

MAYER • BROWN

NSA Data Collection and its Impact on Cloud and Outsourcing and Recent Privacy and Security Developments on Capitol Hill

Marcus Christian
Partner

+1 202 263 3731
mchristian@mayerbrown.com

Rebecca Eisner
Partner

+1 312 701 8577
reisner@mayerbrown.com

Howard W. Waltzman
Partner

+1 202 263 3848
hwaltzman@mayerbrown.com

Global Business & Technology Sourcing

CRITICAL ISSUES FOR CORPORATE COUNSEL

Speakers / Moderator

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL



Marcus Christian is a Washington DC partner in Mayer Brown's Litigation & Dispute Resolution practice and White Collar Defense & Compliance group. Prior to joining Mayer Brown, Marcus was the third-ranking prosecutor at the United States attorney at the US Attorney's Office for the Southern District of Florida. During Marcus' career as a federal prosecutor, he conducted wiretaps, participated in investigations involving classified information, and led task forces investigating crimes resulting from data breaches, among other things. Marcus is a member of our White Collar Defense and Compliance practice and has represented clients in matters involving cyber fraud, data security, internal investigations, and government enforcement.



Howard Waltzman is a Washington DC partner in Mayer Brown's Government and Global Trade practice. Howard focuses his practice on communications and Internet law and privacy compliance. He represents some of the nation's leading communications service providers, manufacturers and trade associations in regulatory, compliance and legislative matters, including with respect to Internet and wireless services, privacy, video programming and communications-related homeland security. He also represents investors on these and other communications-related matters.



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. Rebecca also regularly advises clients in data transfer and privacy issues affecting corporate initiatives and transactions, such as divestitures, global data programs, data collection and use, and emerging US security and privacy legal standards.

Business & Technology Sourcing Practice

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- More than 50 lawyers around the world focused on helping clients improve their business operations by sourcing services and technology
- Advised on more than 300 significant outsourcing transactions valued at an aggregate of more than \$100 billion
- Recognized Market Leader



- “Band 1” ranking in IT/Outsourcing for ten consecutive years (*Chambers 2004-2014*)



- Named “MTT Team of the Year” in 2014 and ranked in the top tier from 2010 thru 2014



- Ranked as one of the top law firms in 2009 thru 2014 on The World's Best Outsourcing Advisors list for The Global Outsourcing 100™

MAYER • BROWN

NSA Data Collection and its Impact on Cloud Computing and Outsourcing

Marcus Christian
Partner

+1 202 263 3731
mchristian@mayerbrown.com

Global Business & Technology Sourcing
CRITICAL ISSUES FOR CORPORATE COUNSEL

Agenda

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- I. Understanding the NSA's Activities
- II. Beyond the NSA: Other Governments' Activities
- III. Beyond Governments: Organized Crime
- IV. Minimizing Your Risks

I. Understanding the NSA's Activities

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- US gathering information through a variety of means:
 - Phone Records Program
 - PRISM
 - Upstream
 - Backdoors

I. Understanding the NSA's Activities

A. Phone Records Program

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Collects the metadata of telephone calls made within the US
- Authorized by Section 215 of the USA PATRIOT Act and supervised by the FISC (limits unclear)
- 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
- Several lawsuits are pending challenging the constitutionality of the program
 - Lawsuits will be moot if Congress terminates the program



