

# Global Sourcing & Technology Changes: Reboot Your Sourcing Strategies

May 8, 2014

GLOBAL SOURCING AND TECHNOLOGY CHANGES:

Reboot Your Sourcing Strategies

- 1,500 Lawyers in the Americas, Europe and Asia
- More than 50 lawyers around the world focused on Business & Technology Sourcing
- Advised on more than 300 significant outsourcing transactions valued at more than \$100 billion
- Recognized Market Leader



- “Top tier” ranking in IT/Outsourcing for nine consecutive years (*Chambers 2004-2012*)



- Sole occupant of the top Outsourcing ranking for the US in 2009 and ranked again in the top tier for 2010 and 2011



- Ranked as one of the top law firms in 2009, 2010 and 2011 on The World's Best Outsourcing Advisors list for The Global Outsourcing 100™

# Our BTS Team in North America

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



**Rebecca Eisner**  
Partner



**Geoffrey Master**  
Partner



**Daniel Masur**  
Partner



**Brad Peterson**  
Partner



**Paul Roy**  
Partner



**Linda Rhodes**  
Partner



**Kevin Rang**  
Partner



**Derek Schaffner**  
Counsel



**Paul Chandler**  
Counsel



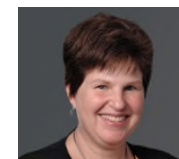
**Robert Kriss**  
Partner - Litigation



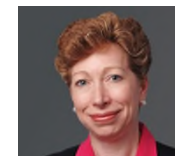
**Jason Bazar**  
Partner - Tax



**William Knull**  
Partner - Litigation



**Marcia Goodman**  
Partner - Employment



**Kim Leffert**  
Counsel - Litigation

# Our BTS Team in South America

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



**Guilherme Vieira**  
Partner



**Salim Saud**  
Partner



# Our BTS Team in Asia

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



**Rosita Li**  
Partner



**Gabriella Kennedy**  
Partner



**Duncan Abate**  
Partner - Employment & Benefits

# Our BTS Team in Europe

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



**David Bates**  
Partner



**Peter Dickinson**  
Partner



**Serge Levine**  
Partner



**Mark Prinsley**  
Partner



**Andrew Stewart**  
Partner



**Guido Zeppenfeld**  
Partner



**Laurence Dumure Lambert**  
Partner - Employment & Benefits



**Nicholas Robertson**  
Partner - Employment & Benefits



**Miles Robinson**  
Partner - Litigation-Dispute Resolution



**Rani Mina**  
Partner - Litigation-Dispute Resolution

MAYER • BROWN

# Talking SMAC: Contracting for Social, Mobile, Analytics and Cloud

Paul Roy

*Partner*

Mayer Brown LLP

+1 312 701 7370

[proy@mayerbrown.com](mailto:proy@mayerbrown.com)

Brad Peterson

*Partner*

Mayer Brown LLP

+1 312 701 8568

[bpeterson@mayerbrown.com](mailto:bpeterson@mayerbrown.com)

GLOBAL SOURCING AND TECHNOLOGY CHANGES:

## Reboot Your Sourcing Strategies

# Speakers

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



**Paul Roy** is a partner in the Business & Technology Sourcing practice in Mayer Brown's Chicago office. He 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.

---



**Brad Peterson** is a partner in the Business & Technology Sourcing Practice in our Chicago office. He has represented clients in dozens of large outsourcing transactions and hundreds of software license and services agreements. In the past year, he has represented leading companies in entering into mission-critical agreements for information technology, finance & accounting and human resources services and in replacing critical information technology. With both an MBA from the University of Chicago and a JD from Harvard Law School, he provides practical, business-focused advice and completes transactions efficiently and effectively.

# Agenda

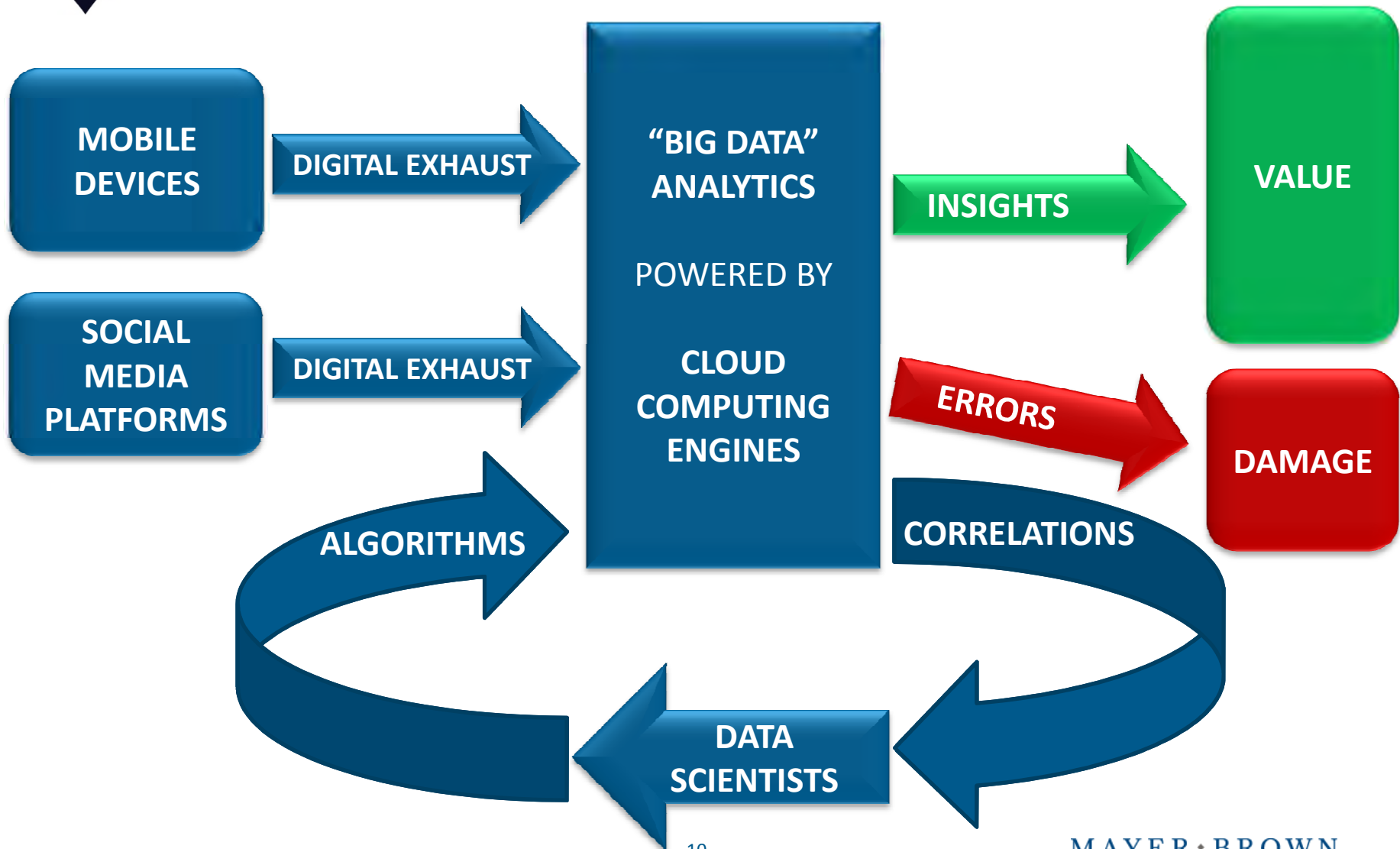
GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- How the confluence of SMAC technologies creates revolutionary new value
- How to help your company maximize value
- How to help your company avoid legal pitfalls



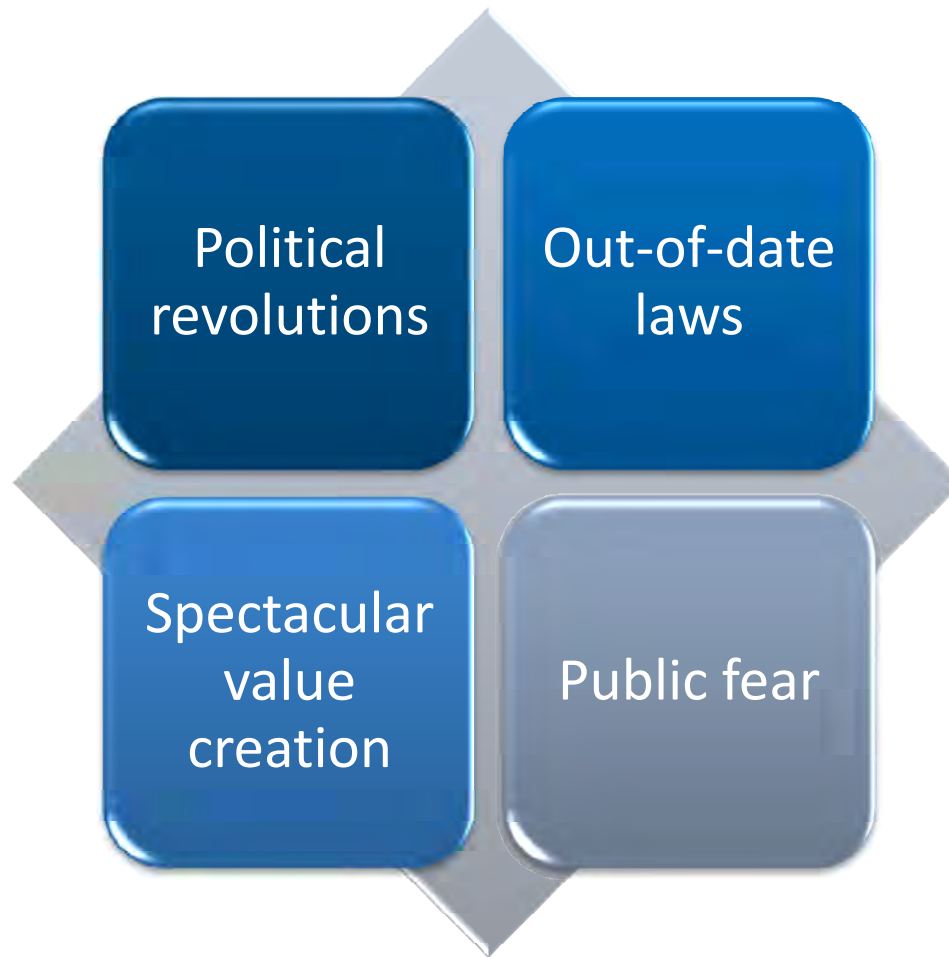
# How SMAC Technologies Combine to Create Value

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



# The Confluence of the SMAC Technologies is Truly Revolutionary

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



# HOW TO HELP YOUR COMPANY TO MAXIMIZE VALUE

# A Cautionary Tale

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

“For example, in Amazon’s early days it signed a deal with AOL to run the technology behind AOL’s e-commerce site. To most people, it looked like an ordinary outsourcing deal. But what really interested Amazon, explains Andreas Weigend, Amazon’s former chief scientist, was getting hold of data on what AOL users were looking at and buying, which would improve the performance of [Amazon’s] recommendation engine. Poor AOL never realized this. It only saw the data’s value in terms of its primary purpose — sales. Clever Amazon knew it could reap benefits by putting the data to a secondary use.”

*From Big Data: A Revolution That Will Transform How We Live, Work, and Think*  
Viktor Mayer-Schonberger and Kenneth Cukier (Houghton Mifflin Harcourt, 2013), p. 105.

