive data. In these instances, customers may favor a fixed-fee pricing structure using a cost-plus methodology to ensure certainty and pricing transparency.

Automatic Downward Adjustment

Where agreements are of relatively short duration—i.e., lasting only for a couple of years, or perhaps one-year rolling terms—the parties may agree that there would be no value in taking considerable time to benchmark the service or any part of them. In such circumstances, the customer is unlikely to spend time negotiating a benchmarking provision where it has no intention of ever relying on it. However, that does not mean that the customer should be satisfied with the charges remaining the same for the duration of the term. In these instances, a customer could consider negotiating an automatic downward adjustment based on certain triggers, such as the customer maintaining an agreed minimum volume over a period of months, or the vendor failing to reach certain service levels in a given period. Such automatic downward adjustments can also apply on any extension or roll-over of the term.

Automatic Renegotiation

In the same way that automatic downward adjustments favor short-term contracts, an automatic renegotiation of the charges based on "new" information received by the customer can be a useful mechanic in longer-term contracts. Where a vendor has been providing service for a number of years, it should be familiar with the customer's infrastructure and the efficiency of its service delivery should increase, causing costs to comparatively reduce.

At the start of the term, the parties may wish to agree that there will be an automatic renegotiation of the charges prior to any contract renewal. For example, one year before an agreement expires, a customer may seek to leverage management information provided by the vendor to reduce costs in exchange for a service term extension, thereby preventing the vendor from holding its services to "ransom" at the expiry of the term. Locking-in the expectation of a price renegotiation on renewal should help the customer have a better negotiation platform to ensure competitive pricing going forward.

Directors Certificate

In some instances, vendors may believe that their pricing is competitive in situations where they are utilizing a non-standard service packaging or delivery methodology as a means to differentiate themselves within the marketplace. In these circumstances, a like-for-like benchmarking may not be possible given the vendor's unique approach.

> The absence of a formal, contractual benchmarking process in an agreement should not prevent a customer from undertaking an informal benchmarking exercise.

One alternative to what could be viewed as an unfair and unreasonable benchmarking exercise is to have the vendor's chief financial officer (or other senior corporate officer) confirm to the customer in writing on the commencement of the agreement that the pricing it is offering the customer is competitive with that offered by the vendor to similar customers for equivalent services. That certificate is then renewed and reissued every contract year. This can be a powerful tool, as no senior corporate officer should sign such a statement if known to be false. However, we would usually only recommend relying on such a statement where the vendor is a large, well-known vendor. Similarly, a senior corporate officer is only likely to be willing to put pen to paper in this way for large, multinational customers.

Informal Benchmarking

The absence of a formal, contractual benchmarking process in an agreement should not prevent a customer from undertaking an informal benchmarking exercise. An informal benchmarking exercise differs from the formal approach in the following principal characteristics: it is conducted solely by the customer based on information obtained by it; there is no role for the vendor, or requirement that it assist with the benchmarking process; and there are no automatic consequences or other contractual processes for dealing with the outcome of the benchmarking exercise. Despite this lack of vendor participation and contractual process for dealing the consequences of the exercise, we have seen informal benchmarking results prove to be a powerful tool in the context of renegotiation discussions. The results can also have significant weight in ongoing governance discussions.

Conclusion

Benchmarking is unlikely to fall out of practice, but it is not always appropriate, and alternatives should be considered. The right to benchmark should not be viewed as a negative tool to break down vendors. Drafted and implemented in a reasonable and fair manner, benchmarking should be utilized as frequently as necessary to ensure its effectiveness.

Benchmarking can be costly and time consuming for the customer, so the consequences should have legal implications or there is little point in conducting the exercise.

Benchmarking can be costly and time consuming for the customer, so the consequences should have legal implications or there is little point in conducting the exercise. Market standards anticipate that any adjustments to fees be downward only and that the costs of the exercise be shared between the parties unless the pricing variance to "market" is shown to be in excess of a certain pre-agreed threshold, at which point, the vendor would be expected to cover the full cost of the benchmark exercise.

However, where benchmarking is inappropriate due to the nature, cost or duration of the services, or where a benchmark cannot be agreed to, the methodologies set out above may be alternatives that can be used to help ensure that costs are both transparent and reasonable. ◆

Legal Issues in Contracting for SMAC Services

Brad L. Peterson
Paul J.N. Roy

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

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

This article is a scan of key legal issues for companies sourcing what are popularly called SMAC: an acronym for Social media, Mobile computing, "big data" Analytics and Cloud computing. SMAC service providers deliver insights that sell products, increase efficiency, improve outcomes and otherwise generate value by capturing the digital exhaust from social media interactions and mobile devices and then analyzing that digital exhaust with specialized software powered by cloud computing engines.

