THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 7 | Number 1 Article 5

2012

Applying the ACPO Principles in Public Cloud Forensic Investigations

Harjinder S. Lallie
University of Warwick, Coventry

Lee Pimlott

Applying the ACPO Principles in Public Cloud Forensic Investigations

Harjinder Singh Lallie
International Digital Laboratory (WMG)
University of Warwick, Coventry, CV4 7AL
h.s.lallie@warwick.ac.uk
(0044)7956-837371

Lee Pimlott
19c High Street, Kilburn, Belper, Derbyshire DE56 0NS,
lee.pimlott@gmail.com

ABSTRACT

The numerous advantages offered by cloud computing has fuelled its growth and has made it one of the most significant of current computing trends. The same advantages have created complex issues for those conducting digital forensic investigations. Digital forensic investigators rely on the ACPO (Association of Chief Police Officers) or similar guidelines when conducting an investigation, however the guidelines make no reference to some of the issues presented by cloud investigations. This study investigates the impact of cloud computing on ACPO's core principles and asks whether these principles can still be applied in a cloud investigation and the challenges presented thereof. We conclude that the ACPO principles can generally be upheld but that additional precautions must be taken throughout the investigation.

Keywords: ACPO, Evidence, Investigation, Cloud computing, Digital Investigation Guidelines

1. INTRODUCTION

Cloud computing has generally received considerable interest from researchers in recent years, a lot of this research has been focussed particularly on security and privacy (Birk, 2011; Casey & Stellatos, 2008; Chen, Paxson, & Katz, 2010; Joint, Baker, & Eccles, 2009), possibly because cloud security seems to be the most frequently cited concern on the part of business leaders surveyed by organisations such as Gartner (Brodkin, 2008) and IDC (Mullins, 2010).

Research into cloud forensic investigation has tended to focus on two key areas: the use of the cloud in aiding investigations; and the investigation of incidents involving the cloud. The present text focuses on the investigation of the cloud rather than the use of the cloud in aiding investigations.

Some of the complexities of the acquisition process where data is in the cloud,

have previously been outlined by Navetta (2009), Shipley (2009), Taylor, Haggerty, Gresty, and Lamb (2011), and Reilly, Wren, and Berry (2011). Taylor et al. (2011) have outlined further complexities of cloud investigation and Reilly et al. (2011) note the difficulties in applying guidelines to a cloud investigation and also the benefits that cloud computing may provide in assisting an investigation wherein the tremendous storage offered by the cloud could be used to store digital forensic images and the computational power of the cloud may assist in cracking passwords and in processing the case. Birk (2011) has explored some of the complexities of investigating various cloud platforms and presents a very useful insight into the problems encountered in investigating Software as a Service (SaaS), Platform as a Service (PaaS), and Information as a Service (IaaS).

Where cloud systems incorporate elements of virtualisation, there are particular benefits which have been outlined by Reilly et al. (2011) and Bem & Huebner (2007), who note that the imaging of virtual systems (whether live or off-line) can be easier in comparison with normal non-virtualised systems. Birk (2011) notes that the *snapshot* feature which was introduced to a number of hypervisors (Xen, VMware, etc.) can be the equivalent of a forensic image of the cloud storage system.

Whereas there is some research conducted into the investigation of cloud systems, Beebe (2009) has noted that there is still considerable scope for further research and the European Network and Information Security Agency (ENISA) has highlighted forensics and evidence gathering mechanisms as priority areas of research (ENISA, 2009).

This study focuses on the issue of digital forensic guidelines, more specifically the Association of Chief Police Officers (ACPO) 'Good Practice Guide for Computer-Based Electronic Evidence' guidelines (referred to hereon simply as 'the ACPO guidelines' or 'the ACPO principles') and the challenges in applying them to a cloud investigation.

The ACPO guidelines consist of a set of four principles and then the detailed guidelines, they are aimed specifically at 'police officers, police staff, and private sector investigators working in conjunction with law enforcement' (ACPO, 1998). The original guidelines were developed in consultation with a digital forensics consultancy called 7Safe (7Safe, 2011) and whilst they were originally aimed specifically at the law enforcement agencies in the UK, they have come into general use throughout many digital forensic investigations.

