MANAGING THE CHALLENGES OF CROSS-BORDER INVESTIGATIONS

A GUIDE TO IDENTIFYING AND AVOIDING THE COMMON ISSUES THAT COMPLICATE CROSS-BORDER INVESTIGATIONS
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>NAVIGATING GLOBAL PRIVACY ISSUES</td>
<td>1</td>
</tr>
<tr>
<td>The global data-protection framework</td>
<td>2</td>
</tr>
<tr>
<td>Privacy as a fundamental right</td>
<td>2</td>
</tr>
<tr>
<td>The US exception</td>
<td>2</td>
</tr>
<tr>
<td>Limits on cross-border data transfer</td>
<td>2</td>
</tr>
<tr>
<td>Legal system structure</td>
<td>3</td>
</tr>
<tr>
<td>EVEN IF YOU CAN MOVE DATA, SHOULD YOU?</td>
<td>3</td>
</tr>
<tr>
<td>UNDERESTIMATING THE CHALLENGES OF IN-COUNTRY REVIEW</td>
<td>4</td>
</tr>
<tr>
<td>Beyond language translation</td>
<td>4</td>
</tr>
<tr>
<td>Integrated teams</td>
<td>4</td>
</tr>
<tr>
<td>Special considerations for emerging markets</td>
<td>4</td>
</tr>
<tr>
<td>MISSED OPPORTUNITIES AND DEFENSIBILITY</td>
<td>5</td>
</tr>
<tr>
<td>BEST PRACTICES FOR AVOIDING THE UNANTICIPATED</td>
<td>5</td>
</tr>
<tr>
<td>Use plans to prevent, detect and respond</td>
<td>5</td>
</tr>
<tr>
<td>Understand your data</td>
<td>5</td>
</tr>
<tr>
<td>Build the right team</td>
<td>6</td>
</tr>
<tr>
<td>Technical experience</td>
<td>6</td>
</tr>
<tr>
<td>Local knowledge</td>
<td>6</td>
</tr>
<tr>
<td>Boots versus roots</td>
<td>6</td>
</tr>
<tr>
<td>Rethink technical requirements</td>
<td>6</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>7</td>
</tr>
<tr>
<td>ABOUT CONTROL RISKS</td>
<td>7</td>
</tr>
<tr>
<td>CONTRIBUTING AUTHORS</td>
<td>8</td>
</tr>
</tbody>
</table>
MANAGING THE CHALLENGES OF CROSS-BORDER INVESTIGATIONS

Introduction

With the world becoming more interconnected and diversified, corporations looking across borders to take advantage of business opportunities face new conflicts between risk and reward. In Dickensian terms: it is the best of times; it is the worst of times.

It is a time of opportunity. Advancements in technology make global communication and business dealings easier than ever. The decentralisation of global financial centres creates new sources of investment. Emerging countries create new markets for raw materials, cheap labour, energy sources and low-cost goods.

It is also a time of risk. Opportunities in economically and politically unstable markets heighten the threat of corporate corruption. Social media, new technology devices and the intermingling of personal and business data raise questions about privacy expectations as laws regulating such issues continue to evolve. Government punishment of wrongdoing is at an all-time high. Combined, these risks have significant legal implications and, ultimately, could have a broad and lasting impact on corporate reputation.

For corporations doing business across international borders, the need to prevent and detect wrongdoing has never been greater. When these efforts fail and investigation ensues, the ability to anticipate the unexpected is critical to ensuring an efficient, defensible and cost-effective response.

Some frequent challenges for companies include:

- Underestimating the impact of global data-protection laws: Global rules relating to data privacy and protection are constantly evolving, making it almost impossible to anticipate all the data issues that may affect an investigation.
- Presuming data should and can be moved: Whether and how to move data between countries are complicated issues. Getting it wrong can incur substantial fines and, in some instances, imprisonment.
- Miscalculating the importance of local knowledge: The depth of experience and resources needed on the ground go far beyond language translation alone.
- Underestimating the process of data collection: It is hard to know from the onset of the investigation what the volume and diversity of data will be, as well as the number and relevance of custodians, and the way to obtain access to data sources.
- Maximising technology: New and evolving global requirements regarding data disclosure and budgeting make selection of the right technology more important than ever.