I. Understanding the NSA's Activities

B. PRISM

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

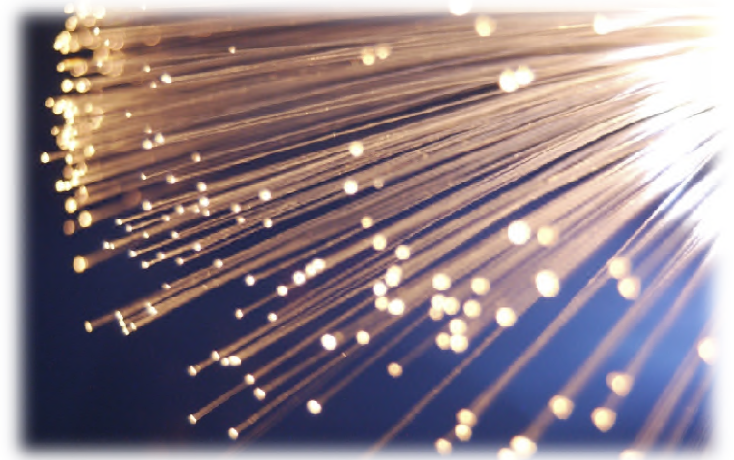
- Collects internet-related data from foreign targets overseas who are using US networks
 - Fewer targets than phone records program, but more types of information captured
 - 91% of 250M NSA-collected internet communications
 - Authorized by Section 702 of the FAA
- Publicized through 2013 Snowden leaks
 - Very controversial in EU 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. Upstream

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Intercepts telephone and internet traffic from major internet cables and switches and retains them for at least two years
 - Gathers metadata and captures communications “about targets,” so sweeps more broadly than PRISM
 - 9% of 250M NSA-collected internet communications
 - Authorized by FISA, FAA, “Transit Authority,” and EO 12333



I. Understanding the NSA's Activities

D. Backdoors

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Appears to be unknown to industry
- Tactics include:
 - Weakening NIST encryption
 - Exploiting NSA tools used by private companies
 - Infecting hardware via malware and advance surveillance
 - Disguising as website server
 - Maintaining collections of known weaknesses in various products
 - Use of Heartbleed exploit for two years prior to public discovery



II. Beyond the NSA: Other Governments' Activities

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- US not the only country engaging in information-gathering
- Widespread evidence that many nations—including traditional allies—gathering information
- Some information-gathering occurring in concert with US
- Tactics include:
 - Call monitoring
 - Data collection and sharing
 - Hacking

II. Beyond the NSA: Other Governments' Activities

A. Call Monitoring

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Of 29 countries reviewed, not including China and Russia, six had laws providing for the government's unrestricted access to telecommunications:



II. Beyond the NSA: Other Governments' Activities

B. Data Collection and Sharing

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners



<u>Second Parties</u>	<u>Third Parties</u>		
Australia	Algeria	Israel	Spain
Canada	Austria	Italy	Sweden
New Zealand	Belgium	Japan	Taiwan
United Kingdom	Croatia	Jordan	Thailand
	Czech Republic	Korea	Tunisia
	Denmark	Macedonia	Turkey
	Ethiopia	Netherlands	UAE
	Finland	Norway	
	France	Pakistan	
	Germany	Poland	
	Greece	Romania	
	Hungary	Saudi Arabia	
	India	Singapore	

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

II. Beyond the NSA: Other Governments' Activities

C. Hacking

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Hackers alleged to have:
 - Infected computers with malware
 - Stolen trade secrets
 - Captured personal and security information



III. Beyond Governments: Organized Crime

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

Rapidly growing
black market for
hacker tools and
stolen data

Organized crime
cyber activities and
techniques are
expanding and
changing

*United States v.
Bogachev*

IV. Minimizing Your Risks

A. Overview

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The first step to preparing a response is to understand the risks/threats
- Some risks arise from actual threats to 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 might not actually be vulnerable
 - Or at least, it might be no more vulnerable than most other data
 - But, negative perceptions can have serious implications

IV. Minimizing Your Risks

B. The Risks

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

Data Appropriation

- Trade secrets
- Business plans
- Security information
- Personal information of executives and employees

Data Loss

- Site downnage
- Server and file seizure (likely not a significant risk from governments)

IV. Minimizing Your Risks

B. The Risks (cont'd)

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

Hardware Damage

- Malware
- Seizure

Business Loss

Damaged Customer Relations

Investigations/Legal Liabilities

IV. Minimizing the NSA Effect

C. Responses: Vendor Contracts

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Your vendors may be cooperating with one or more governments through “back-doors” in their products
- 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



