Name: Jamie Cropley
P Number: P15188432
Module: CTEC1412 - Law Component
Date: 19th of April 2016

Discuss and critically assess the Association of Chief Police Officers (ACPO) Guidelines for the investigation of computer crime

The Association of Chief Police Officers (ACPO) can be defined as a body that deals with the development of policing practices in the United Kingdom. They developed a set of guidelines for the Investigation of computer crimes whilst mainly aimed at the practise of digital forensics these guidelines can be useful for a variety of professions that have to deal with the various and ever changing aspects of digital evidence, therefore it is a guide designed to be an underlying structure to what would be required when working with Digital Forensic Units.

The initial aspects of this guide indicates how technology changes and such for example the last version used to refer to computer based evidence but the most current version now refers to digital based evidence and tries to include the ever changing diversity of the digital world.

The guide is written around the original four guiding principles which are listed in short as below, for digital forensics with slight amendment to the wording of principle four. Although these four principles give a good basic plan on how to deal with digital evidence, consideration still must be taken on how evidence is generally dealt with regarding the skills, processes and capacities. Much more detail is encompassed within this guide to cover as much of this area of digital evidence as possible and its practices therein.

- To not change any of the evidence for example the date.
- Only a competent person should access the data.
- Keep an audit trail that others can follow.
- The person in charge of the investigation has overall responsibility.

There are four key areas in the ACPO guidelines,this is split up into four chapters which consist of how to plan, capture, analyse and present forms of digital evidence these as such I believe are the key areas of the ACPO guidelines. Plan gives an idea of the rough areas as to where digital evidence can be found, it also advises such investigative professionals to be aware of the ‘Regulation of Investigatory Powers Act 2000 (RIPA)’. Capture goes into detail on how to preserve and manage data at a

crime scene. Analyse entails the investigator to prepare data or such digital devices for a forensic specialist to analyse and review such evidence to prepare so that it is suitable for presentation in front of a court, which would be the final key area of the guide, present advises such investigator on how to basically bring everything together in respect of this guide, statements, evidences and such so that it is amicable to present in front of a court.

It is common that such obtained evidence by utilising the aforementioned areas, is organised and registered using the popular software known as EnCase Forensic, this software is designed to simplify the process of evidence gathering and make it easier to present such evidence to a court. This software works well with the ACPO guidelines in respect of plan, capture, analyse and present, the software allows for evidence to be triaged, collected, processed, analyzed and reports to be created which are all synonymous almost apart from the word triaged. Although you can apply the ACPO guidelines to the use of this specific software in this respect, the ACPO guidelines themselves barely make any such reference to utilisation of such software which I believe is beneficial as it allows the guidelines to be applied to different types of cases, evidence and situations more easily.

Triage is a term used in the context of investigations where a particular framework is utilised in order to prioritise and organise evidence or data in terms of urgency, this allows for better and more efficient allocation of resources during an investigation. Despite its advantageous uses in this profession, three writers (Graeme Horsman, Christopher Laing, Paul Vickers: 2014) question that triage generally is not an effective method used throughout investigations within regards to reliability of identifying evidential data, they believe that based on various studies that the “Case-Based Reasoning Forensic Triager (CBR-FT) framework is a method for collecting and reusing past digital forensic investigation data in order to highlight likely evidential areas on a suspect operating system” Graeme Horsman, Christopher Laing, Paul Vicker (Elsevier, 2014, p69) based on twenty test triage examinations that CBR-FT was a more effective method of triage in comparison to standard triage methods, this was also compared with an investigator using a leading commercial application such as encase.

Even through utilising such methods as triage, by solely using the ACPO guidelines on there own throughout an investigation, I believe them to be ambiguous in the way they are put across. Technology is inevitably progressing at a fast rate, I do not think law is struggling to keep up with it however I believe law is struggling to interpret it and put certain aspects across to the right people in the right way. A Satellite Navigation system inside a vehicle to most people would be solely considered a

single use type of device where it simply navigates its user to a chosen destination, however a computer hacker would see such a device as many different things from a storage device to navigation system that utilises satellites. Although this is mentioned in the ACPO guidelines under Appendix C as “Mobile devices which have wireless connectivity/ communications capability (such as tablet computers and satellite navigation systems) fall under the heading of 'mobile devices'.” (ACPO,2012,p31).

If seen only from the non-hacker perspective, it would be down to the forensics in the majority of cases to interpret the device as something more, but what if such a system is part of another system, for example a navigation system can be part of robotic type of cars, it would use this system to navigate then link to other systems almost like a human body relies on different organs for different tasks, it may be possible therefore to link via the flow of data into different parts of this complex robotic car, break up the data and encrypt it so much it becomes invisible, although this is a somewhat hypothetical scenario I fail to see that the ACPO guidelines go into this type of complexity, therefore they do not interpret technology well. The ACPO guidelines do not mention anything at all in relation to the word robot however it does mention something in relation to such an automated system but in a very outdated context, under the section mobile phones point 6 it indicates “Be aware that some mobile phone handsets may have automatic housekeeping functions, which clear data after a number of days.” (ACPO,2012,p33)

Data can be manipulated and moved around automatically but there is no more complex mentions of this throughout the ACPO guidelines, I believe that it lacks an ability to help such a person using the guidelines be able to think in a more abstract and complex manner about retrieving data off all types of digital devices. Another good example is the guide makes no mention of steganography which is the ability to conceal data within data, for example you could store some type of data that is crucial to an investigation like bank account details within a photographic image which would not be visible unless decoded, in a sense the data is encrypted and invisible to the naked eye. There are many difficulties that arise when utilising the ACPO guidelines, some of that which include the aforementioned hidden data, investigating the cloud and using it within other frameworks where they may contradict the goals of an investigation.