The rest of this paper is structured as follows. We begin in section 0 by presenting a short review of the ACPO guidelines. The study proceeds to exploring issues relating to the interpretation of the ACPO guidelines and the case – if any, for reviewing these to include cloud computing. The cloud models and the challenges of investigating public clouds (versus private clouds) are analysed next in section 3. This is followed in section 4 by an analysis of each of the ACPO principles and their application in cloud investigations, we proceed in the same section to

analyse some of the particular problems and challenges posed by public cloud investigations and the contextual application of the ACPO guidelines.

2. INVESTIGATIVE GUIDELINES AND THE INTERPRETATION OF THE ACPO GUIDELINES IN CLOUD FORENSIC INVESTIGATIONS

The ACPO 'Good Practice Guide for Computer-Based Electronic Evidence' guidelines have become the standard for UK based digital investigations. They have also become accepted in most other EU countries (Mason, 2008) and for many law enforcement agencies around the world (Janes, 2006) - most of which have no similar guidelines relating to the collection and management of electronic evidence.

The ACPO guidelines however are not universally accepted, Belgium and the USA are two notable exceptions. In the USA, there are specific guidelines relating to evidence acquisition from mobile devices (Jansen & Ayers, 2007), electronic evidence seizure guidelines for the United States Secret Services (USSS, 2006), electronic evidence seizure guidelines for US law enforcement (USDOJ, 2009), and, in the past, there have even been guidelines for Internet Service Providers (ISPs) (USISPA, 2003).

It is beyond the remit of this study to explore the content and scope of all these respective guidelines, however by considering the ACPO guidelines as an example, the digital forensics community should be better placed to contextualise some of the arguments presented herein. Furthermore, there are some views that the ACPO guidelines are more matured and perhaps the most practical of the published guidelines (Casey, 2011), we therefore consider that it may be pertinent to use these guidelines as an example and proceed to consider some of the complexities in applying the ACPO principles to cloud investigations.

Adoption of the ACPO guidelines in a UK investigation ensures that a legally accepted process is followed in the investigation. The importance of robust guidelines was demonstrated in 1997 (before the guidelines were published) when the case of Police Sergeant Gurpal Virdi vs Metropolitan Police Service (MPS) demonstrated the repercussions of failing to follow best practice guidelines (MPA, 2001). Turner (2001) notes that in this case the handling of computer evidence was inadequate and had there been such guidance at the time of the investigation, it is likely that the mistakes of this landmark case might have been avoided.

Whilst the guidelines were developed within the area of law enforcement, they can be applied to any investigation that may involve digital evidence, numerous private companies (CFA, 2009; Disklabs, 2008; 7Safe, 2011) have adopted these as a standard. Jones & Valli (2009) have highlighted the benefits of this approach by warning that what may start as a civil litigation inquiry may ultimately become a criminal investigation.

The traditional approach to a digital forensic investigation involves seizing

computer equipment such as a personal computer and extracting evidence from the device in a forensically sound manner. This approach generally involves the investigation of equipment that is tangible and normally easily isolated from a network or intranet. Where the device is not easily isolated, network forensics and real time (live) forensic techniques can be used to investigate the device and some of the network components.

The ACPO guidelines have previously been updated to reflect the increased use of home networks and mobile devices. The advent of cloud computing represents a significant development of technology and raises the question as to whether future versions of the guidelines should be updated to reflect best practice in conducting cloud investigations.

Owen & Thomas (2009) have criticised the lack of specific guidance for the investigation of mobile devices. They argue that the integrity of evidence extracted from the device can be jeopardised if issues facing an investigator are not covered in the guidelines. However this raises particular questions about the depth that the guidelines can be expected to cover and also whether a cloud investigation could be jeopardised due to its lack of coverage in the guidelines.