Navigating global privacy issues

Cross-border investigations typically require global co-ordination throughout a business and can involve subsidiaries, partners and other affiliates worldwide. Knowing where an investigation will lead may be difficult, and equally challenging may be understanding the nuances of international privacy laws.

Prior to the late 1990s, only a few countries comprehensively regulated data privacy and these laws had had minimal impact on corporate compliance. Today virtually every country has, or is in the process of developing, regulations for the protection of data. Navigating these complex, evolving and often conflicting regulations is becoming harder when trying to detect or respond to allegations of corruption.

But failing to anticipate the effect local data-protection laws can have on an investigation can be costly, leading to sanctions, fines and, in some cases, even prosecution.
The global data-protection framework
Understanding the full scope of evolving international data-protection laws is perhaps unrealistic. However, a general familiarity with the emerging global framework of data privacy and transfer can help anticipate problems and inform decisions about how to manage them.

Privacy as a fundamental right
The growing international consensus about data protection is based on the view of most governments: privacy is a fundamental right. Most countries that have enacted laws take this approach and give high priority to personal data privacy.

The model regulation for laws driven by this view comes from the EU. The EU data-protection directive requires that individuals be informed and provide express consent prior to the collection and search of personal data.

Under the EU directive – which is supported by legislation in each member state – personal data includes electronic, written, internet and even oral communication. There is a presumption against the collection and processing of personal data unless it is for a specific and legitimate purpose. “Processing” of personal data is broadly defined and includes storage. This means the mere act of holding personal data is regulated under the EU directive and each member state’s national legislation.

The roots of the EU directive stem from the Second World War, when Nazi military officials used databases containing personal information to track down and kill suspected Dutch Resistance members and supporters. With the increase in data and emergence of technology, the Europeans’ scepticism towards government has transferred to corporate enterprises, which use sophisticated databases to collect, track and store the personal data of employees, customers, vendors, suppliers and other third parties.

In addition to EU member countries, the governments of Australia, Canada, Japan, Hong Kong and Switzerland are among those that follow this model for data protection. Additionally, emerging markets – including all of the BRIC countries (Brazil, Russia, India and China) – have or are working to finalise highly restrictive legislation to protect personal data and limit its transfer outside individual country borders.

The US exception
The major exception to the presumption toward data protection is the US. Despite its aggressive and complex regulatory environment, the US does not consider personal data privacy in the context of an investigation to be a fundamental right. Conversely, there is a presumption towards permissible disclosure of personal data rather than against it.

US data-protection laws generally favour corporate access to information over protections for the individual, with certain exceptions. Unlike in Europe, where data on an employee’s company-issued computer is considered private, in the US personal data on a work computer is considered company property. Generally, the US only regulates the use of personal data in certain sectors, such as healthcare (under the Health Insurance Portability and Accountability Act) and financial services (under the Gramm-Leach-Bliley Act).

Any investigation involving US authorities or operations almost assuredly will bring with it inherent conflicts with data-privacy laws of other countries. The conflict between the approach of the EU and the US towards privacy already exists. As the rest of the world moves to follow the EU model, the likelihood for increased conflicts will grow. This is a particular concern in corporate investigations given that the US is one of the most aggressive enforcers of foreign corrupt practice regulation as well as being the dominant force in international litigation.

Limits on cross-border data transfer
The ability to access data is one issue; transferring data across international borders is another. Done right, transferring or restricting the transfer of data across borders brings procedural hurdles, as well as time and expense. Done wrong, the cost of potential fines and sanctions is even higher; in some cases, the risks become criminal. There are several factors that come into play when companies or their lawyers want to transfer data across international borders. Among them are Safe Harbor principles, blocking statutes and state secret laws.