The law, I believe covers a vast range of elements in relation to technology however it is apparent that due to lack of updates in such guidelines as ACPO for example, it would be better to define technology in a more abstract way than specifically listing

types of technology, this I believe would make such guidelines more compatible with the law.

The case where the founder of the Jimmy Choo shoe empire, hired a private investigator to hack his wife to spy on her financial transaction during a harsh divorce, is a good example of where certain aspects of the law and its investigations are not carried out appropriately, currently private investigators are not required to be licensed in England, however most tend to use certain guidelines, laws and such to carry out their job to ensure it is done ethically and legally, this notion rather than the case itself can show an example of malpractice without the intent of doing so. Private investigators adhere to all different standards across the country, it can quickly become difficult and complex to determine where the law is being broken on certain cases, how can the public determine whether an investigative professional as such is actually legitimate or not, this can make a simple instance of something technological turn quite complex in terms of the law as it currently stands because it is difficult for them in that profession to always apply the correct legalities to every situation.

I believe such aforementioned methods and such along with the ACPO guidelines and the law can all be beneficial sometimes within regards to some circumstances, when a member of the hacking group known as Anonymous, which are a very large scale hacking group, hacked the British Pregnancy Advisory service although not specified it seems apparent from the article that he was quickly apprehended and prosecuted under the ‘Computer Misuse Act 1990’ which specifically covers illegal unauthorised access to a computer and its data therein.

The creation of the ‘Computer Misuse Act 1990’ led from the case of R V Gold & Schifreen (1988), this case utilised aspects of the ‘Forgery and Counterfeiting Act 1981’ to bring about a prosecution based on the aspect that they obtained unauthorised access to various computers comprised in the Prestel Computer Network owned and operated by British Telecommunications Plc., they were prosecuted under this act by means of the data that was obtained and in the way that they impersonated someone else, to access the Prestel database they needed to register or impersonate another user whilst accessing the system. The initial point from this case is that the ‘Computer Misuse Act 1990’ derived from this case which shows the law can be a strong tool in bringing about prosecution even if such technology and laws do not exist yet.

It is apparent the ACPO guidelines can work under certain frameworks, different types of investigations and work well with certain laws and such, however I conclude

that it is not an easy task for them to do so, where the ACPO guidelines are defined as a series of guidelines to that of which I believe should only aid such investigations in the area of computer crimes, the main points being that they are outdated in some respects, ambiguous and not fully consistent with the possible and concurrent varying types of investigations that investigators may or will come across in the area of computer crime.

There can be so many different possible combinations and comparisons of how the ACPO can be implemented and utilised overall, I believe it sets a good basis for future and current implications of computer crime especially in regards to ascertaining and dealing with forensic evidence appropriately. In conclusion it should always be taken with caution, it is completely apparent that the ACPO guidelines now or in the future can not fundamentally be the only guide you use and rely upon to carry out an investigation especially to that of which is in the area of computer crime.

(Total word count: 1926 words.)

Bibliography:

- *Computer Misuse act 1990*

- *Forgery and Counterfeiting Act 1981*

- GALLAGHER, P. (2012) Abortion website hacker caught. *TheGuardian*, 11th Mar. Available from: http://www.guardian.co.uk [Accessed 31/03/2016].

- GUIDANCE SOFTWARE, INC. (2016) *EnCase Forensic.* [Online]. Available from: http://www.guidancesoftware.com/encase-forensic [Accessed 31/03/2016].

- HALIL IBRAHIM, B., GUCLU YAVUZCAN, H., AND OZEL, M. (2013) Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Elsevier - Forensic Science International,* 233, pp. 244-256.

- JONES, A., VALLI C., DARDICK, G. and SUTHERLAND, I. (2007) The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market. *Journal of Digital Forensics, Security and Law,* 3 (1), pp. 5-24.

- LALLIE, H.S. and PIMLOTT, P. (2012) Applying the ACPO Principles in Public Cloud Forensic Investigations. *Journal of Digital Forensics, Security and Law,* 7 (1), pp. 71-86.

- LAWINDEXPRO (n.d.) *Regina -v- Stephen William Gold, and Robert Jonathan Schifreen.* [Online] Available from: http://www.swarb.co.uk/c/hl/1988r_goldschifreen.html [Accessed 31/03/2016].

- OWEN, P. and THOMAS, P., (2011) An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. *Elsevier - Digital Investigation,* 8, pp. 135 - 140.

- *Regulation of Investigatory Powers Act 2000*

- SUTHERLAND, I., DAVIES, G., PRINGLE, N., and BLYTH, A. (2009) The Impact of Hard Disk Firmware Steganography on Computer Forensics. *Journal of Digital Forensics, Security and Law,* 4 (2), pp. 73-84.

- TAYLOR, M. (2007) Choo founder's ex-husband cleared of spying on her. *TheGuardian*, 27th Jun. Available from: http://www.guardian.co.uk [Accessed 31/03/2016].

- VAN BAAR, R.B., VAN BEEK, H.M.A. and VAN EIJK, E.J. (2014) Digital Forensics as a Service: A game changer. *Elsevier - Digital Investigation,* 11, pp. S54-S62.

References:

- ASSOCIATION OF CHIEF POLICE OFFICERS (2012) *Good Practice Guide for ComputerBased Electronic Evidence.* London: ACPO.

- LAING, C., HORSMAN, G. and VICKERS, P. (2014) A case-based reasoning method for locating evidence during digital forensic device triage. *Elsevier - Decision Support Systems*, 61, pp. 69-78.