The convergence of the SMAC technologies is having a revolutionary impact on business, creating enormous opportunities for those that embrace them and serious risks for those that fail to do so, or that overlook the legal pitfalls that SMAC technologies introduce. While the full ramifications of SMAC services in any area or industry are not yet known, we do know that SMAC and the big data output from SMAC services have, and will continue to have, a substantial disruptive effect on businesses and, as with other major shifts in technologies, some companies will be winners and others will be losers.

None of these SMAC services is entirely new. For example, credit reporting agencies have for many decades generated insights for lenders by using powerful computer systems to analyze the digital exhaust of transactions by consumers in various locations. The difference now is in the recent, extraordinary growth in volume, variety and velocity of the data being generated and analyzed, and the stunning reductions in the cost of doing so. Statistics abound. For example, IBM estimates that 90 percent of the data ever stored was stored in the last two years.[1]

Laws written before these SMAC technologies and capabilities existed are ill-designed to address some of the risks from SMAC services. Similarly, many companies are unprepared to deal with the issues that evolved along with these technologies. Our goal in this article is to help identify those legal issues and associated risks and to provide recommendations on how to be among the winners in the SMAC revolution.

Reduce Restrictions on Your Rights to Use Data

When your company wants to use, analyze and commercialize data gathered in the course of its business, will it have the rights to do so under its contracts? There are a number of traps that can block a company's right to use the data, including confidentiality and intellectual property provisions and restrictions on use of data. Some of these restrictions may be in signed contracts, but others may

be in your company's own publicly stated privacy policies. We recommend reviewing your contracts and stated policies now to reduce the risk that old provisions will restrict use or analysis rights that will be important for your company as you increase your use of SMAC services.

Reduce Data Value Leakage and Increase Data Value Gains in Supplier Contracts

With the broad expansion of third-party service contracts, ranging from full outsourcing of IT and business process functions to SMAC services, there is a risk that the rights to valuable data generated about your company's business could be forfeited to service providers, or that you could enable service providers to gather and use the most valuable insights from the data. We recommend reviewing your service provider contracts and forms and developing provisions for addressing data rights and licenses to preserve value for your company. In addition, we recommend considering your prospective service providers as a valuable source of data and analytics as a result of their provision of similar services for others, and making that a part of the value measures you will be evaluating in choosing service providers generally.

Protect Your Databases

Intellectual property protections for data and insights vary by country. The laws in European countries confer IP rights in databases but also give protections to individuals, referred to as data subjects, to obtain information about, and in some cases require the removal of, their data in your databases. EU laws also limit the use and transfer of personal data, though these restrictions do not apply to anonymized data. These IP rights in databases, as well as the data subject rights, do not exist in the United States, which instead relies on a patchwork of federal and state laws to protect data rights and the privacy of individuals.

Consequently, the protection of competitively sensitive information data in the United States relies on practical security protections and trade secrecy laws. Unlike copyright protection in the United States, trade secret laws (which vary by state) require that the data actually be secret, and that it be subject to reasonable measures to preserve that secrecy in your company's handling of that data and in the contracts that enable access of that data to any third party. In some cases, it may be more practical to use these protections for the distilled, integrated or analyzed data and insights resulting from SMAC analytics.

As is common with new technologies, enthusiasm for the possible value of SMAC services runs ahead of caution about the risks. There are a host of technical issues in distinguishing between insights and errors, including the accuracy of the data and the proper interpretation of correlations found in the analysis.

With the variety of laws across countries and the rapid expansion of SMAC services, managing data protection and compliance with laws in an international economy is becoming increasingly challenging.

Caution in Applying Results of Analysis

As is common with new technologies, enthusiasm for the possible value of SMAC services runs ahead of caution about the risks. There are a host of technical issues in distinguishing between insights and errors, including the accuracy of the data and the proper interpretation of correlations found in the analysis. There are also reputational and legal risks associated with errors, particularly when used to make decisions that affect individuals or customers.

Errors are a real problem. A recent study found material errors in 26 percent of the 1,000 consumer credit reports analyzed, these being problems serious enough to affect consumers' credit scores.[2] While consumer credit agencies are protected against liability under the Fair Credit

Reporting Act, so long as they comply with its requirements, other users of SMAC data do not enjoy the same statutory protections against errors.

Even if the data and insights are accurate, actions taken based on the insights could still violate laws. A recent Reuters news article reported that an upcoming White House report will focus on concerns about how big data technologies "could end up reinforcing existing inequities in housing, credit, employment, health and education."[3] There are numerous possibilities where social media activities or mobile device locations could be profitably correlated with business decisions but result in historically disadvantaged groups facing further disadvantages. We likely will see new laws and expanded interpretations of existing laws that make companies liable for activities that today appear permitted by law.

Due to the risk of errors in SMAC data and analysis, and the increasing regulatory attention paid to these issues, lawyers should ensure appropriate compliance oversight when using and applying the output of SMAC data. This compliance oversight should focus not merely on current laws, but on avoiding harm that might later be found to result in legal liability.