IV. Minimizing Your Risks

C. Responses: Vendor Management

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Select proper locations and vendors
 - Caveats:
 - NSA can still “hack” into non-US servers
 - Other governments may use data-gathering methods of their own, cooperate with US
 - Keeping data outside of US and only with non-US companies might be impractical and/or costly



IV. Minimizing Your Risks

C. Responses: Data Management

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Develop internal classification systems to treat data differently according to sensitivity
- Consider selective in-housing
 - Retaining some data according to sensitivity could decrease the impact of government cooperators
- Encrypt data
- Avoid networks and tools known to be compromised



IV. Minimizing Your Risks

C. Responses: Customer Relations/Marketing

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Manage customer expectations about your ability and obligation to safeguard data
- Educate customers about the nature of the risks
 - Many countries pose surveillance risks
 - For some content, NSA not likely to be interested
 - NSA does not appear to have used information to aid commercial actors
 - Some countries do collect information for commercial purposes
- Educate customers that moving data elsewhere might not address their concerns

IV. Minimizing Your Risks

C. Responses: Legal and Legislative

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Evaluate data-storage practices in light of applicable nations' data-protection rules
- Support legislative reform efforts
 - Increase transparency regarding nature of programs
 - Revise or eliminate surveillance programs



MAYER • BROWN

Recent Privacy and Security Developments on Capitol Hill

Howard W. Waltzman

Partner

+1 202 263 3848

hwaltzman@mayerbrown.com

Global Business & Technology Sourcing

CRITICAL ISSUES FOR CORPORATE COUNSEL

A. Information Security

- Contemplated legislative responses
- Possible regulatory responses

B. Cybersecurity

- The origin, purpose, and content of the Framework v. 1.0
- Legislative Responses to the Framework
- Regulatory Responses to the Framework

Part A

INFORMATION SECURITY



There Has Been Renewed Interest in a Legislative Response to Data Breaches

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Congressional interest in data breach notification and information security legislation has been renewed by recent high profile breaches
- Policymakers seek to protect consumers from fraud and enhance security of personal information
- Disagreement over how to achieve these goals has been sharp

The Legislative Debate Presents a Series of Significant Policy Questions

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

How prescriptive should data security standards be?

Should such standards be established through regulations?

What entities should be covered by new requirements?

To what extent should state law be preempted?

Should the law provide a private right of action?

Should the FTC have primary, exclusive, or shared jurisdiction?

What role should state attorneys general and state enforcement agencies have in enforcement of the law?

Senate Legislation: The Toomey-King Bill, S. 1193

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- There are a number of bills that have been introduced in the Senate
- The Toomey-King legislation would:
 - Require entities within the FTC’s jurisdiction and common carriers subject to the FCC to protect data pursuant to a “reasonableness” standard.
 - Require those covered entities to notify affected individuals if the entity reasonably believes that a breach has caused or will cause financial harm.
 - Be self-executing and not require rulemaking

Senate Legislation: The Carper-Blunt Bill, S. 1927

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The bill focuses on financial institutions, but covers any entity that “maintains or communicates sensitive account information or sensitive personal information,”
- The Carper-Blunt bill is before the Banking Committee. It would:
 - Require “reasonable” data security practices and notification to consumers if a breach is “reasonably likely” to cause “substantial harm or inconvenience” to consumers.
 - Require financial regulators (e.g. OCC, FDIC, etc.) and the FTC to issue implementing regulations as to entities within their enforcement jurisdiction.

Senate Legislation: The Leahy Bill, S. 1897

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The Chairman of the Senate Judiciary Committees has introduced data security legislation, and is working with Senator Grassley to make the legislation more bipartisan.
- The bill requires business entities to “take reasonable measures to protect and secure sensitive personally identifiable information.”
- Breach notification is required if there is “a significant risk that the security breach has resulted in, or will result in, identity theft, economic loss or harm, physical harm, or fraud.”