Safe Harbor provisions
The EU directive limits the transfer of data to a limited number of nations deemed as having “adequate protections” for data privacy. Switzerland, Canada and Australia are among the handful determined to be “Safe Harbors”; the US is not. There is a Safe Harbor programme between the US and the EU that certifies companies who comply with its principles to use and transfer data to and from EU organisations. If Safe Harbor is not an option, companies with EU subsidiaries can enter into agreements to provide adequate data protection.
**Blocking statutes**

Blocking statutes prohibit export-of-information requests that are tied to foreign legal proceedings. Such statutes as those of Germany and France create conflict-of-law issues. Companies face potential criminal sanctions if they ignore the law, and they face legal sanctions in courts if they object to discovery on the basis of a blocking statute. US courts have required document production even in cases where the production may violate another country’s blocking statute.

Some countries do provide exceptions to the blocking statute through the Hague Convention. Companies need to carefully navigate the full array of these rules and work with counsel to limit discovery requests or develop a mutually agreeable plan to deal with the conflicting regulations.

**State secrets**

Outside of Europe the challenges with data privacy can be even more difficult. In China, for example, companies must be wary of violating state secret laws. Moving documents containing state secrets outside China’s borders – knowingly or unknowingly – carries severe criminal sanctions that can even include the death penalty. Complicating matters is the Chinese definition of a state secret, which is so broad as to not always be clear what falls under it.

The threat of criminal sanctions rightfully heightens concerns more than the imposition of mere civil fines. Companies that deal with state-owned enterprises or sensitive industries, like defence, must be mindful of the potential risks should an investigation involve Chinese territory.

The goal, of course, is to avoid uncovering any information that could be considered a state secret. However, if an inadvertent disclosure is made, it is important to respond proactively. The ability to demonstrate good faith with authorities is critical. It can be helpful to retain resources on the ground that have established relationships with government officials and can assist in navigating the situation.

**Legal system structure**

In common-law legal systems disclosure is a fundamental part of legal proceedings. In addition to the UK and US, common-law countries include Australia, Hong Kong, Canada and Bangladesh. In these jurisdictions, parties to a legal dispute play the primary role in investigating, developing and presenting the facts of a case. As such, data disclosure is part of the legal process and privacy issues frequently come into play. At the same time, corporations in these jurisdictions are more likely to have formal processes in place regarding disclosure.

Not every common-law system has the same rules, so even among common-law jurisdictions the extent of discovery varies. For example, the scope of the US discovery law is broad. Litigants are required to disclose any document that is only reasonably calculated to lead to admissible evidence and that is not privileged. In the UK litigants are required to disclose any document that will affect a case. Although a subtle difference in language, the scope of the UK law is much narrower.

In civil-law jurisdictions – the most widespread legal system in the world – the judge plays the primary role of investigator. As such, these countries – including all the mainland European countries, China, Mexico, Russia and Brazil – do not have laws pertaining to document disclosure and discovery.

Many companies working in these jurisdictions lack the policies and procedures typical in common-law countries for such matters as privilege, preservation, collection and review. Such lack of corporate governance and information management processes can create challenges when conducting investigations in these countries.

**Even if you can move data, should you?**

A corollary to understanding the myriad laws relating to whether one can access and transfer data across borders is the question of whether one should. Whether to transfer data is a question for the legal team because the rules are ever changing. Many companies fail to appreciate the complexities of data-protection laws and violate them long before an investigation ever starts, because of poor information management procedures or simply lack of knowledge.