# Recommendation: Update Your Contract Clauses To Protect Your Interests in SMAC Data and Insights

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Value may be generated in a form that is not protected by traditional contract clauses
- Review contract templates and standards to guard against value leakage. For example:
  - Designate your data as trade secret *and* as Confidential Information *and* as Customer Data
  - Remove, narrow, or apply royalty rates to exceptions such as:
    - Secondary use, of your data
    - Use “to improve our services”
    - Use of “anonymized” data or data consolidated across customers
    - Information available from other sources



# Recommendation: Obtain Options on Data/Insights

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Providers are rapidly developing their available services and types and sources of data
- Obtain options to:
  - Continue using data that you need, including right to provide that data to outsiders for data analysis, license fees, etc.
  - Obtain copies of other data in provider's possession
  - Obtain access to new data streams or analytical tools when implemented by the provider
  - Learn findings from provider's analysis of aggregated data including your data
  - Continue use of SMAC services that you may depend on
  - Prevent changes in services that may harm you or reduce value

# Recommendation: Use Reasonable Measures to Protect Secrecy of Your Valuable Data and Insights

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Unlike Europe, the US does not offer statutory protection to databases except as trade secrets
- Designating data or insights as trade secrets in a contract is helpful but not sufficient
- Trade secret laws require that the data and insights to be protected are actually secret and subject to reasonable measures to preserve their secrecy
  - This legal standard may be impractical operationally or factually for some key types of data
  - Consider using instead for particularly valuable data and insights

# Recommendation: Use Incentive-based Sourcing Strategies to Drive Value Creation by Providers

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



## Current key challenges in contracting for SMAC services

- Difficulty in specifying outcomes
- Difficulty in specifying skills
- Difficulty in specifying activities
- Rapidly evolving technology and laws

## Sourcing strategies

- Ongoing multi-provider competitive model
- Gain share or other outcome-based model
- Agile sourcing model

# HOW TO HELP YOUR COMPANY AVOID LEGAL PITFALLS

# A Cautionary Tale

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

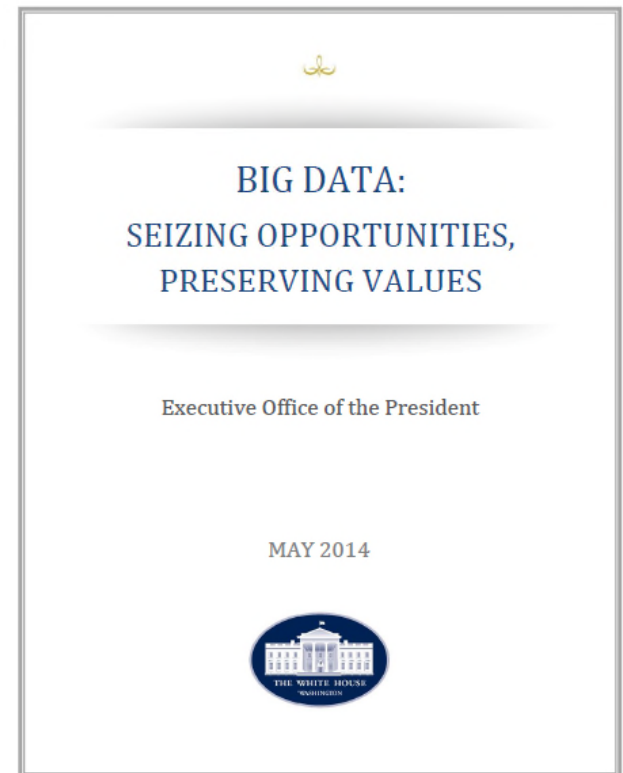
- For over 100 years, credit reporting agencies (CRAs) have analyzed data about borrower behavior to develop credit scores. Prior to regulation, much of that data was more moralistic than directly related to credit.
- The Fair Credit Reporting Act of 1970 defined “permissible uses” of consumer credit information, required that data be verifiable, and gave consumers access and correction rights. By complying with these safeguards, CRAs were shielded from defamation suits.
- Despite long experience, cleaner data than social media postings and oft-amended regulation, a recent landmark study found that 26% of credit reports have errors substantial enough to affect credit scores.



# Recommendation: Obtain Compliance Commitments

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Regulations and market norms are also evolving rapidly
  - A White House report on May 1, 2014 concluded that “The federal government must pay attention to the potential for big data technologies to facilitate discrimination inconsistent with the country’s laws and values.”
- Obtain rights to:
  - Audit and obtain reports on uses of your data
  - Know the basis for recommendations, including sources of data and types of algorithms
  - Prevent use of your data by others without your consent (and perhaps adequate license fees)
  - Stop uses of your data that are prohibited by regulations or your policies (as each may change)



# Recommendation: Flow Down Privacy Obligations to Providers

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- SMAC technologies create new issues and concerns in:
  - Informed consent
  - Access /participation
  - Anonymization/de-identification
  - Do Not Target
  - Legitimate business purposes
  - Data minimization
  - Profiling
- Update your contracts to require your providers to be consistent with your compliance strategies

# Recommendation: Continue to Destroy Appropriate Data as Part of Your Records Retention Policy

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Your big-data enthusiasts will say that it is always better to retain more data because you will find more secondary uses as time goes on
- However, more data may impose more legal burdens, such as:
  - Expense of preservation and production in discovery
  - Expense of complying with contractual and legal obligations to protect and limit use of that data
  - Increased liability for product defects or other safety problems because more harms are arguably foreseeable
  - Risk of privacy or data security breaches and related regulatory actions and consumer class actions

# Recommendation: Carefully Allocate Liability for Potential Harm

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

The law isn't clear on allocation or extent of SMAC liability, making it hard to size the risks when contracting and expensive to resolve disputes when they occur

SMAC providers often seek broad liability waivers

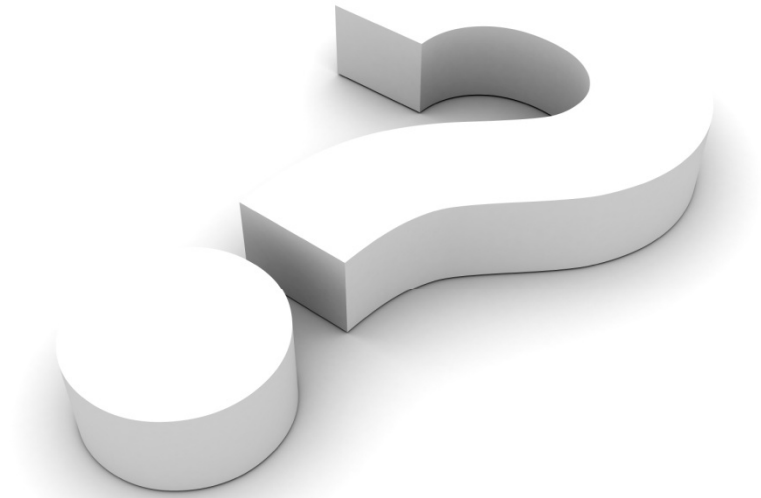
Identify and allocate risks such as:

- Collection or retention of data in violation of law or contract
- Improper or unwanted disclosure of data
- Inaccurate, incomplete or misleading data
- Incorrect analysis or recommendations
- Use of analysis and recommendations

- The confluence of social media, mobile devices, “big data” analytics and cloud computing engines is generating new value and new risks.
- There’s a lot you can do right now to capture value and mitigate risks, including:
  - Reviewing and improving contract clauses to reduce restrictions on your use of data and secure options and commitments from providers
  - Establishing trade secret or other protection
  - Updating policies



# QUESTIONS



**Paul Roy**

*Partner*

Mayer Brown LLP

+1 312 701 7370

[proy@mayerbrown.com](mailto:proy@mayerbrown.com)

**Brad Peterson**

*Partner*

Mayer Brown LLP

+1 312 701 8568

[bpeterson@mayerbrown.com](mailto:bpeterson@mayerbrown.com)

# Foreign Corrupt Practices Act Compliance

Lori E. Lightfoot

*Partner*

+1 312 701 8680

llightfoot@mayerbrown.com

GLOBAL SOURCING AND TECHNOLOGY CHANGES:

## Reboot Your Sourcing Strategies



**Lori Lightfoot** has extensive experience in every facet of complex commercial litigation in areas ranging from breach of contract and business tort claims; franchisor/franchisee disputes; foreclosure actions and other real estate related litigation; and products liability actions. Lori also has litigated or otherwise resolved disputes concerning employment discrimination, particularly class actions or those involving senior executives. Lori regularly advises clients on avoidance of and preparation for potential litigation. Lori also regularly advises clients on a range of complex criminal law issues stemming from federal, state or local grand jury investigations or investigations by federal, state or local inspectors general.

# Agenda

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Overview of the FCPA
- Trends in FCPA Enforcement
- Risk Management



## What is the FCPA?

The Foreign Corrupt Practices Act (FCPA) makes it a crime to bribe foreign government officials, either directly or through intermediaries, in order to obtain or retain business. The FCPA also imposes record-keeping obligations on certain companies.

# Why the FCPA?

- As a result of SEC investigations in the mid-1970s, over 400 US companies admitted making questionable or illegal payments in excess of \$300 million to foreign government officials, politicians, and political parties.
- The abuses ran from bribery of high foreign officials, to paying the expenses of family members, to making smaller, regular payments to lower-level officials.
- Congress enacted the FCPA in 1977 to halt bribery of foreign officials and to restore public confidence in the integrity of the American business system.

- The FCPA consists of two sections:
  - 1) Anti-bribery Provisions
  - 2) Record-Keeping and Internal Control Provisions
- US Department of Justice (“DOJ”) and the Securities and Exchange Commission (“SEC”) work in conjunction to enforce the FCPA, both separately and in combined efforts.



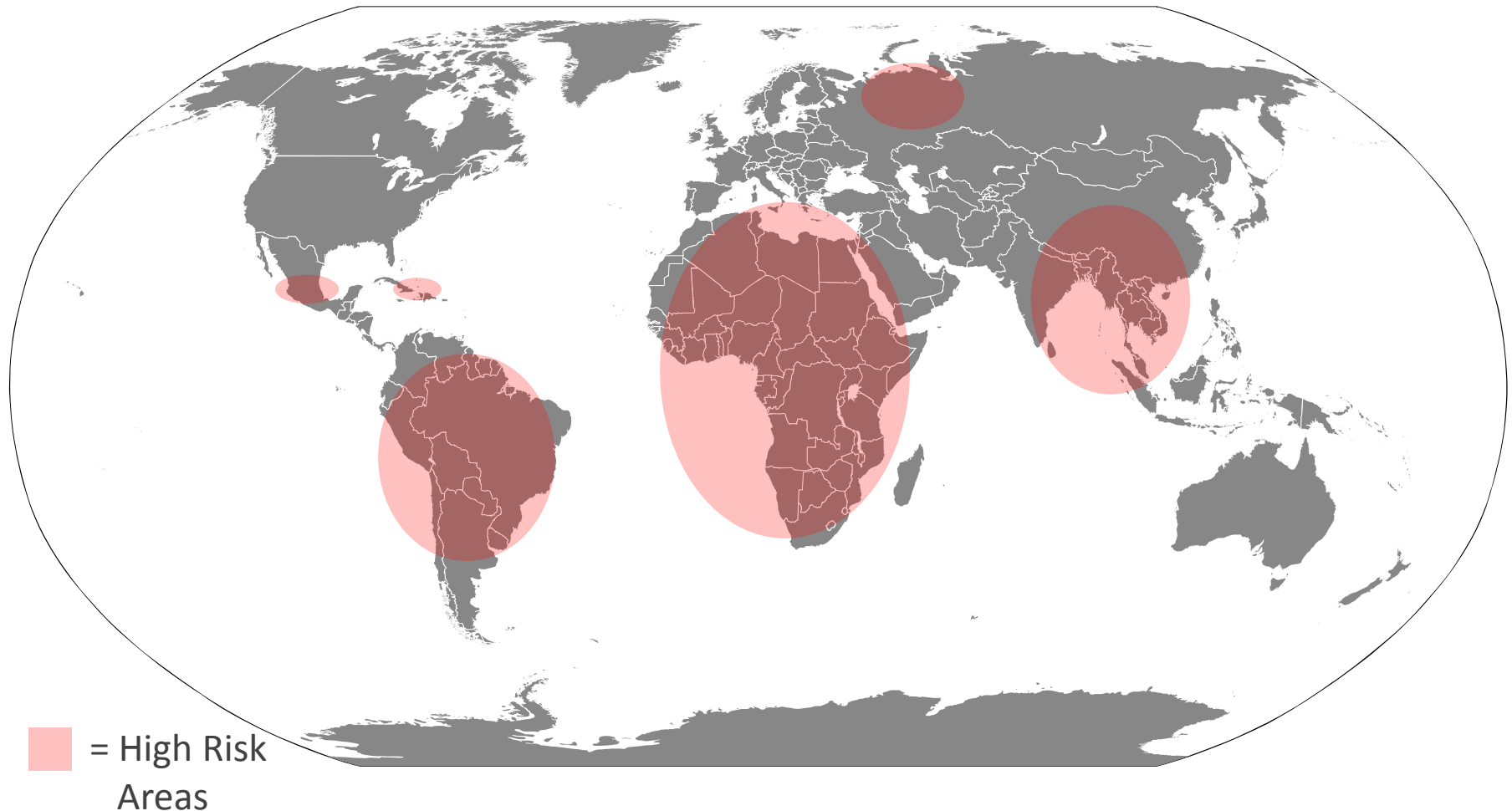
# FCPA: Anti-Bribery Provisions

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The anti-bribery provisions of the FCPA make it unlawful for a US person, a company with ties to the US and for most foreign companies who are issuers of US securities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business, or for directing business to any person.

