



# Risk Advisory

Helping our clients evaluate,  
manage and mitigate risk

Our clients face increasing levels of regulatory scrutiny in all aspects of their commercial life. This is complicated by the growing influence of US "long arm" sanctions which now have a potentially global impact. In many instances, securing and preserving evidence, both internal and from third parties, is an essential step to protect legitimate interests. In this edition of Risk Advisory we focus on how to gather and protect evidence and on recent regulatory developments in the US.



"...securing and preserving evidence both internally and from third parties is an essential step to protect legitimate interests."

Articles by two experts from our Corporate Investigations team provide introductions to the importance of proper evidence collection. Simon Dawson, who heads the Corporate Investigations division, provides guidelines to be used in preparing civil search orders. Michael Penhallurick, a new member of the team, distils the benefits of virtual forensic computing.

Following these insights, we are pleased to include a specially-commissioned article by Michael O'Kane, a partner at Peters & Peters, on the ramifications of ongoing cases and recent trends on US liability for foreign cartel activity. Finally, John Gilliland and Kathryn Cameron Atkinson of Miller & Chevalier, a Washington-DC based law firm, discuss the impact of Washington's recent political scandals on US lobbying culture.

It is our view that these articles offer a useful overview of recent developments and what our clients can do to effectively protect their interests.

We hope you enjoy the articles.

**Bill Waite**  
Group Chief Executive

## IN THIS ISSUE:

- 2 The execution of civil search orders
- 3 Virtual forensic computing
- 4 UK liability in the US for cartel activity
- 5 Washington scandals likely to change lobbying landscape

THE RISK ADVISORY GROUP  
FEBRUARY 2006



# The execution of civil search orders

*Simon Dawson, The Risk Advisory Group*

## Introduction

Civil search orders are very powerful tools in the litigation process. As their name suggests, civil search orders allow a litigating party to enter the premises of another party, without notice, in order to search and seize any material relevant to that party's case.

Rather than discussing the legal requirements that must be met before an order can be obtained, this article distils practical points, which have been compiled from first-hand experience in assisting with the execution of many civil search orders, for the whole team.

## Phase 1 - Reconnaissance, administration and preparation

The first step is to establish the locations to be visited, their occupancy and internal layouts by a pre-execution surveillance operation, if possible. For this, detailed instructions and a full briefing from our client, which is usually a law firm, is essential for success.

Next the locations should be visited to:

- Gather covert photography
- Establish a reconnaissance position
- Identify parking and route from parking to office/residence
- Establish number of exits and consider any CCTV/security measures in place
- Identify a position to monitor the location if the search is suspended
- Identify local facilities (toilets, shops, cafes)
- Attempt to establish the number of computers, operating systems, networks and presence of fax machines, PDAs or phones

“...civil search orders allow a litigating party to enter the premises of another party without notice...”

It is also important to:

- Establish routes to locations from start point
- Identify the local police stations and their contact number should there be any violence or threat of violence during the execution of the order.
- Decide groupings for each location and any language skills needed
- Consult legal team to draft court order, identify names and prepare affidavits
- Organise suitable transport and refreshments

Preparation of appropriate and fully functioning equipment is vital. This should include:

- Digital cameras for each exit
- Computer forensic equipment
- Laptops
- Write blocking devices/computer forensic software
- Sufficient spare storage media to cover all eventualities
- A varied supply of connectors and leads
- Evidence bags
- Examination Schedule to make contemporaneous notes
- Tape, tags and ties for securing draws, lockers, and rooms

Finally:

- Draw up a comprehensive contact list
- Plan to cover each location through the night and into the next day
- Consider manpower and logistics if other locations come to light during the search
- Ensure that the security and computer forensic teams have business cards and are fully briefed
- Ensure that the physical security team is aware of the appropriate action to be taken if persons are observed removing items from the premises, i.e. inform them that they should not remove anything from the premise unless permission has been given. If the persons still persist, then their place, date, time and actions are to be noted and a photograph should be taken of the individuals concerned.