Even if it is permissible to transfer the data, it may be more advantageous to keep the data in the country. Often when an investigation involves multiple affiliates, subsidiaries, custodians or countries, the instinct is to centralise evidence in a single locale – the headquarters of the company or of the law firm managing the investigation. This may seem convenient and cost effective, but there are risks.
Customs agents may not have the proper understanding of the governing laws. Or they may take a “better safe than sorry” approach and prematurely confiscate data, rather than risk being held responsible for letting something leave the country that should not. Encrypted drives – designed to protect data – can inadvertently set off alarm bells. Delays in responding to disclosure requests and missed deadlines only add to the time and cost of an investigation.

Using the cloud to move data does not necessarily lessen the risks. Companies need to be sure their cloud providers comply with Safe Harbor provisions and know where data centres are located. Data could be moved to multiple locations without knowledge, raising issues about legal ownership, availability and privacy. In China state-secret laws are engaged anytime data is moved off the mainland, so even transferring data to a Hong Kong data centre can create problems.

In-country reviews require infrastructure, on-the-ground forensics and, often, access to an in-country data centre. Those come at a price but, over the long run – and particularly given the availability of mobile technologies – may ultimately save time and hard costs.

**Underestimating the challenges of in-country review**

Cross-border investigations often involve vast amounts of electronically stored information on numerous devices in multiple jurisdictions. Management of an in-country document review requires careful co-ordination of the investigative team, technology resources and logistical support.

**Beyond language translation**

When dealing with data from multiple countries, language translation is always an issue. Beyond that, there are broader issues that can arise when working on the ground in a foreign jurisdiction, which companies and their outside counsel often fail to consider. Many make the mistake of assuming that because business development teams, or compliance teams, or even investigative teams frequently travel to a location, that there is an in-depth knowledge of local customs, laws and authorities within the organisation.

Given the intricacy of data-privacy and -transfer laws, local relationships are invaluable. Consider one law firm’s experience conducting an investigation in India on the day after its new data-privacy statute was enacted. When an official threatened to arrest the data-collection agent for violating the law, the firm was able to avoid a confrontation. This was due to its local agents, who helped navigate the law; communicate with local officials, with whom they had relationships; and otherwise neutralise the situation.

**Integrated teams**

The breadth of experience of the investigative team is also important. Some companies mistake forensic accountants for computer forensics specialists. The former may have working knowledge of computers but likely do not have the skills to deal with complex technical issues that can arise during collection and processing.

The ability of an investigative team to work hand-in-hand with the forensics team is also important. In sensitive investigations where getting access to the data is crucial, a diversified and well-co-ordinated team is necessary. Consider a recent investigation in China involving a widespread bribery scheme orchestrated by a group of employees. At the onset, the extent of corruption inside the organisation was not known. Tensions were so high it was not clear whether members of the corporate IT department were involved. Not knowing whom to trust when it came to accessing the data meant the forensics team became part of the undercover investigation. The corporate investigation team was able to examine the computers used by company’s collections unit, under the auspices of addressing a computer virus. This allowed the team to collect data without the suspects having knowledge of what was taking place. Had the team lacked tight integration between investigators and forensic technologists, this would not have been possible.

**Special considerations for emerging markets**

With access to raw materials, cheap labour, energy sources and low-cost goods, growth in emerging markets is expected to outpace that of advanced economies by nearly four to one in 2013.

The largest emerging markets – the BRIC countries – have recently enacted or are considering data-protection legislation. UK and US investigators are focusing on these evolving and often unstable business markets for potential fraud and bribery. Thus these regions will invariably become the new frontier for data-protection conflicts.
Due to the increased economic and political instability of these regions, physical security can be an issue. Corporate officials, lawyers and other principals who travel in for an investigation may need security escorts. If tensions are high, the investigation site itself may require physical security. Although these situations are rare, they are serious; it is important to be proactive in assessing these risks.