Risks in Amassing Big Data

If you read the business and IT press, you come away with the conclusion that more data is always better than less data. Legally, however, that conclusion is less clear. Privacy laws have minimization standards requiring that personal data not be retained longer than the period of its usefulness and not be used for unintended purposes. The cost of a data breach depends on the amount and value of data. Similarly, the cost of electronic discovery is directly proportional to the amount of relevant electronically stored data.

Also, the more data your company has, the harder it will be to argue that you did not have reason to know of product defects and other dangers, potentially increasing the range of foreseeable harm.

For these reasons, companies should pay careful attention to their data retention policies. You may find that those policies were written before you began collecting data generated by social media and mobile devices, and, thus, require an update. You might find that you can materially reduce risk without materially reducing value by anonymizing data, though it is becoming increasingly difficult to anonymize data in a way that cannot be de-anonymized by combining it with other available databases.

Conclusions

You can help your company succeed in our evolving economy through smart contracting for SMAC services. However, to mitigate the risks while delivering the value of SMAC services, we recommend that you review your contracts to secure the data rights you need, protect data with contractual, operational and legal defenses, and manage the legal risks that can come with amassing SMAC data and acting on the findings gleaned from that data.

Endnotes

1 John Marshall School of Law Information Technology & Privacy Law Journal, Vol XXX, Prism & European Union's Data Privacy Protection, p. 230; see also Joe Pappalardo, NSA Data Mining: How It Works, *Popular Mechanics* (Sept. 11, 2013).

2 How the Fair Credit Reporting Act Regulated Big Data by Chris Jay Hoofnagle; Future of Privacy Forum, September 10, 2013, Stanford Law School, The Center for Internet and Society.

3 How While House looks at how 'Big Data' can discriminate, Reuters Mobile, April 26, 2014, reporting by Roberta Rampton; http://www.reuters.com/article/idUSBREA3Q00M20140427.

Privacy Updates

Rebecca S. Eisner
Lei Shen

Rebecca S. Eisner
Chicago
+1 312 701 8577
reisner@mayerbrown.com

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

Privacy and data security have become increasingly critical topics, making it even more important for companies to remain up to date on global privacy developments. In this article, we provide an overview of some of the privacy and data security developments that have taken place in 2014.

Data Breaches

There have been several high-profile data breaches since the beginning of 2014, which have received increased coverage due to heightened sensitivity after Target's breach in late 2013. Affected organizations include retailers such as Michaels and Neiman Marcus, hospitals such as St. Joseph Health System and universities such as the University of Maryland. Due to the varied ways in which the data was compromised from each organization, the cyber attacks do not appear to be part of a coordinated breach campaign.[1] The hackers have usually been very sophisticated and have used methods such as targeting a company's vendor or giving their malware a nearly identical name to common software used by a company (e.g., its payment software) to increase the likelihood that any resulting security alerts would be disregarded.[2]

In response to these breaches, a number of US senators have proposed new federal data breach notification laws, including the Personal Data Privacy and Security Act, the Data Security and Breach Notification Act, and the Personal Data Protection and Breach Accountability Act. As of the date of this writing, none of these laws have been passed; however, both the US Attorney General and the Federal Trade Commission have urged Congress to pass a federal data breach law.[3]

Cybersecurity

In the United States, two cybersecurity guides were released in February 2014. Though not mandatory, they do offer good policies for companies to consider.

In response to President Barack Obama's Executive Order 13636[4] from last year, the National Institute of Standards and Technology (NIST) released the final version of its voluntary cybersecurity framework on February 12, 2014, titled "Framework for Improving Critical Infrastructure Cybersecurity."[5] The Framework urges banks, utilities and operators of other critical infrastructure to adopt the Framework's set of industry standards and best practices to manage their cybersecurity risks. While the Framework is aimed at critical infrastructure, organizations of any size or degree of cybersecurity sophistication are able to use the Framework as a guideline to assess their existing cybersecurity program or to build one from scratch.

The California Attorney General also issued a cybersecurity guide in February. Unlike the Framework, this guide is targeted toward small businesses rather than critical infrastructure. The guide, titled "Cybersecurity in the Golden State,"[6] urges small businesses to take steps such as encrypting sensitive data and developing an incident response plan to protect against cyber intrusions. It offers "specific and straightforward" recommendations to help businesses better protect against and respond to the increasing threats of malware, data breaches and other cyber risks.

Lawsuits

Two companies, LabMD and Wyndham Hotels, have recently challenged the Federal Trade Commission's (FTC) authority to enforce data security. The FTC had charged both companies with "unfair and deceptive acts and practices" due to their data security practices.[7] Both companies responded by disputing whether the FTC has the authority to regulate data security, especially since there is no definitive legal security standard for the FTC to enforce. Both companies were unsuccessful in their challenges. LabMD closed its doors in January, blaming the FTC enforcement action, and a New Jersey district court recently denied Wyndham's motion to dismiss, stating that there is "binding and persuasive precedent" upholding the FTC's authority to enforce data security.[8]

In the United States and several other jurisdictions, a number of new laws and amendments were passed in early 2014.