The difficulties in applying the ACPO guidelines in a cloud investigation and achieving a successful subsequent prosecution have previously been outlined by Reilly et al. (2011) and also by Taylor et al. (2011). Taylor et al., believe that the guidelines:

> cover crime scenes on the internet, in terms of the forensic examination of physical devices connected to the Internet, and the necessity in some instances of capturing evidence directly from the Internet possibly during 'live' interaction with a suspect or by capturing live website content. The use of checkpoints might be useful in order to make live systems easier to analyse. The ACPO guide also provides advice regarding the difficulty in capturing evidence where target machine(s) may be sited outside UK jurisdiction.

What Taylor et al. (2011) seem to suggest is that the guidelines are sufficiently generic for an investigator to be able to contextualise them, this is a view echoed by Marshall (2008) as well who adds that the terms 'law enforcement' (from Principle 1) and 'case officer' (from Principle 4) could be substituted for 'investigator' and 'manager' respectively, showing that the principles can easily be adapted for a commercial investigation and presumably a cloud investigation.

Mobile device technology has changed significantly from the point it was incorporated within the guidelines to today, however if the changes are taken out of their historical context they are quite incremental. This incremental development becomes significant over time and has resulted in an increased use of *phone apps*, some of which give users access to a vast amount of cloud storage (Evernote, 2010) and processing power providing more sophisticated and flexible

applications (Qamar et al., 2010).

Should the guidelines be technology specific and receive revisions with each incremental development or when a 'significant' change has taken place? If it is to be the latter, then how do we determine when a change is significant? The question of whether cloud computing is a significant change for investigators might be determined by the number of cases being dealt with. As yet there seems little empirical data which confirms the level of cloud investigations being undertaken by law enforcement agencies.

Given the global context (which is not of course new), it may be useful to consider a proposal for developing a set of international guidelines which may in turn be more appropriate for investigating digital investigation cases which so clearly cross jurisdictional boundaries. Such work has been undertaken in other contexts (Hesser, 2010).

3. THE PROBLEMS WITH INVESTIGATING THE PUBLIC CLOUD

The way in which an investigation will be conducted (in terms of complexity and procedures followed) will depend largely on whether the cloud under investigation is a public or private cloud. Mell and Grance (2011) and NIST (2011) defines three service models (SaaS, PaaS, and IaaS) and four main deployment models (public, private, community or hybrid).

This research focuses primarily on the public cloud infrastructure although some of the issues discussed herein will apply to one or more of the deployment models. Private clouds are a more popular way in which to outsource IT through tailor made contracts and are generally easier to investigate in comparison with public clouds. In a private cloud, the data stores, IT infrastructure (servers and network components) and the personnel are in known locations and are generally accessible. The organisation is generally familiar with the applications used to access the data stores and manage the servers, they are familiar with the audit trail systems used (assuming that they are used of course). The personnel involved in managing the services are in the employ (either directly or contractually) of the company and in general there is a lot more *certainty* surrounding the investigation.

Public clouds are owned by an organisation – a Cloud Services Provider (CSP) that sells its cloud computing services to public and business users. Public clouds have the potential to be the more popular implementation of the cloud (Armburst, 2009) particularly as they are more universally available.

Badger, Grance, Patt-Corner, and Voas (2011) suggest that where SaaS is used as the cloud service, the investigative responsibility lies with the CSP, in an IaaS model with the subscriber (with perhaps some collaboration with the provider) and in a PaaS model the responsibility may be split between the two.

The primary difficulty of investigating a public cloud is highlighted by Taylor et

al. (2011) who add that the problem is not that data may be located remotely, but being able to prove *actus reus*, i.e., that of "a specific person undertaking a specific action at a specified time, date and place". This in turn is related to a number of issues which arise primarily out of the uncertainty of the location of data stores, the ownership of those data stores and platform related issues more specifically because:

- A public cloud storage infrastructure may consist of dozens of server farms/data stores, some of which may be dynamically routed and stored, i.e. the data is not held in a *fixed* geographical location. There are numerous reasons for the dynamic routing and storing of data, some of which are highlighted by Qureshi (2008) who outlines economic benefits to be achieved therein. The investigator needs to identify the precise locations of the data stores so as to be able to acquire the evidence source, this may be very difficult in such an environment.
- The movement of data makes it difficult to develop an accurate timeline, this is a problem partially related to the way in which metadata is stored/managed. The file metadata does not store information relating to file movement, how therefore would an investigator identify the movements of data over a period of a month for the purpose of developing the timeline from the metadata? If anything a cloud investigation requires heightened awareness to assist in being able to develop a timeline, any evidence found on the local machine pointing to artefacts that might have been accessed in the cloud has to be correlated with the evidence found on a local machine pointing to that interaction. Clock synchronisation across data centres may also impact on the ability to develop an accurate timeline.

4. APPLYING THE ACPO PRINCIPLES IN PUBLIC CLOUD INVESTIGATIONS

Given the difficulties in investigating the cloud and the views relating to the applicability (or contextualisation) of the ACPO guidelines, we now proceed to exploring the central question of this study by analysing each of the four ACPO principles in the context of a public cloud investigation and asking whether each of the four principles can be upheld in a cloud investigation.

4.1 Implications on data integrity due to delay related loss of control (Principle 1)

From the moment the investigation begins to the point that physical seizure of the data store takes place by the relevant investigator/case technician, a significant time gap may have elapsed, particularly if the data is located in another legal

jurisdiction. Effectively the investigator loses control of the investigation for a short period – an issue previously highlighted by Cunningham (2009) and Shipley (2009). This increases the risk of the evidence becoming corrupted, a 'live data store' may have changed significantly in the interim period. The first principle of the ACPO guidelines states that:

> 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

The challenge presented by the first ACPO principle in a cloud investigation in comparison with a normal investigation, is the in the *remoteness* of the data source and it is this remoteness that takes some control away from the investigator.

Furthermore, the issue under investigation may not be a crime in the local jurisdiction (discussed further in §0) therefore placing no compulsion on the CSP to cooperate. Should the CSP be willing to cooperate, they may place very specific restrictions on the investigation particularly as the data store to be investigated may contain data belonging to other organisations outside of the investigation. This issue has recently been extended by Badger et al. (2011) who point to concerns regarding the release of audit logs and log data wherein some of that data also may belong to third parties which are not within the scope of the investigation.

At this juncture it is useful to note that there is scope for CSPs to collectively begin establishing forensic readiness plans and establishing measures to demonstrate that they are capable of conducting sound investigations. A forensic readiness plan would:

- Better guide the investigation
- Answer some of the issued raised in this study
- Become a key selling point for service providers as the cloud market matures and competition increases

In the absence of a forensic readiness plan, and given that the investigator is endeavouring to acquire (image) the data source at the earliest opportunity, the following alternatives are presented:

- Relying on a case technician at the CSP to properly acquire the data store
- Achieving mutual agreement with the CSP to involve a local 3rd party case technician in the investigation
- Performing a remote acquisition of the data store.

Often the remote acquisition (given the nature of the data source) may have to be

a live remote acquisition – a prospect that has hitherto perhaps been given less consideration. The issue of live forensics has previously been highlighted as an area of considerable growth (Adelstein, 2006), the growth of cloud computing makes this more likely in such investigation cases.

We can summarise that whilst it is possible to expedite the imaging of the data store, it is likely that there will be a delay in acquiring that data store due to its remoteness and that this is not as a result of direct action taken by the investigator.

4.2 Competency (Principle 2)

The involvement of a third party in the investigation raises particular concerns regarding the competency of the third party investigator. The second principle states that:

> In 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.

The issue of competency in this context relates to two particular points – competency in giving evidence and competency in being able to handle and investigate the evidence. The former is less of an issue as a competent investigator should be able to give evidence relating to that investigation – notwithstanding some of the challenges therein which are discussed later in this section.

With the absence of an internationally recognised standard, the competency of an *agent* conducting any part of the investigation overseas could be brought into scrutiny; however we argue that the issue of competency in a cloud investigation is not that different to a normal localised investigation and that it should be just as easy to demonstrate competency in this scenario.