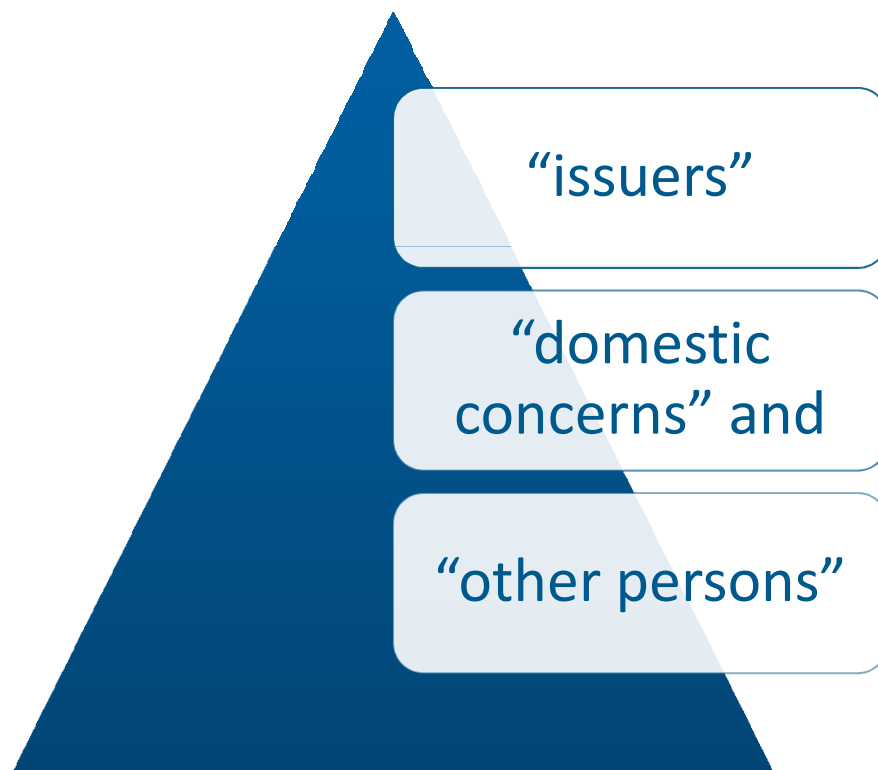
# FCPA Corruption Perception Index Risk

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



# To Whom Does the FCPA Apply?

The FCPA's anti-bribery provisions apply to three categories of companies or persons:



...as defined under the statute.

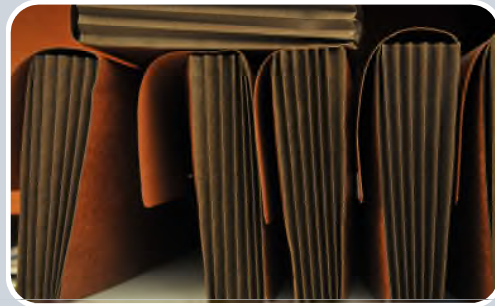
# FCPA: Anti-Bribery Provisions

## Who is an “Issuer”?

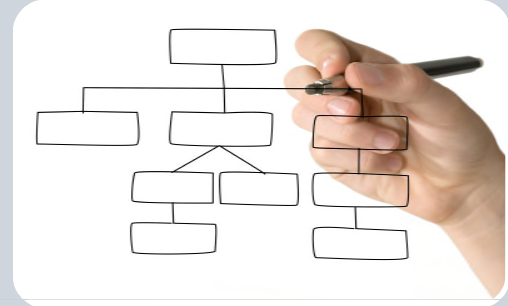
GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



All companies  
with US  
publicly  
registered  
securities



All companies  
required to file  
reports with  
the SEC



All the officers,  
directors,  
employees and  
agents of those  
companies

# Who is a “Domestic Concern”?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



All US Citizens
All US nationals
All US residents and non-issuer businesses with a principal place of business in the US or that are organized under US law

All US Citizens

All US nationals

All US residents and non-issuer businesses  
with a principal place of business in the US  
or that are organized under US law

## Who are the “other persons” to Whom the FCPA Applies?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The Act also applies to foreign firms and persons (“other persons”) who are neither issuers nor domestic concerns, but who take any act in furtherance of the corrupt payment while within the territory of the United States.

# Bribery — What Acts are Covered?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- For a specific act to be considered an illegal bribe under the FCPA anti-bribery provisions, there needs to be adequate proof of:
  - Payment
  - Foreign Official Recipient
  - Corrupt Intent
  - Business Purpose





# Corrupt Payments

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The FCPA prohibits paying, offering, promising to pay (or authorizing to pay or offer) money or anything of value.
- “Anything of value” can include paying for trips or hotel rooms, meals, promises of future employment, loans, entertainment expenses, etc.



# FCPA Covers Direct and Indirect Payments

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The FCPA does not just prohibit direct transactions. It also prohibits corrupt payments through intermediaries.
- Intermediaries may include suppliers or their subcontractors or agents. It is unlawful to make a payment to a third party, while knowing that all or a portion of the payment will go directly or indirectly to a foreign official.
- The offer or promise of a corrupt payment can constitute a violation (the corrupt payment need not actually be made).

# Who is a Foreign Official?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Officer or employee of a foreign (i.e. non-US) government or agency, member of a political party, party official, legislator or candidate
- Member of royal family who has official governmental responsibilities
- Employee of state-controlled business (such as a doctor in a state-controlled hospital or employees at state-owned airports)
- Business person who is a government agent acting on behalf of the government
- A public international organization as well as its employees (UN, IMF, etc.)
- The official's rank is not significant, focus is on the payment's purpose not duties

## **Practice Point:**

In many countries, the line between “public” and “private” may be blurred so be careful.

# Compliance Point: Political Donations Prohibited

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Because officials, political parties, and even candidates for office are considered “Foreign Officials,” no company funds, assets, or personnel should be used to make any political donation, or render assistance to any party or candidate for office.
- For example, use of company office space for a political meeting would be prohibited.
- Similarly, charitable donations are only permitted after they are cleared through an approval process.  
*Guidelines at Section 6.0.*

# Anti-Bribery – Corrupt Intent

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- To constitute a “corrupt payment” under the FCPA, the person offering or authorizing the payment must have a “corrupt intent” and the payment must be intended to induce the recipient to misuse his or her official position to affect a decision by a government institution or employee to secure an improper advantage or to assist in obtaining, retaining, or directing business to anyone.

# Anti-Bribery – Corrupt Intent

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- A person may be liable under the FCPA if he knows a corrupt payment will be made to a foreign official.  
“Knowledge” includes:
  - Actual knowledge
  - Awareness or suspicion that an event is likely to occur
  - Avoiding actual knowledge of corrupt acts through willful blindness
  - In other words, you can’t “play dumb.”

# Anti-Bribery – Corrupt Intent

## Practice Point:

The FCPA prohibits corrupt payments through intermediaries. It is unlawful to make a payment to a third party, while “knowing” that all or a portion of the payment will go directly or indirectly to a foreign official.

**Remember:** The term “knowing” includes “conscious disregard” and “deliberate ignorance.”



# Anti-Bribery – Corrupt Intent

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



**"That's all I know, because it was at precisely that moment that I pulled the wool over my eyes."**

# FCPA - Business Purpose

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The FCPA prohibits payments made in order to assist the firm in obtaining or retaining business, or directing business to, any person.
- The Department of Justice interprets “obtaining or retaining business” broadly, such that the term encompasses more than the mere award or renewal of a contract. The Act prohibits payments for the purpose of obtaining “any improper advantage” in obtaining or retaining business such as waivers and licenses.
- The business to be obtained or retained does not need to be with a foreign government or foreign governmental authority.

# Facilitating Payments: Defined

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The FCPA does not prohibit “facilitating payments for routine governmental action.” Facilitating payments are also known as “grease payments.”
- “Grease payments” can be thought of as small payments to persuade low-level government officials to perform functions or services which they are obliged to perform as part of their governmental responsibilities, but which they may refuse or delay unless compensated.

## **Practice Point:**

“routine governmental action” does not include any decision by a foreign official to award new business or to continue business with a particular party.

# Facilitating Payments: Examples

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

are ordinarily  
and commonly  
performed by  
a foreign  
official:

- Approving permits, licenses, or other official documents
- Processing papers such as visas and work orders
- Providing police protection, mail pick-up and delivery or scheduling inspections associated with contract performance or transit of goods
- Providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products

# Compliance Point: Facilitating Payments

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Smart Company Policy should require employees and business partners to obtain prior written approval before making any facilitating payment.

**NOTE:** While the FCPA contains an exception for Facilitating Payments, other countries' laws do not. (UK Bribery Act; Chinese law).

# Reasonable and Bona Fide Business Expenses

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The Act permits payment of reasonable businesses expenses, such as travel and lodging if the expenses are:
  - Related to the promotion, demonstration, or explanation of products and services, or
  - The execution or performance of a contract with a foreign government.
- Gifts are permitted under the FCPA, but only if they are reasonable and not given as a *quid pro quo* to get or retain business.

## Additional Affirmative Defenses

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The payment was lawful under the written laws of the foreign country; or
- The money was spent as part of demonstrating a product or performing a contractual obligation.
- An affirmative defense requires that a defendant show that the payment met these requirements.



# Indirect Payments Are NOT Protected

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

The FCPA also prohibits corrupt payments made through third parties or intermediaries. Thus, you can't do through someone else what you are prohibited yourself from doing.



# Overview of Record-Keeping Requirements

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The FCPA requires every issuer to “make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect the transactions and disposition of assets.”

# Overview of Accounting Control Requirements

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The FCPA also requires issuers to maintain a system of internal accounting controls sufficient to provide reasonable assurances that:
  - 1) transactions are executed in accordance with management's general or specific authorization;
  - 2) transactions are recorded as necessary;
  - 3) access to assets is permitted only in accordance with management's general or specific authorization; and
  - 4) the recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken w/r/t any differences.

These rules codify existing auditing standards.

## Compliance Point: Policies on Record Keeping and Internal Accounting Controls

- Company Guidelines should specify how books and records must be kept for all suppliers, subsidiaries and affiliates both in the US and abroad.
- Guidelines should identify examples of prohibited record keeping activities that must be reported immediately, such as:
  - False expense reports
  - “Slush funds” or other unrecorded petty cash funds
  - Misabeled expenditures

# Ultimate Risks: Serious Criminal and Civil Penalties

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

## Corporate sanctions:

- **Heavy fines** (up to \$2 million for each violation of the anti-bribery prohibition, up to \$25 million for violation of accounting provision, or up to twice the benefit sought to be obtained) and disgorgement of proceeds associated with improper payments
- Injunction to prevent future violations
- Suspension and debarment

## Individual Liability

- Heavy fines up to \$100,000 (No indemnification allowed)
- Prison sentences up to five years

## Collateral Consequences

- Damage to reputation, recession of contracts, loss of government licenses or business with the federal government

# How FCPA Issues Can Arise In Outsourcing

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

As discussed, FCPA issues can arise in a number of ways, including:

- Direct bribery to government officials
- Indirect bribes to government officials (via agents or third parties)
- Negotiations related to licenses or waivers
- Renegotiation of government contract terms
- Marketing of products or services to government agencies

## FCPA Prosecutions Continue to Rise; FCPA Remains High Government Priority

- The number of FCPA prosecutions has increased significantly since 2004, and has remained high in recent years.