With the increasing number of data privacy and security breach-related lawsuits, the courts have been split with regard to whether actual injury is required in order to have standing in such lawsuits. For example, a Kansas federal judge dismissed two proposed class actions related to a data breach at Nationwide Mutual Insurance Company, stating that there was no evidence that anyone had been harmed.[9] A Florida judge, on the other hand, approved a class action settlement involving AvMed, Inc.'s, breach that resulted in the release of 1.2 million sensitive records from encrypted laptops, even though the class members may not have experienced identity theft or actual financial harm.[10] Similarly, in a decision against Spokeo Inc., the US Court of Appeals for the Ninth Circuit held that the plaintiffs did not need to allege actual injury to demonstrate standing.[11]

New Laws

In the United States and several other jurisdictions, a number of new laws and amendments were passed in early 2014.

California amended several of its privacy laws. It amended its data breach notification statute[12] by expanding the definition of "personal information" to include data elements that permit access to an online account (e.g., user name and/or email address in combination with a password). This change now makes data breaches that do not compromise traditional sensitive financial information subject to its data breach notification law. California also amended its California Online Privacy Protection Act (CalOPPA)[13] to require websites to tell visitors how they respond to "Do-Not-Track" signals from web browsers, and enacted the Privacy Rights for California Minors in the Digital World law (effective January 1, 2015), which gives minors the right to erase content they post on websites.[14]

Kentucky enacted a data breach notification statute, H.B. 232, in April 2014, making it the 47th state to enact such a law. Prior to its enactment, Kentucky was one of four states (including Alabama, New Mexico and South Dakota) that did not have data breach notification legislation. H.B. 232 is similar to other states' data breach notification statutes but differs in that it also protects student data in the cloud by prohibiting cloud service providers from selling, disclosing or otherwise processing such data for any commercial purpose.

Australia and Canada each had significant privacy developments. In Australia, the Office of the Australian Information Commissioner issued the final iteration of the Australian Privacy Principles (APPs), which became effective on March 12, 2014.[15] The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 also became active. It gives the Australian Privacy Commissioner the right to seek civil penalties of up to $340,000 for individuals and $1.7 million for businesses in cases of serious breaches. The APPs and the Privacy Amendment apply to both public and private organizations.

CASL is far broader and more punitive than the CAN-SPAM Act (the US anti-spam law), and it does not deal solely with email "spam."

In Canada, certain provisions in Canada's Anti-Spam Law (CASL) become effective starting this year.[16] The provisions governing commercial electronic messages (CEMs) will become effective on July 1, 2014; the provisions governing unsolicited installations of computer programs will become effective on January 1, 2015; and the private right of action provisions will become effective on July 1, 2017. CASL is far broader and more punitive than the CAN-SPAM Act (the US anti-spam law), and it does not deal solely with email "spam." The new law applies to all CEMs sent to instant message and social network accounts and by short message service (SMS) texts to cell phones, and also regulates the installation of computer programs. When the new law is fully in force, it will apply to all CEMs sent from, or accessed by, a computer system located in Canada, thereby governing CEMs that are sent from other countries, including the United States. ◆

Endnotes

1 See Danny Yadron, Cyberattacks on Retailers Not 'Coordinated,' Says FBI, The Wall St. J. Law Blog (Feb. 10, 2014), http://blogs.wsj.com/law/2014/02/10/cyberattacks-on-retailers-not-coordinated-says-fbi/.

2 See Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data, Bloomberg Businessweek (Feb. 21, 2014), http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data.

3 See Prepared Statement of the Federal Trade Commission on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches before the United States Senate, Mar. 26, 2014, available at http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf.

4 Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity (Feb. 19, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

5 NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST.gov (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

6 Cybersecurity in the Golden State (Feb. 2014), available at https://oag.ca.gov/cybersecurity.

7 See, e.g., FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy, http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

8 *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.*, Civil Action No. 13-1887 (D.N.J. Apr. 7, 2014).

9 *Galaria v. Nationwide Mutual Insurance Co.*, Case No. 2:13-cv-118 (N.D. Ohio) and Hancox v. Nationwide Mutual Insurance Company, Case No. 2:13-cv-257 (N.D. Ohio).

10 See *Curry v. AvMed, Inc.*, No. 10-cv-24513, available at http://www.databreachsettlement.com/docs/sa.pdf.

11 *Robins v. Spokeo Inc.*, Case No. 11-56843 (9th Cir.).

12 Cal. Civ. Code § 1798.82.

13 Cal. Bus. and Prof. Code §§ 22575-22579.

14 See SB-568, available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

15 See Australian Privacy Principles, Australian Government – Office of the Australian Information Commissioner, http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles.