Competency in the digital forensics domain can generally be demonstrated through any or a combination of:

- Advanced academic study in a relevant field
- Advanced professional/vendor certification
- Experience in the field
- Demonstrable adherence to recognised standards

All except the last can be demonstrated by 3rd parties in the investigation, however, the issue of recognised standards in digital investigation (or in this case a lack thereof) is both a UK problem as well as an international one and is therefore not unique in this context. The closest that there may be in terms of an international standard may be ISO 17025 which some UK law enforcement agencies require.

The case for the requirement of an international standard in digital forensics has

been well made (Barbara, 2005; Jones, 2004; Meyers & Rogers, 2004; Schwerha, 2008; Yasinsac et al., 2003; Young, 2007). The second consultation draft of The Forensic Science Regulator's Codes of Practice and Conduct, states that "*The forensic examination of computers and telephones is a common aspect of police investigations leading to the production of intelligence and evidence. This is a forensic process and must be subject to the same standards as other forensic processes"* (Home Office, 2010). The Digital Forensics Specialist Group has identified digital forensics as a growing area of police business (in the UK) which specifically suffers from a lack of scientific quality standards, stating that police, digital forensic practitioners and academic scientists have expressed a need for both "*process standards, governing the production of digital forensic evidence and standards of individual competence"* (Home Office, 2008, section 6.1.2).

The absence of national and international standardisation in this area does not mean that competency cannot be proven, we have already highlighted above that competency can be demonstrated through other means. Three further issues relating to competency do however apply in the context of a cloud investigation:

- Extended technical competency
- Extended competency in giving evidence
- The complexity of a multitude of bespoke/customised/virtualised systems

A case manager should be able to demonstrate 'additional competency' to what s/he might already be used to so as to demonstrate a clear understanding of cloud computing technology, the legal context and the challenges arising thereof of a cloud investigation and in further demonstrating that all precautions and considerations were taken throughout the investigation.

Whereas the explanation of technical IT related concepts to juries may already be an issue, there are further challenges presented in being able to explain the technicalities of cloud computing and most importantly the technicalities of extracting evidence from the cloud to a jury.

The issue of competency is complicated somewhat because the investigator may be dealing with complex and often bespoke (customised) systems some of which may be virtualised (although one would assume that they support a recognised file system). Taylor et al. (2011) have noted that the cross platform nature of cloud computing means that the tools used to undertake an investigation must be able to support these platforms, such tools may not exist and there becomes an increased requirement for investigator training.

We conclude that the issue of competency in a cloud investigation can be easily adhered to but that an investigator needs to demonstrate extended competence in understanding cloud technology and then subsequently being able to explain this to a jury.

4.3 Maintaining an Audit Trail (Principle 3)

The distributed nature of the data stores presents problems in being able to record an accurate audit trail. In a cloud investigation the investigator may need to access and image multiple data stores which are held in separate geographic locations and jurisdictions. Realistically these may need to be accessed and imaged by local case technicians as discussed in §0. The third ACPO principle requires that:

> 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.

In the context of a cloud investigation, this principle presents a challenge and the case manager would need to maintain and consolidate a consistent audit trail between the case technicians and his/her own audit trail of the investigation. In such instances, it may useful to formulate a specific agreement through Mutual Legal Assistance Treaties (MLAT) protocols which may provide an opportunity for declaring and agreeing the principles for the investigation at the outset.

4.4 Legal Jurisdiction (Principle 4)

There are very particular legal complexities (beyond the scope of this article's remit) presented by an international cloud investigation. Some of these have been highlighted by Frowen (2009) who identifies the 'legal and legislative hurdles' facing those involved in international investigations. We highlight some of the issues briefly herein. The fourth principles states that:

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

This raises the question as to whether the spirit of this principle refers to the UK law, the overseas law or both. The fourth ACPO principle becomes more difficult to apply particularly where the issue under investigation does not contravene local jurisdiction.