YEAR	2009		2010		2011		2012		2013	
AGENCY	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC	DOJ	SEC
# OF PROSECUTIONS	26	14	48	26	23	25	11	12	19	8

- Prosecutions grew both of companies and persons in the US and those abroad.
- Do no misinterpret smaller numbers in 2012 and 2013.



# Principles for Due Diligence

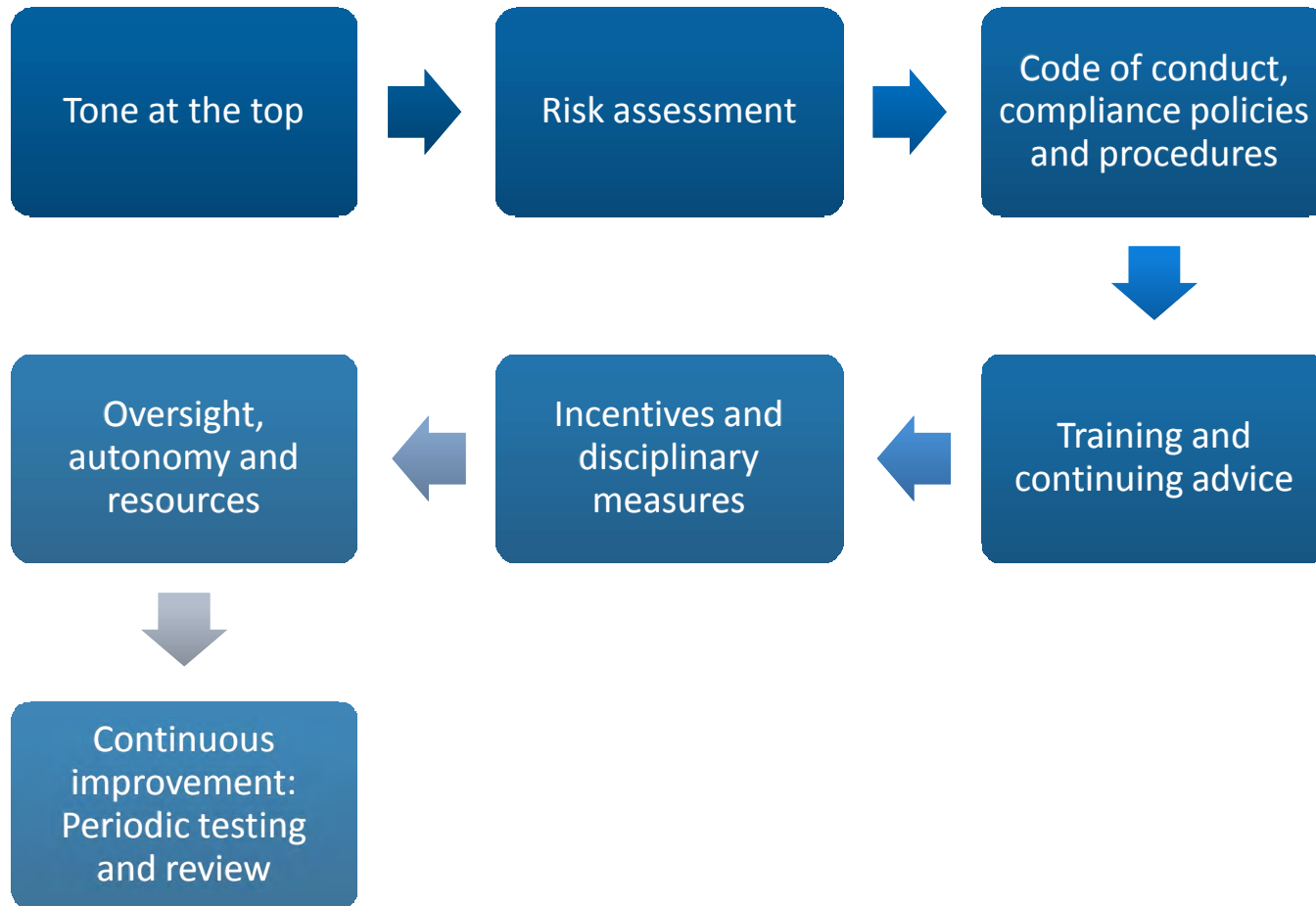
GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

The Guidance issued by DOJ & SEC in November 2012 set forth three guiding principles for conducting important due diligence, which are acknowledged risk areas for companies.

- 1) Qualifications and associations, including reputation and relationships with foreign officials;
- 2) Business Rational for the use of the supplier;
- 3) Continuously monitor the relationship, exercising audit rights, training and requiring certifications.

# Elements of a Successful Compliance Plan








GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



# Due Diligence – Risk Assessment

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

The level of due diligence is always a balance based upon risk assessment. Certain geographic areas of the globe have always been known to have a more significant risk of corruption. However, any acquisition should look at the following:

- (A) substantial revenue from government contracts; 
- (B) lack of training on FCPA; 
- (C) questionable financial statements or unexplainable expenditures; 
- (D) lack of an adequate compliance infrastructure; 
- (E) contracts involving excessive use of the same consultants; 
- (F) relationships of owners, directors, employees or consultants to foreign officials; and 
- (G) involvement with governmental agencies that appear inconsistent with economic purpose. 

# Supplier Compliance Issues

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

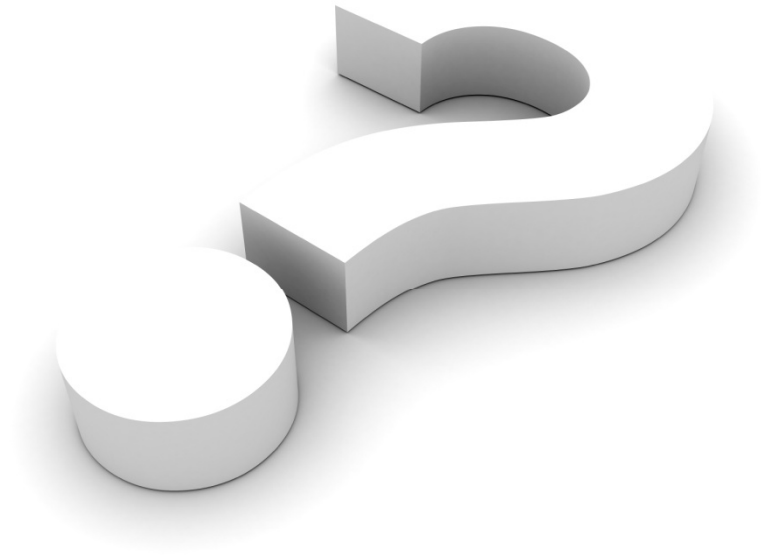
- 1) Is compliance audited for suppliers? (How?)
- 2) Is compliance training mandated for suppliers? (How?)
- 3) Suppliers disciplined for non-compliance? (How?)
- 4) What mechanisms are in place to memorialize this?
- 5) What systems are in place to check on relationships to Foreign Officials prior to and during use of suppliers?
- 6) Who manages the review of contracts with suppliers to ensure they are with reputable, pay is within industry norms, terms do not allow for "slush funds" or kickbacks?

# Supplier Compliance Issues: Risk Management

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Are reps, warranties and an indemnity from a supplier related to anti-corruption law violations enough?

# QUESTIONS



Lori E. Lightfoot

*Partner*

+1 312 701 8680

[llightfoot@mayerbrown.com](mailto:llightfoot@mayerbrown.com)

# NSA Data Collection: Your Risks and Potential Responses

Marcus A. Christian  
*Partner*

+1 202.263.3731  
mchristian@mayerbrown.com

May 2014

GLOBAL SOURCING AND TECHNOLOGY CHANGES:

Reboot Your Sourcing Strategies





**Marcus Christian** is a Washington DC partner in Mayer Brown's Litigation & Dispute Resolution practice and White Collar Defense & Compliance group. Previously, he was the executive assistant United States attorney at the US Attorney's Office for the Southern District of Florida, the third-highest ranking position in one of America's largest and busiest offices of federal prosecutors. In this role, Marcus worked on the senior management team with responsibility for the Criminal, Civil, Appellate, Asset Forfeiture and Administrative Divisions. In addition, Marcus conducted and supervised numerous investigations involving communications data analysis, electronic surveillance, and intercepted communications.

# This Presentation Will Cover

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- I. Understanding the NSA's data collection activities
- II. Assessing the risks to your company
- III. Mitigating the effect on your company of the NSA's activities

# I. Understanding the NSA's Activities

## A. Patriot Act Tools

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

### FISA Orders

Granted for intelligence agencies by Foreign Intelligence Surveillance Court on application by DOJ

For electronic and physical searches, pen registers, and certain business records; all generally regarding foreign persons or for foreign intelligence purposes

- Must meet "minimization requirements" for US person-only information

Hearings are *ex parte* and judicial opinions are classified

Authorized by FISA Amendments Act (FAA) and USA PATRIOT Act

DOJ appealed 2 FISA Order denials to FISC and several telecom companies have challenged FISA Orders

# I. Understanding the NSA's Activities

## A. Patriot Act Tools (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

### National Security Letters

Generally, FBI requests for telephone/e-mail metadata and financial/credit records

Subjects cannot disclose receipt to targeted person or other personnel not essential to fulfilling the request

Authorized by five federal statutes; Right to Financial Privacy Act, Electronic Communications Privacy Act, Fair Credit Reporting Act, Patriot Act amendments, and National Security Act

Several challenges in court, but not all documented due to gag orders

- Pending court action to prohibit use of gag orders regarding challenges

# I. Understanding the NSA's Activities

## B. PRISM

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Collects internet communications from various companies
  - 91% of 250M NSA-collected internet communications
  - Authorized by Section 702 of the FAA
- Publicized through 2013 Snowden unauthorized disclosures
  - Very controversial in parts of Europe due to privacy laws and norms
- Companies deny allowing the NSA direct access to their systems
  - Accepted that the NSA used the DOJ to obtain FISA orders that compelled the companies to turn over data to the NSA
- Interest groups have sued the government and the companies on various constitutional, administrative, and other statutory grounds

# I. Understanding the NSA's Activities

## C. Phone Records Program

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Collects the metadata of telephone calls made within the US
  - Authorized by Section 215 of the USA PATRIOT Act and supervised by the FISC
- Industry provides the government with the data and the government retains it for up to five years
- Industry was granted immunity from private lawsuits in 2007, but challenges against the government remain
- At least six lawsuits are pending challenging the constitutionality of the program
  - Lawsuits will be moot if Congress acts to terminate the program





# I. Understanding the NSA's Activities

## D. Upstream

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Intercepts telephone and internet traffic from major internet cables and switches and retains them for at least two years
  - 9% of 250M NSA-collected internet communications
  - Authorized by FISA, FAA, “Transit Authority,” and EO 12333
- Publicized through 2013 Snowden unauthorized disclosures





# I. Understanding the NSA's Activities

## E. Backdoors

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Appears to be unknown to industry
  - Weakening NIST encryption
  - Encryption companies' use of NSA tools
  - Access via advanced surveillance technologies
  - Disguising as website server
  - Maintaining collections of known weaknesses in various products
    - Use of Heartbleed exploit for two years prior to public discovery



# II. Assessing the Risks to Your Company

## A. Overview

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- The first step to preparing a response is to understand the risks
- Some risks arise from concerns regarding the integrity and confidentiality of your data (or your customers' data in your custody)
- Some risks arise from the perception that your data (or your customers' data in your custody) is vulnerable
  - Your data may not actually be vulnerable
  - Or at least, it may be no more vulnerable than most other data
  - But, negative perceptions can have serious implications

# II. Assessing the Risks to Your Company

## B. Assessing Reputational Risk

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Will NSA access (or the perception of possible NSA access) be a concern for your customers? Will customers:
  - Ask you questions;
  - Seek other providers;
  - Request new contract terms;
  - Request whole or partial refunds; and/or
  - Consider legal action?
- Will investors/shareholders be concerned?
- Senior executives and board?