16 S.C. 2010, c. 23, available at http://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html.

A Recap of 2013 by the Privacy Commissioner of Hong Kong and Strategic Focus for 2014

Gabriela Kennedy
Eugene Ito Low

Gabriela Kennedy
Hong Kong
+852 2843 2380
gabriela.kennedy@
mayerbrownjsm.com

Eugene Ito Low
Hong Kong
+852 2843 4572
eugene.low@
mayerbrownjsm.com

The year 2013 proved to be a significant milestone in the development of data privacy in Hong Kong. One of the most important changes was the commencement of new statutory provisions regulating direct marketing on 1 April 2013. The year was also significant because of the record high number of enquiries and complaints received by the Privacy Commissioner of Hong Kong. This increase reflects the public's growing concern for data privacy and underscores the belief held by the Privacy Commissioner that all organisations need to treat this subject seriously. This article provides a summary of the Privacy Commissioner's Annual Report for 2012/2013 and his report to the Legislative Council on work carried out by his office in 2013. The article concludes with the strategic focus of the Privacy Commissioner for 2014.

Record-High Number of Enquiries and Complaints

In 2013, the Privacy Commissioner received a total of 24,161 enquiries and 1,792 complaints, a record high in both categories since the commencement of the Personal Data (Privacy) Ordinance, ("Ordinance") in 1996. Interestingly, over half of the enquiries related to the new provisions in the Ordinance, which tightened the requirements for use of personal data for direct marketing. A massive spike of enquires occurred in April and May 2013 right after the new direct marketing provisions came into force on 1 April 2013.

New Statutory Provisions on Direct Marketing

The introduction of the new statutory provisions on direct marketing in April 2013 was one of the most important changes to the data privacy regime in Hong Kong since the enactment of the Ordinance. In essence, the new provisions tighten control over the use of personal data in direct marketing by requiring data users to clearly explain the scope of their intended direct marketing use and obtain explicit consent (as opposed to implicit consent obtained by silence or non-response) from data subjects before they can use or transfer the personal data for direct marketing activities.

The introduction of the new statutory provisions on direct marketing in April 2013 was one of the most important changes to the data privacy regime in Hong Kong since the enactment of the Ordinance.

Under the new regime, data subjects are also entitled to opt out of or withdraw their consent for further direct marketing use of their personal data at any time. Failure to comply with these new requirements consti-

tutes a criminal offence punishable by a maximum fine of HK$500,000 and imprisonment for up to 3 years; if the data is transferred for gain to a third party for use in direct marketing, non-compliance with the new requirements may result in a maximum fine of HK$1 million and 5 years' imprisonment. A transitional "grandfathering" arrangement was introduced to exempt the use of personal data collected prior to 1 April 2013 from these new requirements, provided that certain conditions had been met, such as that the data users had collected and used such personal data for the same direct marketing purposes before 1 April 2013.

Another important amendment to the Ordinance which came into force on 1 April 2013 was the introduction of the "Legal Assistance Scheme." The Scheme aims to provide legal assistance to aggrieved individuals to lodge civil proceedings against data users who are in breach of the Ordinance so as to seek compensation from the data user for damage, including injury to feelings.

In 2013, since the new provisions came into force, 14 cases were referred to the Police for potential prosecution for suspected contraventions of the new direct marketing requirements.

Legal Assistance for Civil Claims

Another important amendment to the Ordinance which came into force on 1 April 2013 was the introduction of the "Legal Assistance Scheme." The Scheme aims to provide legal assistance to aggrieved individuals to lodge civil proceedings against data users who are in breach of the Ordinance so as to seek compensation from the data user for damage, including injury to feelings. The legal assistance may take the form of legal advice, mediation and legal representation in court. The Scheme is administered by the Privacy Commissioner.

In 2013, the Privacy Commissioner received 16 applications for legal assistance under the Scheme and granted assistance to one applicant.

Increasing Enforcement Efforts

Thirty-two warnings and 25 enforcement notices were issued in 2013 — more than double the number of enforcement notices (11) issued in 2012. This increase is a direct result of the enhanced power of the Privacy Commissioner to issue enforcement notices pursuant to the amendments to the Ordinance in 2012. The Privacy Commissioner also conducted more compliance checks and self-initiated investigations in 2013. In particular, the Privacy Commissioner focused its efforts on promoting data privacy compliance in the field of information and communications technologies ("ICT"). The Privacy Commissioner conducted a survey of smartphone applications developed by Hong Kong entities which revealed that their privacy policies were generally inadequate. The Privacy Commissioner advised smartphone application developers to make improvements on data privacy compliance (an information leaflet was issued by the Privacy Commissioner in November 2012 to highlight the privacy implications that mobile applications developers and operators should consider in connection with designing and developing mobile applications).

In 2013, the Privacy Commissioner also received reports of more than 60 data breach incidents affecting 90,000 individuals. These incidents were either made known to the Privacy Commissioner through voluntary notifications from the data users or through reports from the media and the general public.