International investigations involving a G8 country would normally involve a request through the appropriate law enforcement agency (for instance, Serious Organised Crime Agency) who would issue a request for their counterparts in the G8 country to secure the data (thereby generating the appropriate summons, subpoena, search warrant etc.). If the country is not a member of the G8, there may be specific trans-national agreements between the two countries amounting to the same. An officer of the law in the local jurisdiction would enter the premises (of the CSP) with the corresponding local warrant or authority.

Some of the issues outlined herein could probably be resolved somewhat if there

were clear guidelines which more specifically directed a cloud investigation, as we have established, no such guidelines presently exist.

The issue of ensuring that the law is adhered to is a particular problem in a cloud investigation and often the best that an investigator might be able to achieve is to ensure that the local law (at the origin of the investigation) is indeed adhered to.

5. CONCLUSIONS

We set out in this manuscript to consider whether the core ACPO principles could be applied and upheld within a cloud investigation scenario. Within that context we sought also to consider some of the challenges involved in applying these principles.

We have recognised that there is a lack of specific guidelines for cloud investigation and that upholding the ACPO principles in particular within the context of a cloud investigation is problematic for a number of reasons cited herein but in brief include: complexities relating to the distribution of the data stores, associated problems with metadata, a general lack of control over the investigation and the problems associated with maintaining an audit trail.

We have suggested that some of the issues may be offset by relying on third party investigators and with the investigators (whether third party or not) needing to demonstrate additional competency in understanding cloud technology and being able to competently perform the investigation notwithstanding its remoteness. The issue of the audit trail can be overcome through increased collaboration, organisation and mutual agreement between the investigators.

ACKNOWLEDGMENTS

Steve Edwards (Forensic lead at the Police Central eCrime Unit (PCeU) and Chairman of the ACPO review board for the guidelines on computer evidence.). Harry Parsonage (former Detective Sergeant at Nottinghamshire Police Digital Forensics Unit and Member of the ACPO review board for the guidelines on computer evidence). Jelle Niemantsverdriet (Principal Consultant, Forensics and Investigative Response at Verizon Business Security Solutions and Member of the ACPO review board for the guidelines on computer evidence). Simon Janes (Operations Director at Computer Forensic Alliance, Former Head of Scotland Yard's Computer Crime Unit and co-author of the original ACPO guidelines). Nigel Jones MBE (Director at Technology Risk Limited and co-author of the original ACPO guidelines). Paul Wright (MEA Principal Consultant at Verizon Business).

REFERENCES

7Safe. (2011) Computer Forensics Services. Retrieved April 18, 2012, from http://7safe.com/computer_forensics.html

Adelstein, F. (2006) Live forensics: diagnosing your system without killing it first. *Communications of the ACM*, *49*(2), 63-66.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2009) *Above the Clouds: A Berkeley View of Cloud Computing*. Electrical Engineering and Computer Sciences, University of California at Berkeley Technical Report No. UCB/EECS-2009-28. Retrieved April 18, 2012, from http://www.eecs.harvard.edu/cs261/papers/armbrust09.pdf

Association of Chief Police Officers (ACPO). (1998). *Good Practice Guide For Computer Based Evidence*. Kent: ACPO Crime Committee.

Association of Chief Police Officers (ACPO). (2007). *Good Practice Guide for Computer based Electronic Evidence*. Retrieved April 18, 2012, from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). *DRAFT Cloud Computing Synopsis and Recommendations*. NIST Special Publication 800-146. Gaithersburg, MD: National Institute of Standards and Technology.

Barbara, J.J. (2005). Digital evidence accreditation in the corporate and business environment. *Journal of Digital investigation*, *2*(2), 137-146.

Beebe, N. (2009) Digital Forensic Research: The Good, The Bad and the Unaddressed, In: G. Peterson & S. Shenoi (eds), *Advances in Digital Forensics V*, IFIP AICT 306. Germany: Springer, pp. 17-36.