## II. Assessing the Risks to Your Company

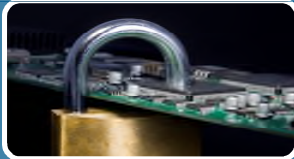
### B. Assessing Reputational Risk (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Greater concern if:



Your company's reputation is based on security, privacy, or safety (e.g., communications systems, customer information databases)



Customers can easily migrate to more secure options (e.g., short-term/retail contracts, fungible product, many small purchasers)



Your client base is sensitive to these issues, e.g., Europeans, certain retail customers, have financial, health or IP or other sensitive data at issue



Your competitors will attempt to advertise or distinguish themselves based on a “firewall” against NSA collection activities

## II. Assessing the Risks to Your Company

### C. Violation of Home Country Privacy Laws

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- If the NSA obtains your non-US customers' data, have you violated non-US privacy laws?
  - Unlikely to be an issue if NSA obtains unauthorized access
  - What about FISA Order or NSA letter to your company or your vendor?
    - Consider gag order vs. obligation in some European countries to notify certain customers before sharing data

# II. Assessing the Risks to Your Company

## D. Violation of Contractual Provisions

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Violation of contractual obligations
  - What do terms of your customer agreements say about obligations not to share data, or to give notice
  - What might you be asked to say in your contract
  - In US, contractual obligations are trumped by government obligations

## II. Assessing the Risks to Your Company

### E. Loss, Interference or Misuse of Data

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- FBI use of NSLs to obtain data has caused some data losses
  - FBI seizure of one company's servers temporarily downed unrelated websites
  - FBI seizure and return of another company's servers was done without communicating the seizure or return to the company
  - We do not view this as a large risk



## II. Assessing the Risks to Your Company

### F. Fairness

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Some companies may wish to take a stand based on concepts of fairness and commitment to privacy
  - Twitter challenged government's gag orders in court to permit it to notify users of government requests for users' information
  - CEOs of major technology companies publicly requested that the government permit them to release sanitized summaries of their responses to government requests

# III. Mitigating the NSA Effect

## A. Strategy Crafted to Specific Effects

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Your strategy should be customized to meet the NSA effects you have identified
  - Example: how one customer might evaluate risks and solutions

	Customer relations / marketing	Customer contract	Vendor contract	Vendor selection	Tech	Lit	US Gov't relations	Overall campaign
Reputational Risk	Y	Y	Y	Y	Y	Y	Y	Y
Home country law	N	?	?	?	?	Y	Y	?
Contractual breach	?	Y	Y	Y	?	?	?	?
Lawsuits	Y	Y	?	?	?	?	?	?
Data loss	N	N	Y	Y	Y	?	?	N
Fairness	N	N	N	N	N	?	Y	Y

# III. Minimizing the NSA Effect

## B. Customer Relations/Marketing

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Manage customer expectations about your ability and obligation to safeguard data
  - Some companies inform customers that customer data cannot be secured against issues like the NSA's activities
  - This aligns customers' expectations of privacy with reality
  - This has sometimes resulted in criticism/backlash

# III. Minimizing the NSA Effect

## B. Customer Relations/Marketing (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Educate customers about the nature of the risks
  - For some content, NSA not likely to be interested
  - NSA does not appear to have used information commercially
- Educate customers that moving data elsewhere may not redress their concerns
  - NSA has long reach (e.g., tapping transatlantic cables)
  - US government obtains treaty assistances
  - Other governments engage in intelligence activities for their own reasons
  - Recent court decisions, such as *Daimler*, may provide some legal comfort, but cannot prevent NSA access through cooperation with foreign intelligence agencies or its own technological tools

# III. Minimizing the NSA Effect

## B. Customer Relations/Marketing (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Broader marketing campaign
  - Can be a positive opportunity to develop and sell new products and services
  - Can be a way to differentiate from competition

# III. Minimizing the NSA Effect

## B. Customer Relations/Marketing (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Broader public relations campaign
  - Many companies have engaged in public dialogue regarding the NSA's activities, including
    - Explaining how their companies are limited in what they can disclose
    - Calls to action requesting the public be allowed to know the full extent of the NSA's activities
    - Discussion of how US interests are harmed by the resulting balkanization of critical infrastructure systems
    - Coordination of messaging with industry peers to guide public action
  - Feature other steps company is taking (industry groups, technological, litigation, government relations, etc.)

# III. Minimizing the NSA Effect

## C. Customer Contracts

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Specific provisions to consider (want to include or exclude, depending on the contract)
  - Waiver of right to notice before data is shared in response to government request
  - No mandatory use of specific encryption protocols or software
  - Waiver of claims for negligence in instances of data breach
  - Arbitration requirements for data breach issues
    - Prohibition on class arbitration
  - Express notice that customer is aware company complies with national security requests
  - Limitation of damages to those foreseeable to the company



# III. Minimizing the NSA Effect

## D. Selecting Vendors

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Moving servers or data to (1) locations outside of the US that are (2) maintained by non-US companies may reduce the NSA's ability to obtain it
  - Recent *Daimler* decision helps protect data with non-US companies that have US offices
  - Perception that data outside US is less vulnerable to NSA may be reassuring to customers and stakeholders



# III. Minimizing the NSA Effect

## D. Selecting Vendors (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Data abroad still may face risk of NSA or similar access
  - NSA may still be able to obtain access to non-US servers
  - Other governments may use the same methods as the NSA to acquire data, and may cooperate with US authorities
  - Data may still pass through the US on its way to and from customers
- Keeping data outside of the United States, and with only non-US companies, may be impractical and/or costly

# III. Minimizing the NSA Effect

## D. Selecting Vendors (cont.)

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- In Housing Options
  - No vendors = fewer potential NSA cooperators
  - Consider “private cloud” or in-house systems for critical data
    - Remember though that proprietary systems tend to have more vulnerabilities than publicly available systems
    - Consider adopting off-line/segregate implementation of publicly available system
    - Incorporate the “human factor”; employees will work-around security systems that are hard to use

# III. Minimizing the NSA Effect

## E. Vendor Contracts

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Your vendors may be cooperating with the NSA through “back-doors” in the products they sell you
- We have seen companies request certifications from their vendors
  - Certifications may be broad or narrow, depending on the concerns
  - They may require affirmative declarations or negative confirmations
  - Even seeing how the vendor responds to the request for certification can be valuable

# III. Minimizing the NSA Effect

## E. Vendor Contracts

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Requiring vendor to provide you with notice of request for your data, and to litigate against gag orders that would interfere with that obligation
  - In December 2010, Twitter received subpoenas for account information of Wikileaks-related persons with gag orders preventing notification of such persons
  - Twitter challenged the gag orders in court and won, permitting it to notify its users of the subpoenas
  - This, in turn, permitted those users to challenge the subpoenas to protect their information

# NIST Framework Compliance

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- NIST released a Framework for Improving Critical Infrastructure Cybersecurity in February 2014
- Companies can demonstrate compliance with the NIST Framework to:
  - Show their commitment cybersecurity
  - Meet minimum basic standards
- Not sufficient alone
  - NIST's Framework is not comprehensive
  - Companies may not want to be seen only doing what the government suggests they do



# Congressional Lobbying

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Many Senators and Representatives have taken public stands against the NSA's US and non-US activities
- A concerned company should engage with members
  - Who serve on its industry-specific Congressional committee or sub-committee
  - Who are from its home-state
  - Who have publicly expressed their concern with the NSA's activities in the company's industry





# Industry “Best Practices”

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Alphabet soup of security and/or privacy programs your company or its employees can become certified in (e.g., IAPP, GIAC, CISSP, etc.)
  - Identify those that your customers think are useful and relevant
  - Identify those adopted by peer companies
- Industry trade associations and conferences offer opportunities to discuss and identify best practices
  - Identify panels at annual conferences discuss privacy and security concerns
  - Attend “brown bags” on “hot topics” in data privacy
  - Participate in association committee on data privacy and security



- Some companies may proactively litigate the NSA's data collection efforts by:
  - Refusing to comply with requests for information and letting the NSA sue them in court to obtain the information
  - Filing Freedom of Information Act (FOIA) lawsuits to dissolve the confidentiality provisions of NSA requests
  - Suing the NSA for unauthorized acquisition or use of their data
    - Generally lawsuits resulting from refusals to comply with NSA requests are more effective than suing the NSA for unauthorized acquisition of data



Conclusions

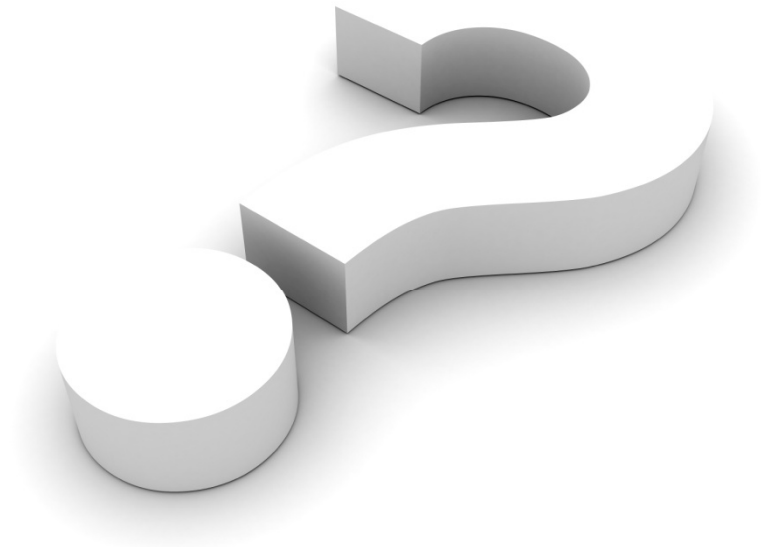
# QUESTIONS

Marcus A. Christian

*Partner*

+1 202.263.3731

[mchristian@mayerbrown.com](mailto:mchristian@mayerbrown.com)



MAYER • BROWN

# Protecting Enterprise Interests in Cloud Computing

Rebecca Eisner

*Partner*

312.701.8577

[reisner@mayerbrown.com](mailto:reisner@mayerbrown.com)

GLOBAL SOURCING AND TECHNOLOGY CHANGES:

## Reboot Your Sourcing Strategies



**Rebecca Eisner**, a partner in the Chicago office, 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 practice focuses on 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. She also regularly advises on complex data protection and data transfer issues, frequently as part of transactions, as well as privacy issues and electronic contracting and signatures.

# Agenda

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- How can you and your enterprise get ready for the cloud
- Five key areas of enterprise interests to protect in the cloud and “**watch outs**”
- How EU Data Protection developments are influencing cloud contracting

# Getting Ready: What Is Cloud Computing?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

*National Institute of Standards and Technology defines it as:*

- A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

## SERVICE MODELS

### Software as a Service

(e.g., Google Gmail, Google Docs, Facebook and Twitter)

### Platform as a Service

(e.g., Microsoft Azure, Force.com, Google App Engine)

### Infrastructure as a Service

(Amazon, Google, Rackspace, IBM, AT&T, etc.)