Strategic Focus for Year 2014

The Privacy Commissioner has made clear that his strategic focus for 2014 will be on:

- The privacy issues associated with the increased use of ICTs and mobile applications;

- Promoting the adoption of privacy management programs for organisations to embrace data privacy protection as part of their corporate governance; and
- Assisting the government in reviewing the regulatory issues concerning cross-border flows of personal data.

The Privacy Commissioner has taken active steps to pursue each of these objectives. In August 2013, the Privacy Commissioner published an investigation report on a smartphone application called "Do No Evil" (which compiled individuals' litigation and bankruptcy data from public sources and allowed users to make searches against targeted individuals), finding that the application seriously invaded data privacy. An enforcement notice was issued against the developer.

The Privacy Commissioner commented that global data flows are prevalent and integral to many businesses today and it is very important for the government to bring into force Section 33 as soon as possible to preserve and enhance Hong Kong's status as an international financial centre and data hub.

Recognising the shift from compliance to accountability, the Privacy Commissioner published a "Best Practice Guide on Privacy Management Programme" on 18 February 2014. The aim of this Guide is to encourage businesses to proactively embrace personal data protection as part of their corporate governance responsibilities rather than merely look at it as a legal compliance issue. As of 18 February 2014, the Hong Kong government (including all bureaux and departments), together with 25 companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors have pledged to implement the Best Practice Guide.

In relation to the regulation of cross-border flows of personal data, the Privacy Commissioner recognised that Section 33 of the Ordinance provides a very comprehensive framework regulating the transfer of personal data outside Hong Kong. The current framework set out in Section 33 prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances, namely, the place has been specified by the Privacy Commissioner as one which has in force a data protection law which is substantially similar to, or serves the same purpose as, the Ordinance, and that the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be handled in a manner tantamount to a contravention of a requirement under the Ordinance. However, Section 33 has not been brought into force since the enactment of the Ordinance in 1995 and the government has no timetable for its implementation. The Privacy Commissioner completed in 2013 a survey of 50 jurisdictions and provided the government with a list of places that have in force data protection laws that are substantially similar to, or that serve the same purpose as, the Ordinance. The Privacy Commissioner commented that global data flows are prevalent and integral to many businesses today and it is very important for the government to bring into force Section 33 as soon as possible to preserve and enhance Hong Kong's status as an international financial centre and data hub.

Conclusion

This year looks to be a busy year again for the Privacy Commissioner. Enforcement of the Ordinance is likely to continue apace and while the plan to bring into force the Data User Return has been shelved for now, the Privacy Commissioner is keen to promote the Privacy Management Programme and will likely take steps to bring into force Section 33 of the Ordinance. ◆

Best Practices on NFC Mobile Payments Issued in Hong Kong

Gabriela Kennedy
Karen H.F. Lee

Gabriela Kennedy
Hong Kong
+852 2843 2380
gabriela.kennedy@
mayerbrownjsm.com

Karen H.F. Lee
Hong Kong
+852 2843 4452
karen.hf.lee@
mayerbrownjsm.com

This article was previously published in Bloomberg BNA in its *World Data Protection Report*, Vol. 14, Number 1 – January 2014

Near field communication ("NFC") mobile payment services are on the rise in Hong Kong, and they are offered in many retail outlets as a payment method. To facilitate the growth of such technology, while balancing the security concerns of the public, the Hong Kong Association of Banks ("HKAB") in consultation with the Hong Kong Monetary Authority ("HKMA"), has recently issued a Best Practice on NFC Mobile Payments in Hong Kong ("Best Practice"). The Best Practice is intended to provide the minimum security requirements and other best practices for the development of NFC mobile payments in Hong Kong.

Background

NFC mobile payment services are already offered in Hong Kong by, among others, HSBC, Hang Seng Bank and the Bank of China. The Octopus Group is also set to introduce NFC mobile payments as an alternative to its widely popular Octopus card, and Jetco recently announced that it will team up with several banks to build an NFC mobile payment platform. With the growing popularity of NFC mobile payments, concerns have arisen as to the security and infrastructure of this new payment method.

In March 2013, the HKMA released the results of a consultancy study that was aimed at identifying an effective NFC mobile payment structure designed to achieve the following four, long-term development objectives for NFC mobile payments:

- The ability of users to use multiple payment services from different banks and service providers on a single NFC-enabled mobile phone;
- The continuity of payment services despite users switching to different mobile network operators;
- The continuity of payment services despite users changing phones; and
- A high-level of security that is consistent with international standards and regulatory requirements.

One of the recommendations of the study was to develop a set of standards and guidelines that dealt with the implementation of NFC mobile payment services in Hong Kong. To achieve this goal, the HKMA established an NFC task force under the HKAB to formulate the standards and guidelines in consultation with the HKMA. On 25 November 2013, the Best Practice was issued by the HKAB.

The Best Practice

The Best Practice applies to banks that are members of the HKAB, as well as to other stakeholders of mobile payment services, including mobile network operators, phone manufacturers, etc. The Best Practice covers three areas: security requirements, technical standards and operational processes.