Bem, B. & Huebner, E. (2007). Computer Forensic Analysis in a virtual environment. *International Journal of Digital Evidence*, *6*(2). Retrieved April 18, 2012, from http://www.utica.edu/academic/institutes/ecii/publications/articles/1C349F35-C73B-DB8A-926F9F46623A1842.pdf

Biggs, S. & Vidalis, S. (2009). Cloud computing: The impact on digital forensic investigations. In *Proceedings of the international conference for Internet technology and secured transactions*, pp. 1-6.

Birk, D. & Wegener, C. (2011). Technical Issues of Forensic Investigations in Cloud Computing Environments. In *Proceedings of the 6th International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, CA.

Brodkin, J. (2008). *Gartner: Seven cloud-computing security risks*. Retrieved April 18, 2012, from http://www.networkworld.com/news/2008/070208-cloud.html

Casey, E. (2011). *Digital Evidence and Computer Crime*, 3rd ed. New York: Academic Press.

Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *SIGOPS Operating Systems Review*, *42*(3), 93-98.

Chen, Y., Paxson, V. & Katz, R. H. (2010). *What's new about cloud computing security*? Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley.

Computer Forensic Alliance (CFA). (2009). Computer Forensic Investigations. Retrieved April 18, 2012, from http://www.cfauk.com /Computer%20Forensics%20Page.htm

Cunningham, P. (2009). Three cloud computing risks to consider. Retrieved April 18, 2012, from http://www.arma.org/press/ARMAnews/Infosecurity.pdf

Disklabs. (2008). Computer Forensics. Retrieved April 18, 2012, from http://www.disklabs.com/computer-forensics.asp

European Network and Information Security Agency (ENISA). (2009). Cloud Computing. Benefits, risks and recommendations for information security. Retrieved April 18, 2012, from http://www.enisa.europa.eu/act/rm/files /deliverables/cloud-computing-risk-assessment

Evernote Corporation. (2010). Evernote. [Online]. Retrieved April 18, 2012, from http://www.evernote.com/

Frowen, A. (2010). Cloud Computing and Computer Forensics. Retrieved April 18, 2012, from http://www.intaforensics.com/Blog/Cloud-Computing-And-Computer-Forensics.aspx

Hesser, W., Feilzer, A., & de Vries, H. (2010). *Standardisation in Companies and Markets*, 3rd ed. Helmut-Schmidt-Universität, Hamburg.

Home Office. (2008). *The Forensic Science Regulator Business Plan 2008/09 – 2010/11*. Retrieved April 18, 2012, from http://www.homeoffice.gov.uk /publications/police/operational-policing/Forensic_Science_Regulator_3.pdf

Home Office. (2010). *Quality Standards Codes of Practice. Second Consultation Draft, July 2010*. Retrieved April 18, 2012, from http://www.homeoffice.gov.uk/publications/police/forensic-science-regulator1/quality-standards-codes-practice

Janes, S. (2006). The effective response to computer crime. Retrieved April 18, 2012, from http://www.computerweekly.com/Articles/2006/03/21/214830/The-effective-response-to-computer-crime.htm

Jansen, W. & Ayers, R. (2007). *Guidelines on Cell Phone Forensics*. NIST Special Publication 800-101. Gaithersburg, MD: National Institute of Standards and Technology.

Joint, A., Baker, E. & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer Law & Security Review*, *25*(3), 270-274.

Jones, A. & Valli, C. (2009). *Building a Digital Forensic Laboratory*. Burlington, MA: Elsevier.

Jones, N. (2004). Training and accreditation – who are the experts? *Journal of Digital Investigation*, *1*(3), 189-194.

Marshall, A. (2008). *Digital Forensics: Digital Evidence in Criminal Investigations*. Chichester: John Wiley & Sons, Ltd.

Mason, S. (ed.). (2008). *International Electronic Evidence*. London: British Institute of International and Comparative Law.

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. Gaithersburg, MD: National Institute of Standards and Technology.