## Phase 2 - Execution of the order

A proper briefing before the order is executed is essential and should cover the status of the operation thus far and:

- Ensure that the team is ready in time. Be prepared for a long wait and a sliding departure schedule to deal with last minute legal issues
- Identify all team leaders and the individual in overall command
- If more than one location is to be visited, coordinate so all locations are served at the same time
- Low-key physical security should be afforded at the point of entry
- All entrances and exits should be covered as the civil search warrant is served



- Be prepared for another long wait while the other side contacts their lawyers
- Computer forensic team should liaise closely with the lawyers, updating them on estimated completion times
- If the search cannot be completed during normal working hours it may be suspended to continue in the morning. If this is the case, the areas that have not been searched need to be sealed. There may also be a requirement to monitor the entrances and exits during this period
- Have the flexibility to re-task both security and computer forensic assets when new locations need to be searched. Understand that completion times vary
- Make contingency plans for an overnight stay

### Phase 3 - Execution and follow up work

Finally we cover several important points that relate to matters arising during or after the execution of the order.

- The order will allow access from 9 am, but there is always a delay!
- The supervising solicitor may take up to an hour to explain the contents of the order to the other side.
- They will want to seek legal advice, which may take between one and three hours depending on solicitor's availability
- The supervising solicitor, applicant's solicitor and the respondent's solicitors will then meet to discuss the

“...with forethought, planning and good communication throughout, the risks of problems will be minimised...”

order and agree on the “terms of engagement”

- The above discussions and procedures will mean that in practical terms, the search is unlikely to begin before noon.
- This in turn means that it is highly likely that the search team will need to return on the following day. Arrangements for overnight security must therefore be considered in all cases.
- The computer forensic team should follow the Association of Chief Police Officers' Computer Forensic Guidelines throughout for evidence acquisition and storage and ensure that all actions are fully and properly documented.
- Remember that you will not get access to the material immediately and it is important to maintain contact with the computer forensic team so that an appropriate timetable and protocol for analysis and searching can be prepared.

### Conclusion

There are many matters which need to be considered in addition to the strict legal considerations on the strength of the applicant's case and the appropriateness of applying for an order. However, with forethought, planning and good communication throughout, the risks of problems will be minimised. Regardless, remember that even the best general's plans rarely survive the first clash of arms.

Simon Dawson is Head of Corporate Investigations at The Risk Advisory Group. If you would like to know more about this topic, please contact him at [simon.dawson@riskadvisory.net](mailto:simon.dawson@riskadvisory.net)



## Virtual forensic computing

*Michael Penhallurick, The Risk Advisory Group*

The science of forensic computing encompasses the identification, analysis, preservation, and presentation of digital evidence in a legally acceptable manner, covering not only computers, but all manner of digital storage devices. This retrieval is undertaken using accepted and proven concepts of digital image acquisition. Subsequent to acquisition, a number of specialist “forensic” tools can be used on the secured data in order to perform detailed examinations. The forensic methodology enables an investigator to report upon their findings and allows them to reach conclusions based upon the scrutinised material, without altering any of the original material.

There are a vast number of specialist tools available to an investigator to assist in the analysis of acquired digital media. Whilst such tools can and do provide a great depth of analysis, it is possible that the “scene of crime” part of the examination process is often overlooked as an additional and perhaps valuable source of information.

Although forensic computing provides great insight into both current and previous activity on a system, the actual environment that a user would experience often remains unvisited during a forensic examination.

Using a clone of a user’s original system provides the best method to gain a feel for what a user would have seen, how he had his desktop settings, and the actual software he used.

Hard disk cloning provides a method by which the original system can be used, just as a user would have seen it, by copying the original disk and placing it back into the original machine.

But what if the original machine is not available? Or indeed it may have been damaged and the hard drive containing the data is all that has been obtained? Any cloned disk will need to be hosted in a different computer environment – one which will doubtless modify some of the settings of the original. Each time the machine is started, changes will be made to the cloned disk – to replicate the processes will involve time-intensive re-cloning of the original.

Virtual Forensic Computing, or more accurately, “methodologies for using virtual environments to access cloned/mounted subject hard disk images”, details an investigation into the restoration of forensically acquired digital data to virtual hardware. The objective of the investigation was to devise a methodology by which a subject operating system could be operated within a wholly virtual environment, in order to enable the investigator to experience the subject system in a controlled environment where file system changes could be discarded and the “original” clone pre-

served for future, repeatable usage, with relatively minimal time-overheads.