## DEPLOYMENT MODELS

**Private Cloud**

**Public Cloud**

**Hybrid Cloud**



# Getting Ready: What Are You Buying? Who Controls?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

Cloud Elements (Stack)	Customer IT/ITO Provider Manages	IAAS	PAAS	SAAS
Network	C	P	P	P
Storage	C	P	P	P
Server	C	P	P	P
VM	C	C/P	C/P	P
Applications	C	C	C/P	P
Data	C	C	C	C/P

C = Customer, P = Provider

# Getting Ready: Know What You Are Buying

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Terms you may hear:
  - Public, private, hybrid, dedicated, shared, multi-tenant, single tenant
  - You need to know what is dedicated (used solely for the particular customer), and what is shared (used by two or more customers)
- What elements of the “stack” are dedicated versus shared?
- Why does this matter?
  - Affects privacy, security and compliance risks
  - Affects control and transparency the customer may have
  - Affects commercial terms of the solution

# Getting Ready: Doing the Due Diligence

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



<b>Need a team</b>	<ul style="list-style-type: none"><li>• Technical/solution</li><li>• Data Security</li><li>• Data Privacy and Data Protection</li><li>• Legal</li><li>• Transition</li></ul>
<b>External help</b>	Most advisors will help with cloud assessments <i>(e.g., Gartner, ISG, KPMG, Booz, Deloitte, McKinsey, PwC, etc.)</i>
<b>Due Diligence Questionnaires</b>	Some focus on technical and security issues, often don't properly address legal issues, but provide helpful information <i>(e.g., BITS Shared Assessments; Cloud Security Alliance Cloud Matrix; advisor tools)</i>
<b>RFPs and RFIs</b>	In cloud, RFIs may be better
<b>Key Point</b>	<i>Buying cloud is different from buying other outsourced services. The due diligence process is about evaluating the provider's offering as compared to your requirements, versus setting out your requirements, and having the provider develop a solution around them.</i>

# Getting Ready: Have a Cloud Policy

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Many companies are developing cloud computing policies that cover these and other topics:
  - Linking cloud use policy with security policies for gap analysis and risk review
  - Requirement for a business case  
(build versus buy versus keep what you have)
  - Risk review  
(risks change depending on the type of cloud service, provider, type of data and criticality to business)
  - Compliance review  
(with data protection, privacy and security at top of the list)
  - Assignment of one or more team members to manage and oversee cloud procurement and ongoing monitoring
  - Acceptable range of contract terms outcomes for cloud (covering the topics in the “5 Key Areas” portion of this presentation)

# Who is in the Cloud?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

Manufacturers  
*(many segments)*

Food and consumer  
products companies

Retailers

Media,  
entertainment  
and hospitality

Financial Institutions and  
Insurance Companies *(selectively)*

Healthcare companies

Media, entertainment  
and hospitality

Professional services organizations  
*(consultants, accountants, etc.)*



# What is in the Cloud?

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

Collaboration (*email, shared sites, enterprise collaboration sites*)

Many HR functions

Back office functions

Many IT functions  
(*enterprises buy “platforms” to host their apps and data*)

Website and  
ecommerce hosting

ERP systems

# Sample List of Cloud Providers

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

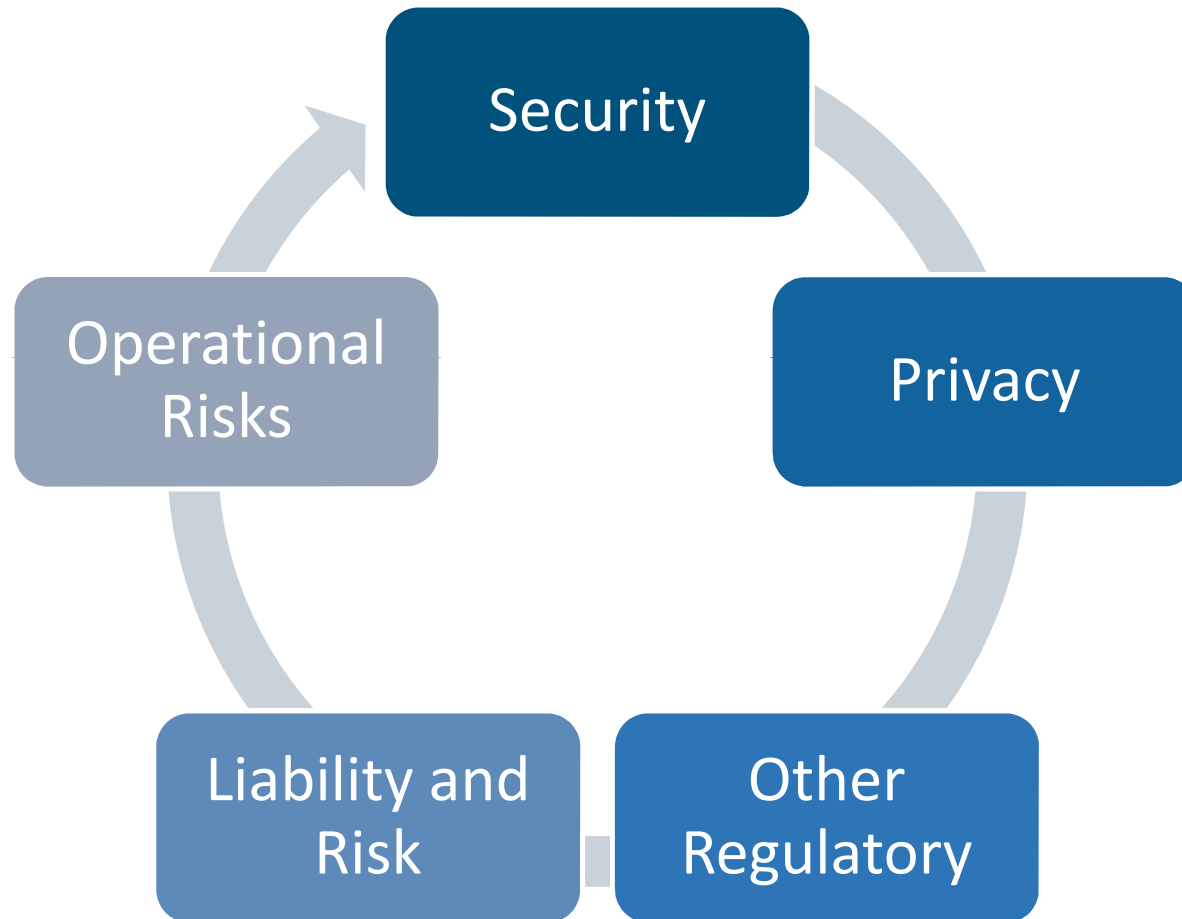




# 5 KEY ENTERPRISE INTERESTS TO PROTECT

# 5 Key Areas

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



# 5 Key Areas: Security

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Audit Rights for customer, regulators and others
- Standards and certifications—e.g., ISO 27001
  - **Watch out:** Exceptions in Statement of Applicability
- Data Breach—timely notification, cooperation, liability
  - **Watch out:** Cover data breach laws applicable to the enterprise
- Background checks for any personnel where administrative access to customer data is possible
- Encryption in transit – standard, including between data centers
- Encryption at rest – for certain sensitive data, becoming more prevalent
- Other security requirements of your business (e.g., PCI compliance)

# 5 Key Areas: Privacy

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Privacy regulation – GLB, HIPAA, States, EU, other countries
  - **Watch out:** IT and Security professionals often don't spot privacy compliance issues in their security due diligence
- Data transfers – data storage, processing, back ups and archives and cases of remote access
  - **Watch out:** Customer support and remote database administration
- Data destruction – how will data be destroyed? wiped, overwritten, pointers removed? How long before it is gone?
- Subcontracting – who, where, and what functions? Are contractual protections properly flowed down?
  - **Watch out:** Cover all tiers of subs, not just first tier of provider
- Privacy “Image” – what is the public and regulatory perception of the cloud provider?

# 5 Key Areas: Other Regulatory

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Compliance – does the solution meet your other compliance requirements?
- E-discovery – tools – do they work, what are the shortcomings? Do they cover all services, or only some? Do you have to find an external provider for ediscovery? How does that impact the ROI of the cloud?
  - **Watch out:** Understand the weaknesses and exceptions in your cloud provider's tools or the cloud architecture, and their impact on ediscovery
- Litigation holds – can they be implemented, or are frequent data “dumps” necessary (costly!)

# 5 Key Areas: Liability and Risk

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Limitations – capped damages (12-24 months or more), some exclusions
- Consequential damages – typically fully excluded, or with limited exceptions
- SLA credit sole remedy – common problem, difficult to overcome – try language that permits damages if some other claim under agreement can be made
  - **Watch out:** The “sole and exclusive remedy” language is often buried in technical service level agreements (versus legal terms)
- Reps and warranties – need more than just meets the SLA’s, need performance warranties and others
  - **Watch out:** Without performance warranties, the customer’s ability to bring claims for damages for service failures will be severely limited

# 5 Key Areas: Operational Risks

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Service Changes
- Changes to terms (links)
- Performance/SLA's
- Suspension of services
- Easy exit rights for provider
- Data use and ownership
- Interoperability with other systems
- Data portability
- DR/BCP



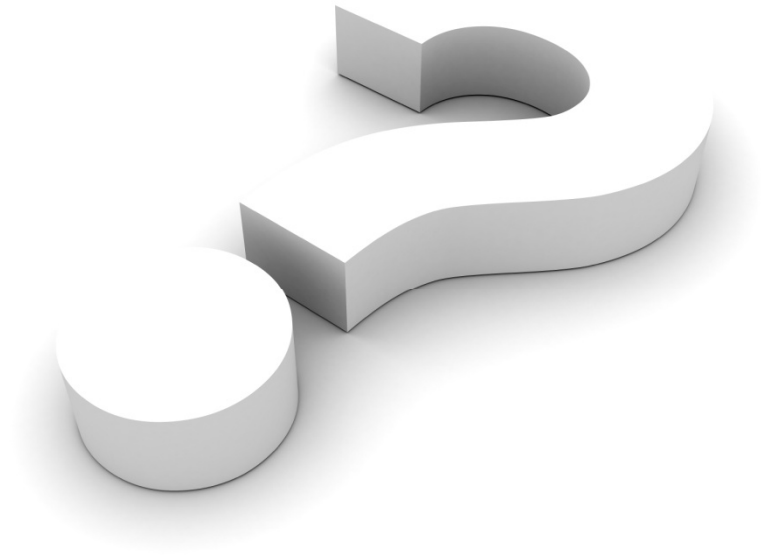
# UPDATE ON EU DATA PROTECTION AND CLOUD COMPUTING

# Additional Resources and Reading

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Cloud Security Alliance – [www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)
- National Institute of Standards and Technology, Cloud Computing Synopsis and Recommendations, Special Publication 800-146, 1 (May 2012), available at [http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=911075](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075) (11 PVLR 977, 6/18/12).
- NIST Special Publication (SP) 800-53 – Guide for Assessing the Security Controls in Federal Information Systems, available at <http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf>
- Federal Financial Institutions Examination Council, Outsourced Cloud Computing (July 10, 2012), available at [http://docs.ismgcorp.com/files/external/062812\\_external\\_cloud\\_computing\\_public\\_statement.pdf](http://docs.ismgcorp.com/files/external/062812_external_cloud_computing_public_statement.pdf).
- Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP 196 (July 1, 2012), available at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf) (11 PVLR 1097, 7/9/12).
- <http://www.mayerbrown.com/Cloud-Computing--Article-29-Working-Party-Guidance-on-EU-Privacy-and-Security-concerns-07-10-2012/>
- CNIL, Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, available at [http://www.cnil.fr/fileadmin/images/la\\_cnil/actualite/Recommandations\\_pour\\_les\\_entreprises\\_qui\\_envisagent\\_de\\_souscrire\\_a\\_des\\_services\\_de\\_Cloud.pdf](http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf) (11 PVLR 1082, 7/2/12).

