Can we continue to effectively police digital crime?

Abstract
Now approximately 30 years old, the field of digital forensics is arguably facing some of its greatest challenges to date. Whilst currently supporting law enforcement in numerous criminal cases annually, questions are beginning to emerge regarding whether it can sustain this contribution, with digital crime remaining prevalent. In his first live interview in September 2015, Head of MI5, Andrew Parker indicated that individuals are now engaging in computing acts which are beyond the control of authorities, confirming earlier remarks made by British Prime Minister David Cameron in the wake of the Charlie Hebdo attacks. Such comments cast doubt on the future effectiveness of the digital forensic discipline and its ability to effectively investigate those who implement the latest forms of technology to carry out illicit acts. This article debates the controversial question, could we be facing an era where digital crime can no longer be effectively policed?

Keywords: Cyber-crime; Digital Forensics; Security; Crime; Research.

1 Introduction

Thought of by many to be within its infancy (Reilly et al., 2011; Lang et al., 2014), such statements regarding the field of digital forensics (DF) are arguably no longer accurate. These perceptions are largely due to societal and technological developments, brought into public consciousness through mounting media coverage, coinciding with increasing computer usage and volumes of digital crime (UNODC, 2013). Since the turn of the millennium, DF has played a major role in digital crime detection and prevention despite being in existence since the 1980's, when the first incidences of computer crime were witnessed (Sommer, 2004). When quantified, the field of DF is around 30 years old and is now a well-established branch of forensic science, embedded into criminal and civil legal practices worldwide where the acquisition and interpretation of digital evidence is often required. Subsequently DF evidence has featured prominently in a number of high profile investigations including those of Dr. Conrad Murray in the trial of Michael Jackson's death (BBC News, 2011), Dr. Harold Shipman, one of the United Kingdom's (UK) most prolific serial killers (Graham, 2010), Lost Prophets member Iain Waktins (BBC News, 2013) and recently convicted athlete Oscar Pistorius (BBC News, 2014a).

The discipline of DF was established in response to the increased availability and affordability of digital devices in order to tackle their potential illicit use. What followed; the commercialisation of the Internet and an unprecedented growth in technology as many services sought to migrate to the digital realm throughout the 1990s, only further highlighted the need for this form of forensic analysis. Some 25 years later, society is now wholly reliant on digital technologies for all aspects of life, ultimately providing an environment that has allowed digital crime to flourish.

As digital devices are now intermeshed into almost all criminal offences, DF is arguably the most active of all our forensic science disciplines, backed by frequent reports of case backlogs, which continue to grow (Overill and Jantje, 2013; Shaw and Browne, 2013; BBC News, 2014b). We now have both cyber-dependant (offences which can only be committed using technology) and cyber-enabled (offences exacerbated by technology) offences (McGuire and Dowling, 2013) as well as instances of digital content indirectly supporting

criminal investigations (for example, through acts such as bystander footage of illegal events captured by portable media recording devices). As a result, DF evidence is frequently used in a court of law to support the criminal justice system (De Santis et al., 2011). There is no doubt that the DF discipline has, and presently does support the fight against digital crime but the question remains as to whether this can be sustained.

1.1 Signs of change

Doubts regarding the continued effectiveness of the DF discipline were first cast in 2010, when Garfinkel suggested that the golden age of DF was reaching an end, a controversial statement given society's dependence upon it had never been greater. Now, some six years later there are increasing signs that Garfinkel's statement was accurate, as the DF field faces some of its greatest challenges yet.

Following attacks in France on the offices of Charlie Hebdo, British Prime Minster David Cameron, pledged to fight against the use of encrypted communication protocols and the haven they provide for terrorist collaboration (BBC News, 2015a). In doing so, he provided a worrying insight into a current inability to effectively police this activity, with Balogun and Zhu (2013) indicating that around 60% of cases where encryption is involved end up non-prosecutable. This was followed in September 2015, by Andrew Parker, Head of MI5s first live interview where it was suggested that individuals were engaging in computing acts which were beyond the control of authorities (BBC News, 2015b). These announcements form part of a general trend in comments indicating techniques used to commit digital crimes are becoming more effective. Following the 'Paris attacks' orchestrated on 13th November 2015, once again, this debate was raised again, where data obfuscation techniques were once again the target of blame (BBC News, 2015c). Michael Morell, former head of the CIA drew attention to the implications of media sensationalism in response to the Edward Snowden revelations and its potential to have driven the development of a security and privacy conscious generation (Hirsh, 2015). Although it is yet to be definitively established, it is suspected that terrorist communication in the lead up to these events utilized encryption techniques, placing it beyond the interpretation of government officials (BBC News, 2015c; Hirsh, 2015). We have now reached a point where privacy is at the forefront of the minds of criminals where those determined to communicate without detection can frequently do so.

Facilities such as online anonymous markets are also regularly reported to have equipped criminals with the tools they need to carry out their illicit acts, with trade continuing to thrive (Phelps and watt, 2014). The Deep Web offers access to a host of unlawful services, widely reported to place those who engage with it, beyond detection (Houses of Parliament, 2015). Moore and Rid (2016) have highlighted the "overwhelming presence of illicit content on the Tor darknet" ranging from facilities to purchase drugs, weapons and illegal imagery. In addition, there are now a host of hacktivist groups operating beyond law enforcement control implementing online attacks against individuals and organisations, acting on socio-political motives. The Internet now plays a role in almost all digital crimes, and it remains debatable as to whether it is now beyond the capability of current law enforcement to police it effectively. In fact, one could almost place the problem of exacerbated levels of digital crime almost exclusively at the foot of the Internet and network technologies. Despite the implementation of filtering techniques to prohibit access to illegal content, combined with the efforts of organisations like the Virtual Global Taskforce and The Internet Crime Complaint Center to police online actions, digital crime online still remains prevalent. A useful example

is provided by the UK Parliament (Thompson, 2015), who reported that 12% of European Internet users have had social media or email accounts hacked, with 7% falling victim to online fraud.