In certain circumstances, it is possible to create a forensically sound virtual clone of a subject computer within minutes of completing the forensic acquisition process. In other circumstances, it is necessary to “clone” out the original disk (from the secure forensic copy), to a “virtual disk” that can be operated inside the virtual machine, in essence exactly as if “real” physical hardware were to be used.

When referring to forensically sound, it is necessary to consider the four Principles of Computer Based Electronic Evidence, as detailed in the Association of Chief Police Officers Good Practice Guide for Computer based Electronic Evidence.

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

By utilising the Virtual Forensic Computing methodology, all aspects of these principles are adhered to, in as much as any subject machine is not accessed other than through a secure forensic image or a “virtual” clone thereof.

The systems researched and activated using the methods described encompasses Windows 95/98/ME & Windows NT/2000/XP. The methods employed were found to be successful for Intel-to-Intel restorations.

Michael Penhallurick is Computer Forensics Manager at The Risk Advisory Group. If you would like to know more about this topic, please contact him at [michael.penhallurick@riskadvisory.net](mailto:michael.penhallurick@riskadvisory.net) or visit [www.riskadvisory.net](http://www.riskadvisory.net) to view Michael’s thesis.



## UK liability in the US for cartel activity

*Michael O'Kane, Peters & Peters*

The ongoing case of Ian Norris, former CEO of Morgan Crucible, highlights the need for UK companies to pay special attention to their potential exposure in the US for breaches of competition law. Unlike European jurisdictions which have sought to regulate rather than prosecute 'hard core' anti competitive practices, the US has demonstrated an increasing appetite to treat such activity as 'white collar' crime.

The reach of US jurisdiction for such offences is extensive, and exacerbated by the fact that almost all financial crimes are now extraditable under the 2003 UK-US Extradition Treaty. The arrangements controversially dispense with the requirement for the US to support requests with evidence. Furthermore although Norris was indicted in the US for cartel practices which occurred before the 2003 introduction of a specific cartel offence in the UK, the UK court found that such activity could have been prosecuted domestically as conspiracy to defraud. The court approved the extradition request and the Secretary of State ordered Norris to be extradited. He has appealed and been granted permission to apply for a judicial review of the US-UK extradition arrangements.

His case is indicative of the clear desire of the US Department of Justice (DOJ) to continue its focus on international cartels. The prospect of detection and prosecution of UK individuals is further increased by the DOJ's success over the last decade. Of the more than \$2 billion dollars in criminal fines imposed in the last six years, over 90% was obtained

in connection with the prosecution of international cartel activity. Recent figures reveal that approximately 50% of corporate defendants in recent criminal cases brought by the DOJ were based abroad. The average prison sentence is 18 months but the maximum sentence has recently been increased from five to ten years, with companies facing a recently increased maximum fine of \$100 million for each offence. In addition, the OECD has similarly encouraged its members to cooperate in combating the most powerful and successful cartels.

However it is not all bad news for those who discover such activity within their UK companies. Unlike other crimes, it is possible for corporates and individuals to obtain complete immunity from criminal and civil liability, provided they come clean at a relatively early stage and comply with standard conditions. In fact the US has attributed the large number of international cartel cases it investigates to its leniency regime, and claims that the regime has directly led to the detection and successful prosecution of more international cartels than all of its investigative powers combined.

Although Morgan Crucible obtained corporate leniency from the European Union, one of the clear lessons of the Norris case is that any corporate or individual considering their position must ensure that any such immunity and/or leniency applications are made simultaneously in all relevant jurisdictions, but particularly in the US.

**"...almost all financial crimes are now extraditable under the 2003 UK-US Extradition Treaty."**

Michael O'Kane is a Partner at Peters & Peters and a member of their Cartel team. Peters & Peters is a law firm which specialises in international fraud related work.