# QUESTIONS



Rebecca Eisner

*Partner*

312.701.8577

[reisner@mayerbrown.com](mailto:reisner@mayerbrown.com)

# Solving Tomorrow's Governance Problems Today

Peter Dickinson

*Partner*

+44(0) 202 3130 3747

[pdickinson@mayerbrown.com](mailto:pdickinson@mayerbrown.com)

Robert J Kriss

*Partner*

+1 312 701 7165

[rkriss@mayerbrown.com](mailto:rkriss@mayerbrown.com)

GLOBAL SOURCING AND TECHNOLOGY CHANGES:

## Reboot Your Sourcing Strategies



**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 multi-jurisdictional outsourcing projects. He is a widely acknowledged leader in the telecommunications industry and is highly recommended in this field by both *Chambers UK* and the *UK Legal 500*. He is also recognized as a leading mergers and acquisitions lawyer and a leading outsourcing lawyer by both *Chambers UK* and the *UK Legal 500*.

---



**Robert Kriss** is a partner in the Litigation Practice in Mayer Brown's Chicago office. He has represented some of the world's largest technology, financial services and manufacturing companies in complex commercial, class action and intellectual property litigation. Bob has substantial experience with disputes arising in the context of financial services, real estate, securities transactions, information technology implementation and outsourcing, mergers and acquisitions, and high technology products.

- Why is a strong governance model critical to a successful sourcing relationship?
- What should a “good” governance model look like?
- How to achieve the desired state of good governance
- The practical application of governance post contract signature
  - Keeping the lines of legal responsibility clear during customer/supplier joint activities
  - Avoiding inadvertent amendments to the contract
  - Positioning disputes for favorable resolutions

# Aligning Interests

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Upfront discussions between parties and key stakeholders
- Jointly agreed vision – mutually beneficial relationship
- What is promised at negotiation stage vs what can be delivered in practice
- Early stage discussions
- Your challenges
- Cultural fit





# Breeding a Culture of Good Governance

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



Good

- Empowered participants
- Direct and honest conversations

Better

- Appropriate behaviours
- Promote trust and accountability

Stronger

- Unfettered visibility across hierarchy
- Strategic implementation

# Clear Governance Framework

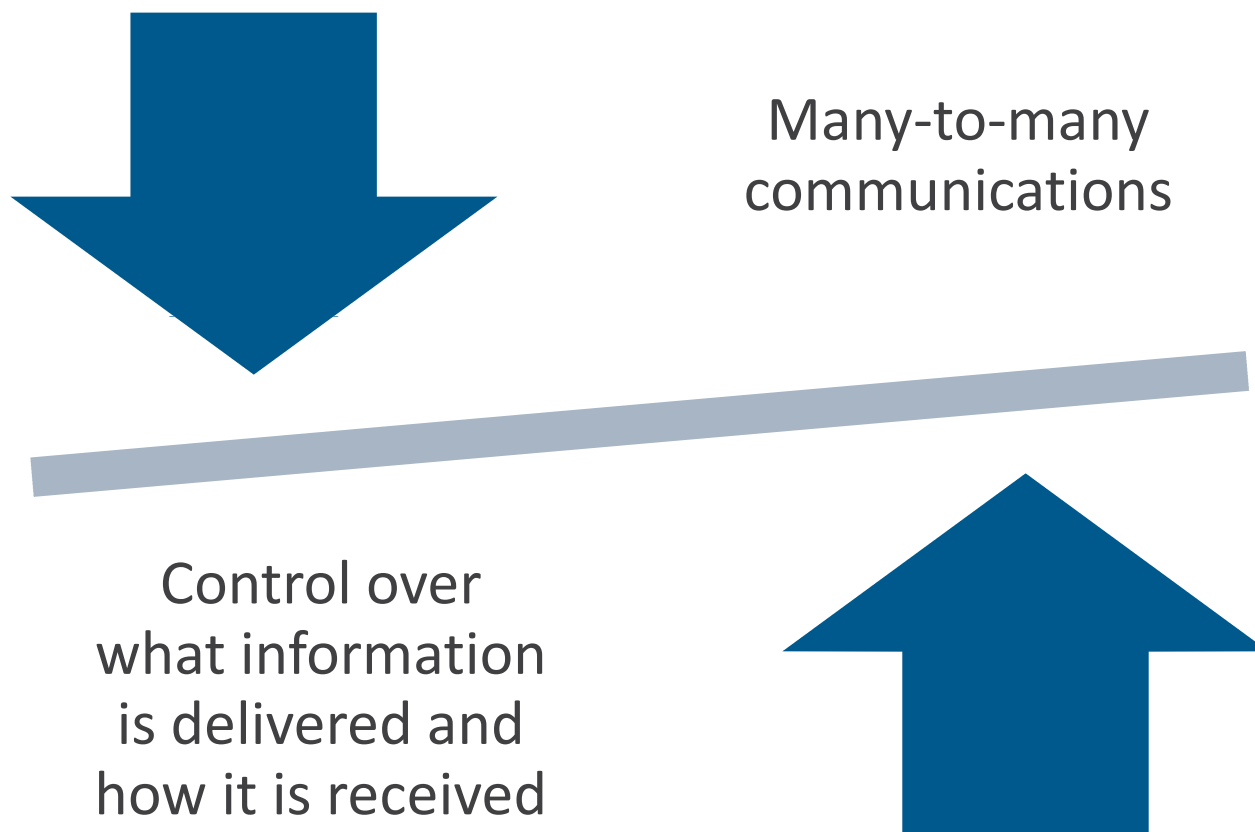
GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Construct a decision-making framework, process and system
- Implement clear, distinctive operating and strategic roles
- Emphasise accountability
  - Individuals
  - Organisational
- Consider authority of participants
- Monitor performance



# Striking a Balance

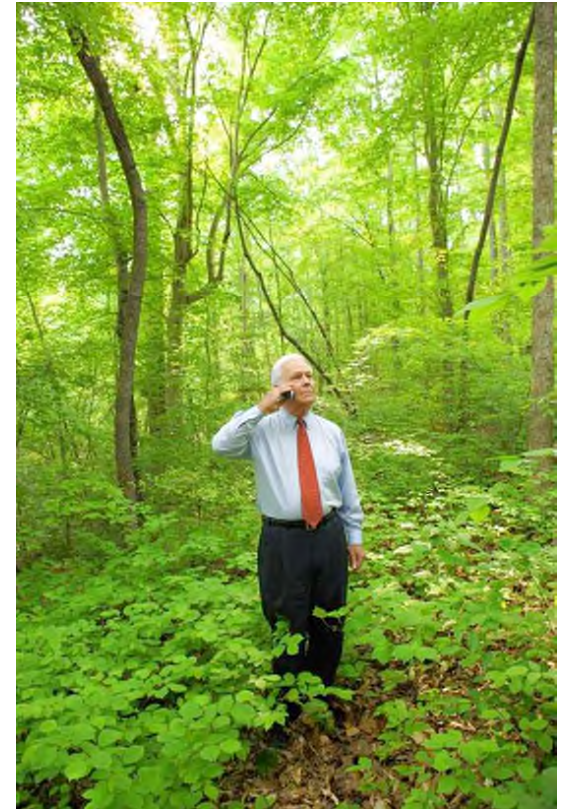
GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



# Don't Get Lost in the Woods

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Focus on strategic business objectives
- Early stage of negotiation
- High level vs detailed discussions
- Common purpose
- Benefits both parties
- Learn from past experience



Governance structure and  
relationship management

Joint governance system which  
helps manage and govern

Complimentary competencies

# Proportionate and Effective Framework

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

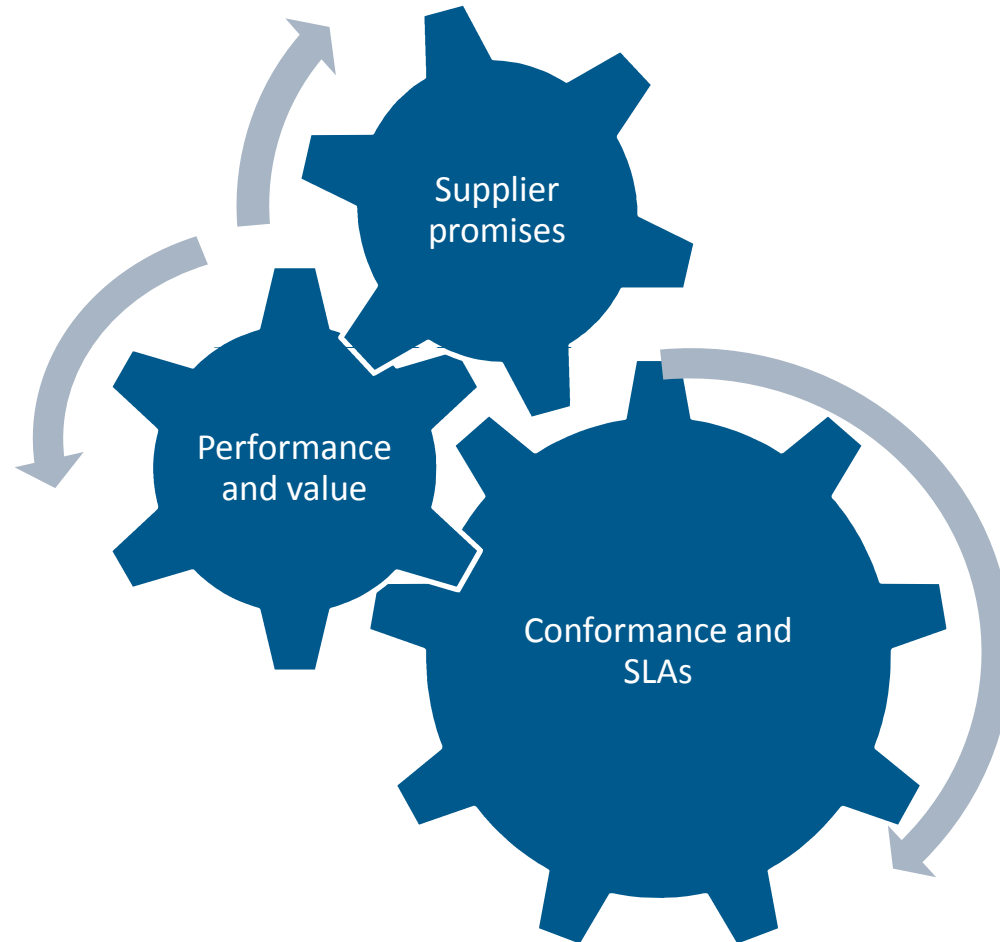
Deal size and complexity

Real time visibility

Evolution and flexibility

# Value to You, Conformance and Performance

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies





# Real-time Resolutions

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Issues should be deal with as they arise, as quickly as possible
- Appropriate solutions; quick resolutions
- Blame culture
- Dispute resolution procedure

- The framework should promote change as a normal part of the business
- Hierarchy vs devolved authority
- Moving forward – post contract
- Changing markets and evolving business demands
- Future-proof contract