**Missed opportunities and defensibility**

With the prevalence of email, text messaging and other electronic communication, the ability to exploit technology is integral to every investigation. Technology makes it possible to collect data from key custodians, uncover relationships and identify relevant product lines, deals or accounts. Armed with the right resources, investigative teams can conduct real-time searches that coincide with witness questioning to uncover falsehoods or corroborate statements. They can even use technology to reduce the likelihood of data-privacy violations. For example, in China, they can filter keywords that might implicate state secrets, prior to a review to eliminate potential exposure.

Unfortunately, many investigative teams fail to use technology effectively. Product choice can be limiting. Out-of-the box products can be difficult to customise to meet the specific parameters of a case. Advanced features like predictive coding, concept clustering and email threading may cost extra. If the product is not familiar to the investigative team members, they may lack the knowledge to use any of its complex features.

Having a multi-disciplinary team experienced in all stages of the Electronic Discovery Reference Model (EDRM) – from initial scoping and data collection to processing, filtering, hosting and producing documents – ensures data is tracked and accounted for at each stage, which is crucial in providing a defensible approach. This includes chain-of-custody logs, processing logs and exception reports.

Bringing in experts from outside the core investigative team to assist in searches can be beneficial, but increases risks. The more hands touch a project, the greater the likelihood of defensibility issues should something go wrong.

**Best practices for avoiding the unanticipated**

International data-privacy and data-transfer regulations affect virtually every investigation that crosses more than one international border. As such, data plays an important role in preventing, detecting and responding to allegations of corporate wrongdoing. To avoid the common pitfalls and minimise risks associated with cross-border investigations, consider the following practice points.

**Use plans to prevent, detect and respond**

Anti-corruption policies and data-management policies are at the heart of effectively managing the unanticipated when it comes to cross-border investigations. Prevent potential issues with in-house training, anti-corruption policies and comprehensive due diligence programmes to assess risk in the early stages of new projects. Whistle-blower lines provide a tool for early detection. And a swift, organised, proactive response will best position the company regardless of the extent of the issue.

Should a triggering event occur, be prepared to rapidly implement a defensible and cost-effective disclosure plan, including data analysis and collection, data processing and hosting, and early case analysis.

**Understand your data**

Anticipate the impact of data on your investigation early. Then determine the most effective way to collect and process data in a range of jurisdictions, considering varying international privacy laws.

At the onset of an investigation, map out the issues that will affect data. Consider the following factors.

1. What data needs to be collected?
2. Where is it located?
3. Can it be collected and processed – if so, how and where?
4. Can it be moved – if so, where and what are the potential implications?
5. What resources are needed and where are they located?
The complexities of transferring data across borders are quickly outpacing the logistical challenges of conducting the review within the country. If the decision is made to transfer data to another jurisdiction, consider who will do it, what the risks are and what, if any, security needs to be in place. If you conduct the review locally, identify the technology, team, cost and parameters needed to do so effectively.

Build the right team
When evaluating outside support, consider all your needs – legal, accounting, forensic, public relations and technology. The more fragmented a team, the greater the likelihood of defensibility issues, missed deadlines and loss of key intelligence.

Including many resources under a single umbrella improves efficiency and decreases the likelihood of mistakes, such as evidence slipping through the cracks. Multi-disciplinary teams typically have internal processes and know-how to work together; communication between team members is strong.

Technical experience
Consider the experience of your technical team. Investigators with access to proprietary review technology provide a real-time advantage to witness questioning. Used properly, they can interview witnesses and search for corroborating or contradicting electronic evidence to validate witness statements.

Form an integrated team that includes investigators working hand-in-hand with those handling the logistics of collecting and processing data. This will substantially reduce the likelihood of problems and, moreover, such a team offers credibility; a software company must justify its processes on its own.

Local knowledge
In cross-border investigations, local knowledge is paramount for human, physical and electronic evidence collection and analysis. A team that knows the local language, customs and laws will be better positioned to find witnesses, gather documents and collect data. It will be able to conduct more valuable interviews, find paper trails and search for key information.