Security Requirements

The security requirements are the minimum security requirements that must be implemented. They cover the security of the back end infrastructure, the front end device and software applications installed on the mobile phone. They include, among other things, the following:

- **Management of Secure Elements** — NFC payment credentials must be adequately segregated from each other by creating secure domain structures and hierarchies.
- **Card Issuance and Provisioning** — measures must be implemented to ensure that the connections and data within the NFC environment are secure.
- **Mobile Payment Services Management:**
  - » **Mobile Wallets** — a mobile wallet, which is the software application installed by a customer onto their handset, acts as an interface to manage the NFC services in the secure environment. The safety and security of a mobile wallet is essential.
  - » **Management of Multiple Payment Credentials** — measures should be implemented to ensure that access controls and authentications in the secure element are put in place, so that only authorised mobile wallet applications can access the assigned payment credentials stored in the secure element.
  - » **Authentication Codes** — mobile wallets must include PIN protection, which should be stored inside the secure element. Customers may be given the option of turning this PIN protection off, but the default position should always be for the PIN protection to be on.
  - » **Access to Sensitive Information** — access to sensitive information should only be allowed upon correct PIN entry. Sensitive information should also be adequately segregated where the mobile wallet has multiple NFC payment credentials linked to different issuers. Measures should be implemented to ensure that access to and use of transaction data is restricted to the authorised end-user or the entity that owns the data.
- **Payment Transactions:**
  - » **Audit Trail and Record** — effective procedures and audit trails must be implemented to prevent and detect any unconfirmed transactions. Refunds should promptly be made upon the detection of any unconfirmed transactions.
  - » **Transactions through Contactless Interface** — all payment transactions should only be allowed via contactless interfaces, unless effective security measures have been put in place to prevent any potential attacks through a contact interface.
  - » **Transaction Limit** — NFC mobile credit card payments should be restricted to the same transaction limit that applies to no-signature contactless credit card payments. This is currently set at HK$1,000 per transaction. For transactions that are higher than the current limit, additional security measures must be in place, e.g., provision of a PIN.
- **Cardholder Authentication:**
  - » **Know Your Customer** — the existing KYC due diligence process for normal payment card products should be followed in order to identify the customer. This is mandatory for financial institutions.
  - » **At Service Activation** — cardholder authentication is mandatory during the activation process. The activation process involves the installation of the mobile wallet application on the phone, and the insertion of the customer's

payment credentials into the application. If an activation code is used as part of the authentication process, then the activation code should be given through a different means than the one used to activate the service, e.g., via SMS.

» **Mobile Pin Management** — mobile PIN's should be used in the NFC mobile payment service.

The HKMA will take the Best Practice security requirements into account during its continual supervision of NFC mobile payment services offered by authorised institutions, to ensure that they maintain a high level of security.

Technical Standards

For the technical standards, the aim was to establish principles with reference to industry and international standards in order to assist in the interoperability of different NFC infrastructures, mobile devices and terminals. As such, the Best Practice requires the adoption of widely accepted standards set by industry and international organisations. This includes the ISO standards, ETSI standards, GlobalPlatform standards and EMVCo standards.

The HKMA is clearly focused on developing the legal structure in relation to retail payment systems (e.g., mobile payments, stored value payment facilities, etc.) in order to protect the public and, in so doing, inspire consumer confidence, which will help further promote the use of new innovative payment methods. While the Best Practice is only a guideline, and does not have the force of law, it may not be long before other measures come into place.

Operational Process

The Best Practice introduces a standardised operational process in order to improve user experience. For example, the Best Practice recommends that for transactions that exceed the current limit of HK$1,000, and where additional authentication is therefore required, a mobile PIN should be adopted as the method for additional verification.

Other Developments

The HKMA is clearly focused on developing the legal structure in relation to retail payment systems (e.g., mobile payments, stored value payment facilities, etc.) in order to protect the public and, in so doing, inspire consumer confidence, which will help further promote the use of new innovative payment methods. While the Best Practice is only a guideline, and does not have the force of law, it may not be long before other measures come into place.

In May 2013, the HKMA and Financial Services and the Treasury Bureau released for public consultation a proposal on the introduction of a regulatory regime for stored value facilities and retail payment systems in Hong Kong. In brief, under the proposed regime:

- All issuers of multipurpose stored value facilities ("SVF") in Hong Kong (whether device or non-device based) would be required to obtain a licence from the HKMA before issuing the SVF;
- Issuers of multipurpose SVFs would be required to keep the float separate from its own funds, which must be fully protected by safeguard measures; and
- The HKMA would have the power to designate certain retail payment systems which would be subject to the HKMA's continuous oversight.

The consultation period ended on 22 August 2013, and a bill is expected to be introduced to the Legislative Council in the first half of 2014 for its consideration. ◆

DAVID BATES

Partner

David Bates is a partner in the London office of Mayer Brown's Corporate practice. He has extensive experience advising clients on all aspects of corporate transactional work, including international and domestic mergers and acquisitions as well as private equity and venture capital transactions. In addition, David also has significant experience in large domestic and international outsourcing transactions.