# CONTRACT MANAGEMENT

# Protecting the Benefit of the Bargain

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

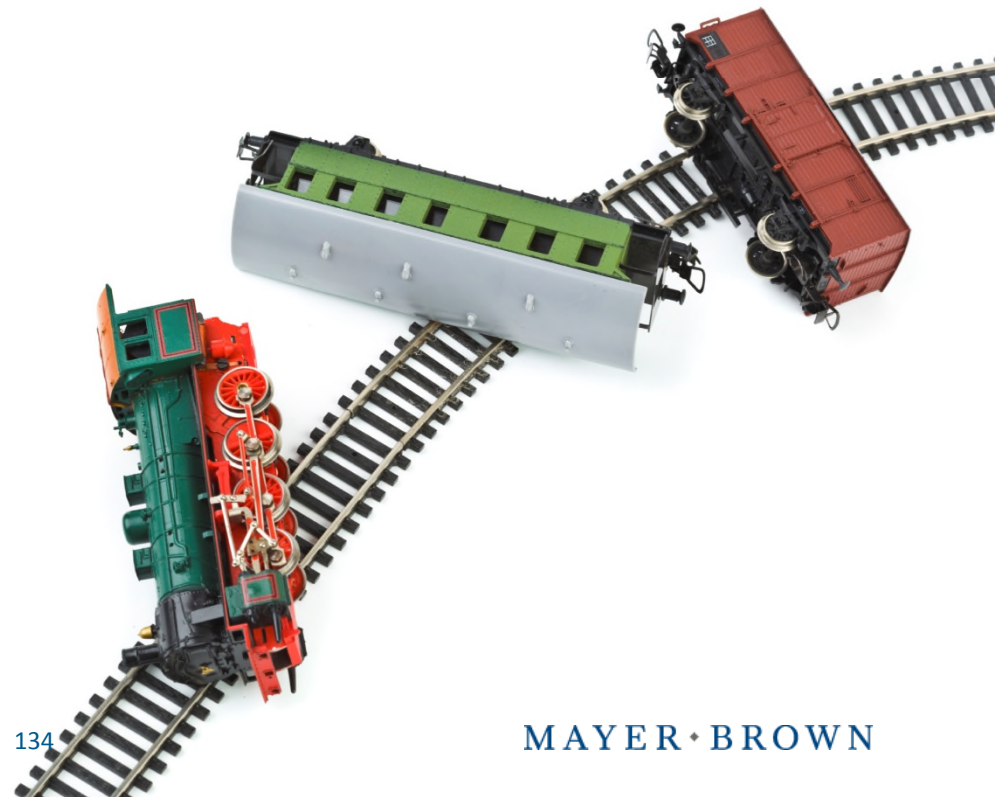
- Good Management Supports Effective Dispute Resolution
  - What you say and do in managing a contract can be used as evidence if a dispute must be resolved in a formal proceeding
  - Course of performance can be used to interpret ambiguous provisions of the contract and to amend the contract
  - Good communication is good management and good evidence
  - Statements and actions must be consistent with your interpretation of the contract



# Examples of Potential Problem Areas

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Collaboration
- Scope disputes
- Inadvertent changes to contract terms



# Hypothetical Case Study

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Outsourcing contract for transformation services
- Milestones for multiple sites
- Your cooperation will be necessary
- Missed milestones
- “Collaborative” status reports
- Procedure Manual
- Resources added by you
- Supplier asserts New Services

# Hypothetical Case Study

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Management personnel added by you
- You want to terminate for cause and be reimbursed for additional personnel costs
- Supplier claims delays and costs were caused by you



# Red Flags and Responses

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Close collaboration/missed milestones
  - Action log; written procedures for asserting excuse
- “Collaborative” Status Reports
  - Clarification of authorship; written objections
- Procedure Manual
  - Level of review; limiting authorization to amend
- Personnel deficiencies
  - Notice of material breach and intent to cover before adding personnel



# Red Flags and Responses

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- New Service claim
  - Escalate immediately to management and legal
  - Consistent action: e.g., do not ask for price quote without reservation of rights
  - Assert contract position and invite response from supplier
  - Give prior notice of intent to cover through alternative vendor and intent to seek reimbursement



# Contract Management Principles

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- State your position in writing and invite supplier to respond before deciding whether to escalate
- Make clear written record of what supplier must do to have standing to blame your company for failure to perform
- Make clear written record of who is authorized to bind your company
- Make sure what you say and what you do is consistent with your interpretation of the contract
- Give notice of material breach before attempting to cover



# Contract Management Principles

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Respond in writing to any material written assertion of supplier with which you disagree
- Require supplier to make real time log of specific actions requested of your company and deadlines for those actions necessary to meet milestones
- Keep written record clear as to responsibilities of supplier; working together does not mean supplier is no longer responsible for outcomes



# Contract Management Principles - Lessons Learned

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Clear lines of responsibility between suppliers and your business in the contract and during contract management will promote productive collaborations
- Communication and actions consistent with the contract will protect the benefits of the bargain
- Changing the contract to address changed business requirements and to obtain enhanced performance from supplier should be deliberate and documented
- Good governance delivers the potential value of the contract and may result in enhanced value over time

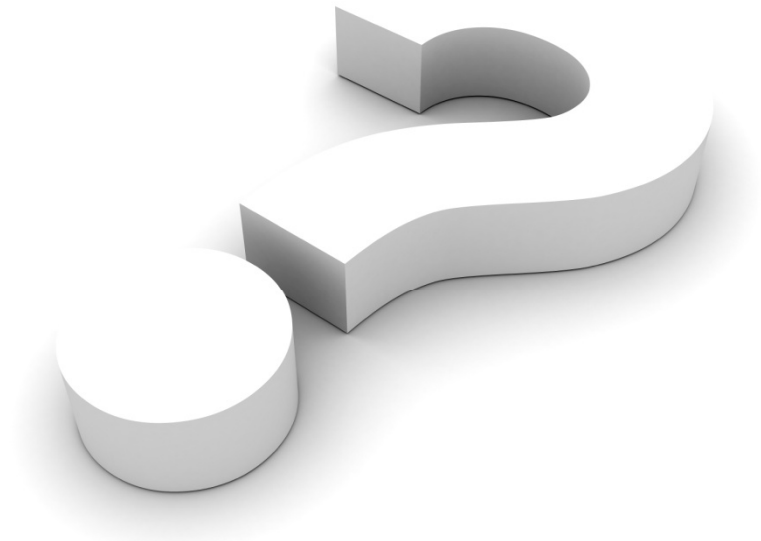
# Conclusions

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Early foundations lead to strong governance
- Learn from past mistakes
- Contract principles
- Value for you



# QUESTIONS



Peter Dickinson

*Partner*

+44(0) 202 3130 3747

[pdickinson@mayerbrown.com](mailto:pdickinson@mayerbrown.com)

Robert J Kriss

*Partner*

+1 312 701 7165

[rkriss@mayerbrown.com](mailto:rkriss@mayerbrown.com)





**Linda Rhodes** is a partner in the Business & Technology Sourcing practice in Mayer Brown's Washington office. Linda focuses her practice on complex commercial transactions, primarily in IT and business process outsourcing matters. She has represented a wide spectrum of clients in a variety of industries, including information technology, telecommunications, pharmaceuticals, health care, automotive, financial services, insurance, energy, chemicals and consumer products. Linda has been recognized in *Chambers USA* as "highly regarded for her 'direct, astute, fast, responsive and efficient' client service."

# Agenda

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Understand and Focus on Deal Objectives
- Establish and Execute Against a Project Plan
- Leverage Expertise and Experience
- Review Results to Improve Processes

## Deal objectives should:

Drive the  
project plan.

Set the  
priorities.

Set the pace  
and  
approach for  
negotiations.

Align the  
team  
members.

# Establish and Execute Against a Project Plan for the Contracting Process

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

## Establish the Project Plan

Set forth the activities and responsible parties.

Set forth the date(s) by which each activity/  
document is to be completed.

Consider the timing for critical path items.

Consider risks and mitigation strategies.

Build in time for sign-offs/approvals.

# Establish and Execute Against a Project Plan for the Contracting Process

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

## Execute Efficiently

Ensure each team member understands his or her area of responsibility.

Plan ahead / Avoid duplication of efforts.

Allow for timely input from subject matter experts.

Ensure checkpoints for alignment of team members.

Avoid interim agreements.

Use competitive leverage to drive results.

# Leverage Expertise and Experience

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies



Invest time in deal templates, tools and methodologies.



Use templates, tools and methodologies wisely.



Build your knowledge database.



Share knowledge with colleagues.



Capture knowledge during the course of the deal where practical.



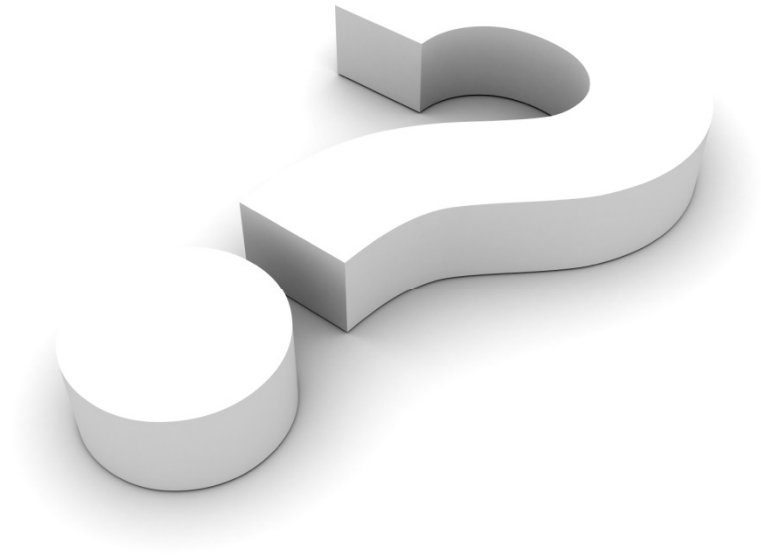
# Review Results to Improve Processes

GLOBAL SOURCING AND TECHNOLOGY CHANGES: Reboot Your Sourcing Strategies

- Review results promptly after deal close for maximum value.
- Assess what worked well and build on successes.
- Assess what can be improved.
- Build that knowledge into templates, tools and methodologies where appropriate.
- Add to your deal database.



# QUESTIONS



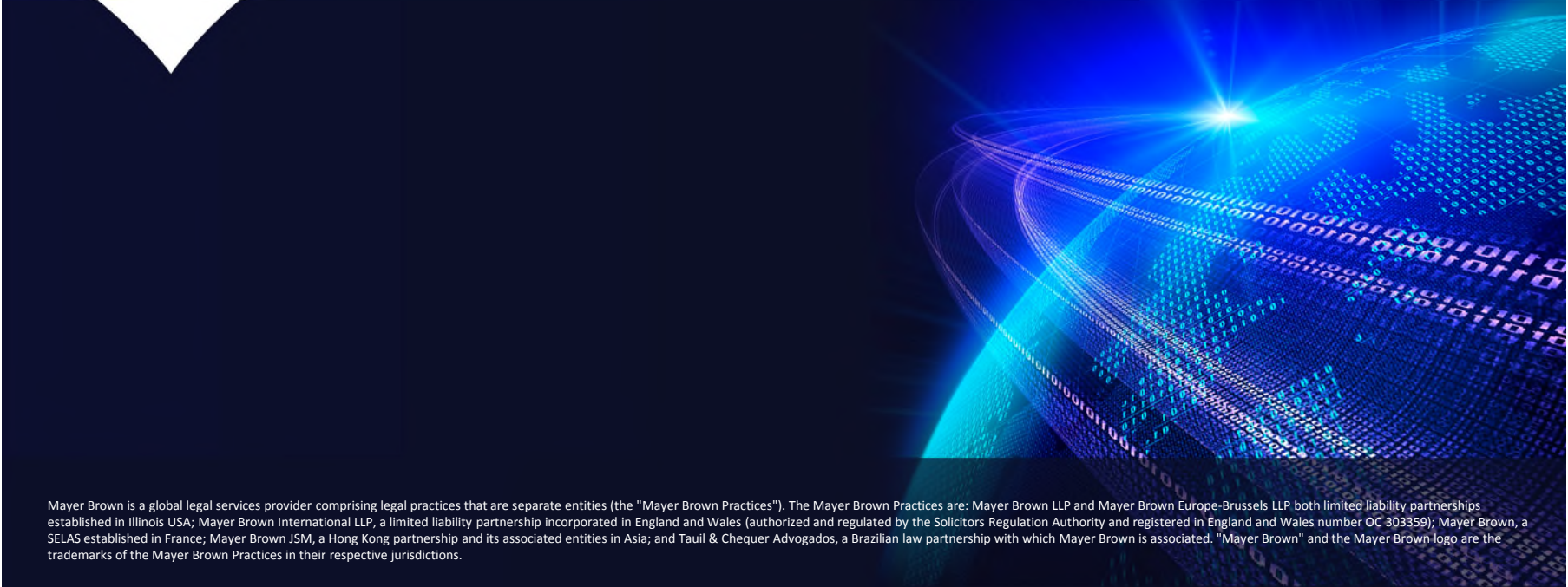
Linda Rhodes

*Partner*

+1 202 263 3382

[lrhodes@mayerbrown.com](mailto:lrhodes@mayerbrown.com)

# MAYER • BROWN



Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.