House Activity

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The Energy & Commerce Committee has held a hearing on information security and data breach notification standards.
- The Committee is expected to consider legislation this summer or fall.
- The legislation is likely to create a new federal regime administered by the FTC that preempts state laws.



Regulatory Enforcement is Poised to Continue at Both the State and Federal Levels

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The FTC continues to attempt to police data security practices through enforcement actions
 - The Wyndham and LabMD actions will determine the scope of the FTC’s data security authority going forward
- As demonstrated in California, state regulators also are likely to continue to be active
 - California AG Kamala Harris has announced the prioritization of data breach investigations
 - California’s breach notification requirement recently was expanded to be triggered by breach of “a user name or email address, in combination with a password or security question and answer that would permit access to an online account”

Part B

CYBERSECURITY



The NIST Framework Has Its Roots in the Failed 2012 Effort to Pass Comprehensive Cybersecurity Legislation

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- In the summer of 2012, Congress considered cyber threats to critical infrastructure:
 - The Senate considered legislation that would have allowed the creation, through regulation, of mandatory cybersecurity standards for critical infrastructure
 - When this approach stalled, a compromise was considered under which incentives, including liability protections, would be given in exchange for adoption of new voluntary cybersecurity standards
- After the legislation failed, President Obama issued Executive Order 13636, which ordered the creation of the NIST Framework

EO 13636 Included Four Key Directives Regarding the NIST Framework

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

The National Institute of Standards and Technology (NIST) was tasked with creating the Cybersecurity Framework

The Department of Homeland Security was tasked with creating a voluntary program to support adoption of the Framework

A number of agencies were tasked with evaluating which incentives – including liability protections – would properly support adoption of the Framework

Regulatory agencies were required (or urged, in the case of independent agencies) to consider whether to act in response to the Framework

Like the Executive Order, the NIST Framework Focuses on Critical Infrastructure

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- “Critical Infrastructure” is defined in the Executive Order and the Framework as:

“[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”

The NIST Framework v. 1.0 Is Consistent With the Principles Behind the Executive Order

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The Framework is based on **industry expertise and best practices** and ultimately is intended to be administered outside the government
- Adoption of the Framework and participation in the DHS program is **voluntary**
- The Framework reflects a **risk-based** approach to cybersecurity:
 - It is *not* one-size-fits-all
 - It is *not* a checklist
 - It is *not* technology specific

Companies Now Must Decide How to Respond to the Framework

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- Companies should make informed business decisions about their cybersecurity – this is not just a technical issue
- Key considerations include:
 - The “leverage” the Framework is intended to exert on industry
 - Possible regulatory activity based on the Framework
 - Possible efforts to use the Framework in litigation
- Critical infrastructure companies are most directly affected, but other companies also will be wise to consider the implications of the Framework

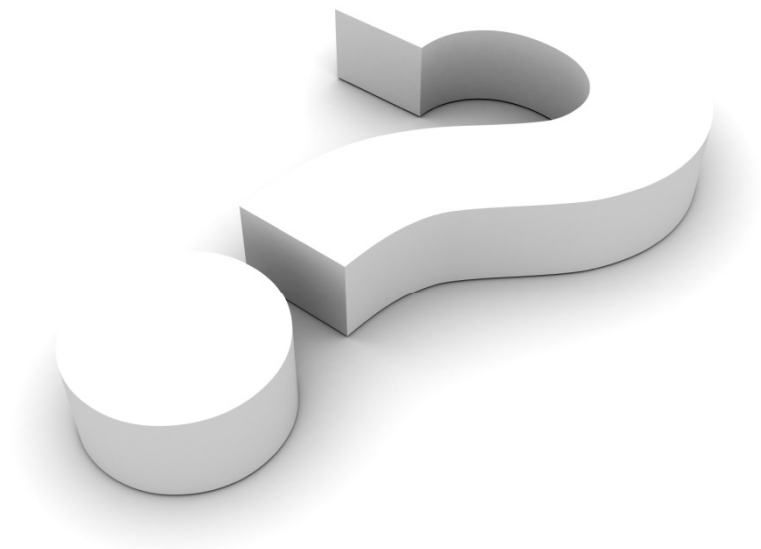
Legislation Has Stalled Since the Adoption of the NIST Framework