Boots versus roots
Don’t mistake a team’s ability to fly to any location as being an advantage over a team with actual roots in the region. Organisations with a global footprint and strong roots in key markets offer greater resources, better communication and established processes for cross-jurisdictional matters. Such assets will increase the efficiency, effectiveness and overall defensibility of the investigation.

Rethink technical requirements
Electronic discovery and disclosure software has reached maturity. As technology continues to become more sophisticated and the market consolidates, there are new factors to consider when evaluating technology needs.

Instead of thinking of technology as a product, consider it a professional service. In other words, focus less on features and benefits and more on the services. More often than not, the team - not the technology - makes or breaks an investigation. Effective forensic searches lead to the identification of witnesses, and witness interviews can inform the development of effective searches. With predictive coding and other analytical capabilities, investigative teams can work faster and even more effectively to identify key pieces of information.

The most successful corporate investigative teams are those that have integrated proprietary technology and data-analysis experts. Such measures offer greater pricing predictability and allow for customisation and real-time reporting, to keep stakeholders informed and manage expectations.

The adage that older is better no longer holds true. Some of the more mature products on the market are working on older platforms that lack flexibility. Beware of products lacking integrated analytics that make review efficiency costly.

Newer platforms offer several benefits. The first is the ability to easily customise the platform to meet the specific needs of an organisation without having to wait for updates or patches. Additionally, newer platforms can more easily integrate advanced analytics into their base models, so taking advantage of technology is more cost effective.
Summary

We’ve entered an era in which cross-border investigations – from civil disputes and anti-corruption to anti-trust, fraud, supply chain and money laundering – play an increasingly important role in risk and reputation management. It is more important than ever to be able to deploy an international, multi-disciplinary team of investigators, legal technologies experts and legal practitioners with substantial local and technical knowledge. In the end, this will be the key to helping corporations and law firms evolve from Dickensian tactics to sophisticated, proactive approaches that improve their ability to anticipate the unexpected.

About Control Risks

Managing the risks and challenges of complex global investigations

Control Risks offers tailored investigation services to meet the unique discovery needs of organisations with legal matters, in complex and emerging markets around the world. From investigation through production, our global network of consultants provides integrity risk management services to securely manage the most vital electronic, human and physical evidence related to your case.

For litigation counsel: Control Risks allows you to co-ordinate the collection and analysis of evidence throughout all phases of the case. We offer the combined experience of on-the-ground investigators, state-of-the-art technology and eDiscovery experts with more than 60 years’ combined experience.

For review managers: We provide high-level analysis of data to keep your litigation team and clients informed about the case. This allows you to easily manage the progress of the review and keep reviewers reviewing.

For litigation support: We offer highly customisable and flexible technology that is easy to set up and secure. Our experienced project managers and technology team troubleshoot and address problems as they arise.
Contributing Authors

Geert Aalbers is the General Manager, Brazil and Director of Corporate Investigations Latin America. Based in São Paulo, he leads teams of consultants in Mexico City, Bogotá and São Paulo that focus on fraud prevention and investigations, anti-corruption and money laundering compliance, business intelligence, reputational due diligence, and asset tracing and litigation support.

Prior to joining Control Risks, Geert was Chief Financial Officer of Makro Venezuela, subsidiary of SHV Group, Netherlands. As CFO he managed all finance and controlling activities including treasury, tax, accounting, cost control, internal auditing and risk management in addition to being a member of the Board and Audit Committee. Before joining Makro, Geert worked at consultancy Roland Berger in São Paulo, and at Armstrong International in New York and London. Geert graduated cum laude in corporate law from the Erasmus University Rotterdam and holds a European Masters in Law & Economics from the same university. He completed an Executive MBA at Business School São Paulo, where he is presently an MBA program lecturer in Corporate Risk Management. Geert is a member of the Association of Certified Fraud Examiners (ACFE) and of the International Bar Association.