PETER DICKINSON

Partner

Peter Dickinson is head of Mayer Brown's Corporate group in the UK and a Firm Practice Leader in Mayer Brown's global corporate and securities practice. Peter's practice focuses on mergers and acquisitions, joint ventures and other significant commercial transactions including, in particular, large-scale multijurisdictional outsourcing projects.

REBECCA EISNER

Partner

Rebecca Eisner, a partner in our Chicago office and serves on Mayer Brown's Partnership Board. She focuses her practice on technology and business process outsourcing and sourcing, information technology transactions, privacy and security. Her experience includes complex global technology, licensing and business process outsourcing transactions, including IT infrastructure and licensing, cloud computing, applications development and maintenance, back office processing, ERP implementations, finance and accounting, payroll processing, call center, HR, technology development, system integration and hosting. She regularly advises clients in Internet and e-commerce law issues, complex data protection and data transfer issues, privacy compliance issues and electronic contracting and signatures. She is a frequent writer and speaker on outsourcing, cloud computing and privacy and data protection topics. Additionally, she is the co-chair of the Data Security Chapter of the International Association of Outsourcing Professionals.

GABRIELA KENNEDY

Partner

Gabriela Kennedy is the head of the Asia IP and TMT group at Mayer Brown JSM based in Hong Kong, practicing intellectual property, media, information technology and telecommunications law. She handles the full spectrum of intellectual property work, including litigation, licensing, strategic advice and portfolio management. Gabriela advises extensively on data protection issues in Hong Kong and throughout Asia, particularly in relation to business processing outsourcing, the cross-border transfer of data, data compliance and data breaches. She has handled a number of data breach complaints filed with the Privacy Commissioner in Hong Kong and has conducted in-depth data audits and drafted/devised privacy manuals and procedures for the Asia operations of a number of multinational companies. On the information technology side, Gabriela's particular focus includes advising on complex IT transactions and projects, IT outsourcing, cloud-computing, mobile payments, smart card projects, the regulation of encryption technology, software licensing and disputes stemming from failed IT projects.

RANI MINA

Partner

Rani Mina is a partner in the London office of Mayer Brown's Litigation & Dispute Resolution practice. She focuses on clients in several areas in which Mayer Brown has sector strength: banking and finance, mining, energy and business and technology sourcing (in particular, IT project and outsourcing). She also has wide experience of acting for companies, corporate trustees, directors and shareholders, private equity funds and joint ventures in complex litigation and international arbitration.

BRAD PETERSON

Partner

Brad Peterson, a partner in our Chicago office, focuses on business process and information

technology outsourcing, joint ventures, strategic alliances and information technology transactions. Brad has represented customers in dozens of large outsourcing agreements with, cumulatively, over $10 billion in contract value. He has represented clients in all major types of outsourcing transactions and has negotiated opposite all of the first-tier and most of the second-tier providers. 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.

PAUL J.N. ROY
Partner

Paul J.N. Roy is a partner in our Business & Technology Sourcing practice in Chicago. He represents clients in a broad range of information technology and business process transactions, including technology development, implementation, support and outsourcing transactions. He regularly advises clients on 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 sourcing of finance and accounting functions, HR/employee services, CRM and financial services operations, among other business process functions.

KAREN LEE
Associate

Karen Lee is an associate in the Intellectual Property, Technology, Media and Telecommunications practice of Mayer Brown JSM in Hong Kong. She mainly handles non-contentious intellectual property, technology and media matters. Karen is experienced in drafting and negotiating outsourcing agreements and IT related contracts. Karen has also advised on data protection issues in Hong Kong and has drafted personal data privacy guidelines and personal information collection statements for various multinational companies and Hong Kong based clients.

EUGENE LOW
Senior Associate

Eugene Low is a senior associate in the Intellectual Property, Technology, Media and Telecommunications practice of Mayer Brown JSM in Hong Kong. He handles a wide range of contentious and non-contentious IP/IT work in Hong Kong and in the PRC, covering copyright, trademark, patent, passing off, domain name, etc. Apart from traditional IPs, Eugene also advises on privacy, data protection and security, cyberworld issues, technology transfer and licensing, as well as sports, gaming and entertainment matters.

MEGAN PAUL
Senior Associate

Megan Paul is a senior associate in the Corporate & Securities practice in our London office. She undertakes a broad spectrum of transactional corporate and commercial work, focusing primarily on international and domestic outsourcing transactions, private equity and venture capital transactions and private mergers and acquisitions. Megan has represented clients in multijurisdictional 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.

LEI SHEN
Senior Associate

Lei Shen is a senior associate in the Business & Technology Sourcing practice in Mayer Brown's Chicago office. Lei focuses her practice on privacy and security, technology and business process outsourcing (including information technology, finance and accounting, procurement, and human resources) and information technology transactions.

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.

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