Global Business & Technology Sourcing: CRITICAL ISSUES FOR CORPORATE COUNSEL

- The House passed the bi-partisan Cyber Intelligence Sharing and Protection Act by a vote of 288-127.
 - The bill would increase information sharing between private entities and the federal government as well as among private entities.
- The Senate Intelligence Committee recently passed similar legislation.



QUESTIONS



Marcus Christian

Partner

+1 202 263 3731

mchristian@mayerbrown.com

Howard W. Waltzman

Partner

+1 202 263 3848

hwaltzman@mayerbrown.com

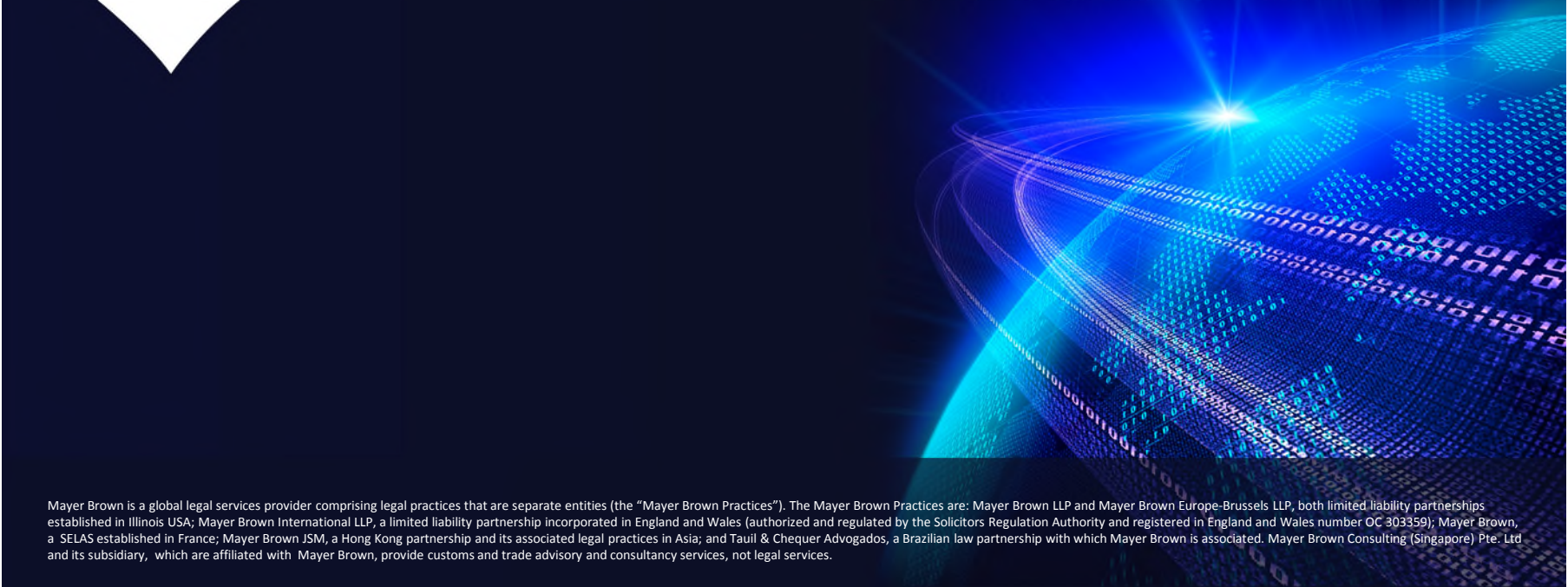
Rebecca Eisner

Partner

+1 312 701 8577

reisner@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 legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services.