Mike Brown is Market Director for Legal Technologies in EMEA. An expert in e-discovery software and service, Mike is responsible for assisting clients in all aspects of preparing for, and responding to, investigations and litigation. This entails the provision of expertise and services to address the complexity of managing data protection/privacy issues in different jurisdictions across EMEA, particularly when dealing with US-based requests for data.

Mike has a long and successful track record in the legal technologies industry, from both a law firm and service provider perspective. Mike’s experience crosses industry sectors including financial services, pharmaceutical, defence, infrastructure, energy, technology, automotive and telecommunications, as well as public inquiries. Projects include Foreign Corrupt Practices Act (FCPA) and Office of Foreign Assets Control (OFAC) investigations; EU competition investigations; and requests for data from the Securities and Exchange Commission (SEC), the Department of Justice (DOJ), the Office of Fair Trading (OFT) and the Serious Fraud Office (SFO).

Mike is a regular speaker at legal conferences and an author in relevant industry media. He graduated with a BA in Business Information Systems from Nottingham Trent University in the UK.

Dmitri Hubbard is the Director, Legal Services Consulting, North Asia. He is a New Zealand qualified Barrister and Solicitor who has spent the last 15 years dealing with technology and law issues, first in the UK for a law firm and latterly in senior management for multinational corporations in Asia Pacific. He has conducted variously M&A, market research, green-fields sales operations, product development, litigation management and client development through the US, the UK, NZ, Australia, HK, Singapore, China, Korea, Macau, Taiwan, India and Malaysia. He has worked closely with clients within many of the world’s biggest law firms, corporations and investment banks on multinational issues.

Resident in HK since 2002, he has lectured at Chinese University of Hong Kong, The University of Hong Kong, and City University of Hong Kong on contract, tort, evidence, employment, commercial crime and criminal matters since 2003. He is a frequent speaker for HK CPD and RME courses on electronic discovery and restrictive covenants, and has spoken throughout Asia at different conferences on regulatory disputes, FCPA investigations, commercial crime, electronic discovery, arbitration and document review.

Ashley Smith is the Global Director of Project Management for Control Risks’ Legal Technologies practice. Her areas of expertise include electronic discovery, complex litigation technology solutions, product development, and project management. She has managed multiple international on-site investigations, consulting on the best practices for data collection, processing, review, and production.

Ashley has managed over 200 electronic discovery projects, including more than twenty Second Requests and several large FCPA matters, and has produced projects for virtually every government agency. She is a member of the Sedona Conference Working Group on International Electronic Information Management and Disclosure, as well as Electronic Document Retention and Production. Ashley was also a panelist at the Inter-Pacific Bar Association Annual Conference on Electronic Discovery.

Ashley is a Certified Computer Examiner (CCE #1443) and earned a Bachelor of Arts in English Language and Literature with a minor in Government from Smith College.
Control Risks' offices

abudhabi@controlrisks.com
alkhobar@controlrisks.com
algiers@controlrisks.com
amsterdam@controlrisks.com
baghdad@controlrisks.com
basra@controlrisks.com
beijing@controlrisks.com
berlin@controlrisks.com
bogota@controlrisks.com
copenhagen@controlrisks.com
delhi@controlrisks.com
dubai@controlrisks.com
erbil@controlrisks.com
hongkong@controlrisks.com
houston@controlrisks.com
islamabad@controlrisks.com
jakarta@controlrisks.com
johannesburg@controlrisks.com
lagos@controlrisks.com
london@controlrisks.com
losangeles@controlrisks.com
mexicocity@controlrisks.com
moscow@controlrisks.com
mumbai@controlrisks.com
newyork@controlrisks.com
panamacity@controlrisks.com
paris@controlrisks.com
saopaulo@controlrisks.com
shanghai@controlrisks.com
singapore@controlrisks.com
sydney@controlrisks.com
tokyo@controlrisks.com
washington@controlrisks.com

www.controlrisks.com