Metropolitan Police Authority (MPA). (2001). *The Virdi Inquiry Report*. Retrieved April 18, 2012, from http://www.mpa.gov.uk/downloads/scrutinites /virdi/virdi-report-01a.pdf

Meyers, M. & Rogers, M. (2004). Computer Forensics: The Need for Standardisation and Certification. *International Journal of Digital Evidence, 3*(2). Retrieved April 18, 2012, from http://www.tech.purdue.edu/Cpt/Courses /TECH581A/meyersrogers_ijde.pdf

Mullins, R. (2010). IDC Survey: Risk In The Cloud. Retrieved April 18, 2012, from http://www.networkcomputing.com/cloud-computing/229501529

Navetta, D. (2009). Legal Implications of Cloud Computing – Part One (the Basics and Framing the Issues). Retrieved April 18, 2012, from http://www.infolawgroup.com/2009/08/tags/security/legal-implications-of-cloud-computing-part-one-the-basics-and-framing-the-issues/

NIST. (2011). Cloud Computing at NIST: Two New Draft Documents and a Wiki. Retrieved April 18, 2012, from http://www.nist.gov/itl/csd/cloud-020111.cfm

Owen, P. & Thomas, P. (2009). Analysis of the Methodology used in Digital Forensic Examinations – Mobile Devices Vs Computer Hard Dis*k*. In *Proceedings of the 3rd International Conference on Cybercrime Forensics Education and Training*. Canterbury, Canterbury Christ Church University, 1-2 September 2009.

Qamar, S., Lal, N. & Singh, M. (2010). Internet Ware Cloud Computing: Challenges. *International Journal of Computer Science and Information Security*, *7*(3), 206-210.

Qureshi, A. (2008). Plugging Into Energy. In *Proceedings of the 7th ACM Workshop on Hot Topics in Networks (HotNets)*. Calgary, Canada, October 2008.

Reilly, D., Wren, C., & Berry, T. (2011). Cloud Computing: Pros and Cons for Computer Forensic Investigations. *International Journal of Multimedia and Image Processing (IJMIP)*, *1*(1-2), 26-34.

Schwerha, J.J. (2008). Why computer forensic professionals shouldn't be required to have private investigator licenses. *Journal of Digital Investigation*, *5*(1-2), 71-72.

Shipley, T.G. (2009). Collection of Evidence from the Internet, Part 2. Retrieved April 18, 2012, from http://www.dfinews.com/article/collection-evidence-internet-part-2?pid=778

Taylor, M., Haggerty, J., Gresty, D. & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, *2011*(3), 4-10.

Turner, M.J.L. (2001). Case of Sergeant Gurpal Virdi. *Computers and Law*, *6*(11). Retrieved April 18, 2012, from http://www.computerevidence.co.uk /Cases/Virdi/Articles/Virdi.htm

U.S. Department of Justice (USDOJ). (2009). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Retrieved April 18, 2012, from http://*www.lb9.uscourts.gov/webcites /08documents/CDT_cyber.pdf*

U.S. Internet Service Provider Association (USISPA). (2003). *Electronic Evidence Compliance – A guide For Internet Service Providers*. Berkeley Technology Law Journal, *18*, 945-986.

United States Secret Service (USSS). (2006). *Best practices for seizing electronic Evidence v.3*. US Department of Homeland Security. Retrieved April 18, 2012, from http://info.publicintelligence.net/usssbestpractices.pdf

Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M., & Sommer, M.S. (2003). Computer Forensic Education. *IEEE Security and Privacy*, *1*(4), 15-23.

Young, T. (2007). Digital forensics lack standards. Retrieved April 18, 2012, from http://www.computing.co.uk/ctg/news/1838051/digital-forensics-lack-standards

AUTHOR BIOGRAPHIES

Harjinder Singh Lallie (BSc., MSc., MPhil, ABCS) is a senior teaching fellow in Cybersecurity at the University of Warwick (International Digital Laboratory, WMG). He has previously led courses successfully in Digital Forensics and Security at the University of Derby. His research focus is in the area of Digital Forensics and Information Security and is currently studying towards his PhD.

Lee Pimlott (BSc., MSc.) has over 15 years ICT work experience, from which he recently took a sabbatical to undertake a Masters in Forensic Computing & Security at the University of Derby, graduating with Distinction. Lee currently works in London for a leading global digital risk management and investigations firm.