## Washington scandals likely to change lobbying landscape

*John Gilliland and Kathryn Cameron Atkinson, Miller & Chevalier*

From *Credit Mobilier* to Watergate, Washington scandals have become something of a rite of passage for each generation. This time, however, the scandals are coming in waves in an election year and when the Republican Party's ability to maintain majority control is already in question. Although the long-term consequences of the scandals are unclear and will depend on America's voters, in the short term, the rules of the lobbying game will likely change, affecting even routine relationships among lobbyists, legislators, and congressional staffs. Of equal importance, industries and interests who hire lobbyists will themselves face demands for greater transparency surrounding their activities in Washington. For all parties involved in the lobbying process, the political stakes are high.

### From K Street With Love

The biggest news came on 3 January, when lobbyist Jack Abramoff, a longtime Republican activist and ally of House Majority Leader Tom DeLay (R-TX), pleaded guilty to corruption charges stemming from his misuse of client funds and illegal gifts and perks he bestowed upon various members of Congress in exchange for their help on legislation. A former business partner, Michael Scanlon, who also once worked for DeLay, pleaded guilty to similar charges last year. In exchange for their pleas, Abramoff and Scanlon agreed to cooperate with prosecutors and provide the names of legislators and staff who accepted the illegal gifts and perks. It remains to be seen whether additional targets will be named.

The Abramoff plea came just weeks after the unrelated resignation of a well-known legislator, Rep. Randy "Duke" Cunningham (R-CA), for allegedly accepting gifts from federal contractors whose business interests fell under the jurisdiction of his committee. News of the Cunningham plea was largely eclipsed by the developments associated with DeLay's indictment for alleged fundraising misdeeds in Texas. Meanwhile, showing that corruption is problematic in both parties, the press has reported that Rep. William Jefferson (D-LA) solicited bribes in exchange for his support of African business interests, and that investigators found bags of cash in his home freezer.

### Competing Proposals for Reform

On 8 January, the Speaker of the House, Dennis Hastert (R-IL), announced that he would push for a major lobbying reform package designed to reduce the influence of perks and gifts on individual Members and their staffs. Ten days later, senior Democrats from both chambers offered a sweeping reform package of their own. Not to be outdone, Senate Republicans declared their intention to introduce reform proposals in early March. From this collection of proposals, several specific ideas relevant to companies active in

or entering the lobbying arena have emerged.

First, some proposals would further circumscribe direct interactions between lobbyists and legislators and their staffs. For example, privately-funded 'fact-finding' travel for members and staffs would be outlawed. Rules allowing lunches or other small gifts that do not exceed \$50 would be tightened. And, the current one-year ban on lobbying activities by former legislators and staff would be extended to two years.

*"...the rules of the lobbying game will likely change..."*

Other proposals seek to improve transparency in the lobbying community. The Senate Republican proposal would require lobbyists to disclose more information regarding their employers' identities and financial interests. A group of conservative House Republicans has even proposed that Congress should impose limits on its own procedures by prohibiting a practice known as "earmarking," in which senior legislators carve out federal funds for favoured projects late in the legislative process. Doing so allows them to circumvent lengthy procedural steps that others could use to block the earmark.

Finally, the Democrat package targets failings associated with the Bush Administration or Republican leadership on Capitol Hill. For example, the proposal targets the "K Street Project", the label given to a House Republican effort to pressure lobbying firms and organisations to hire only Republicans in exchange for better access to lawmakers. The proposal would also impose stronger disclosure and conflict of interest standards on corporations that win federal contracts -- an idea labelled the "Halliburton Reform", after the defence firm once run by Vice-President Cheney that was awarded several high-profile contracts for the reconstruction of Iraq.

### What Lies Ahead

Although they may not stop future Abramoffs, some reforms are probably inevitable. Lobbyists, and their clients, will almost certainly face more stringent disclosure rules. Companies that hire lobbyists will face greater public scrutiny and debate over their activities and interests. This scrutiny may persuade publicity-shy companies not to wade into Washington's lobbying waters at all, and should serve as an additional cautionary flag to all who swim in them.

Kathryn Cameron Atkinson is a Partner and John Gilliland is Counsel at Miller and Chevalier Chartered, a Washington DC law firm specialising in tax, international trade, government contracts, government affairs, fraud and white collar criminal defence, employee benefits and ERISA, and related federal litigation.