Brown (2015) states, with increasing rates of digital crime, one would expect rates of conviction to follow suit, yet this has not been the case. The Internet now provides the main platform for a number of offences, not least the acquisition and distribution of images depicting child sexual abuse. These offences have now become widespread with the volume of illegal images in circulation beyond current quantification methods. As a result, concerns have been raised regarding law enforcement's ability to cope with the influx of cases requiring a DF examination (BBC News 2014c). Figures provided by the Child Exploitation and Online Protection Centre (CEOP) “show that only one in every 15 people caught viewing child pornography on the Internet is arrested” (House of Commons, 2013a) and the Internet Watch Foundation (2013) suggests that despite estimates of 1.5 million people having seen illegal imagery on the Internet, online 40,000 have reported it (House of Commons, 2013b). The Internet has simply become too large to manage given currently available resources, providing a problem source for DF practitioners. Even where criminals opt-out of implementing techniques to obfuscate their behavior through services like Tor, it remains possible that their actions will remain undetected, potentially hidden in plain sight due to the vast amount of activity which takes place on a daily basis. Or perhaps controversially, they cannot be processed by law enforcement through limitations in available resources or due to triage policies. Case backlogs are now reported globally, where specific examples include the Scottish Police Authority (2015) who detail a 47% rise in the need for DF investigations in the last two years. Pressure is growing on practitioners, requiring them to process larger volumes of digital data quicker despite leading to a greater chance of human error (Turner, 2007; Bjelland et al., 2014). Triage techniques are often seen as a viable solution, yet an inherent risk of missing evidential data persists.

The discipline of DF is unquestionably now facing a rising number of issues which must be faced head on. It is both at its most advanced stage in terms of available analysis techniques, whilst remaining more vulnerable than ever. Despite research indicating those who commit crime maintain a lower standard of edification (Webbink et al., 2008) or on average are less intelligent than non-criminals (Kanazawa, 2010), Education in the context of digital crimes cannot be discounted as a catalyst for digital crime and is now discussed.

2 A smarter cybercriminal?

Providing a starting point for discussions, issues which may be overlooked when considering the threats to the continued effectiveness of DF are the changing demographic of society, the availability of scientific computing knowledge and their combined impact on digital crime. There is a fundamental alteration occurring within current cultures where an increasing younger populous of computer-savvy individuals are replacing an older, more computer-illiterate generation. With this in mind, it should be questioned as to whether this natural progression is in part responsible for a new wave of digital crime and in addition, a smarter digital criminal when combined with the increased availability of computing knowledge.

For those of an older cohort, a first taste of computing stemmed from the first realistically priced devices such as the Commodore 64 or Amiga computing systems. Their functionality is considered archaic in comparison to what is witnessed now, a factor that limited the

amount of ‘damage’ a cyber-criminal could commit, in contrast to today’s technology. Now, computers are available to the masses in developed countries, with around 3.1 billion Internet users, a figure that has tripled in the last 10 years (Statista, 2015). As more individuals maintain a digital profile, the pool of targets from which cyber-criminals have to target is far greater which has inevitably increased the risk of becoming a victim of digital crime. This is confirmed by the National Crime Agency (2016) which estimates that in 2015, acts of cyber-enabled fraud accounted for 36% of the total volume of crime in the United Kingdom. Yet it is not just changing technology usage which poses a challenge, with levels of a user’s computing knowledge continuing to increase.

It is important to state that by no means does this article condemn formal computing education or suggest it is responsible for increasing acts of digital crime, which is vital for the development of the computing field. In fact it has helped to support the development of core aspects of the field of computing, including sub-disciplines designed to tackle acts of digital crime including online security, cybercrime countermeasures and DF. Whilst profiling research often focuses on the attacks themselves (Alazab, 2015), published work on cyber-criminal characteristics and demographics is sparse. There is no published content offering a definitive link between those who commit digital crime and their levels of education. However, as with all learning, its application can be for both constructive and destructive means. Education itself is not to blame, but we must accept that increased knowledge and awareness of IT systems, coupled with an inquisitive mind, is likely to have not only led to the design of applications and services that benefit society, but also for the active recognition of methods for abusing technology for the purpose of deviant behaviour. The availability of computing information which can be acquired at a relative ease is arguably a contributing factor, leading to a more informed society and potentially, a more informed cyber-criminal.

Individuals are now better equipped to facilitate their interest in computing which is no longer just for the ‘hobbyists’; instead an affordable activity forming a fundamental part of many school and college curricular. Although not representative of the cyber-criminal populous, Xu et al’s (2013) survey into the development of young hackers found that all but one participant maintained an interest in computing from a young age. In the UK, computing education now commences at a significantly younger age, covering a more complex syllabus than ever seen before, with a number of nationwide projects such as ‘Code Clubs’, designed to introduce children as young as nine, to the principles of programming (Code Club, 2014). Such initiatives are in no way to blame for any future act of cybercrime committed by an attendee, but we must accept that a an increased exposure to these activities (as in many other disciplines) may result in more individuals seeking an interest in ways to exploit such technology.

Consideration must also be given to the wealth of resources available to a wannabe cybercriminal in order to self-educate on the principles of planning and committing a successful digital offence, where the finger of blame has already been pointed at individuals like Edward Snowden and their role in publicising encryption technologies for covert communications (Hirsh, 2015). The media also plays a role, popularising technological development and bringing it to the forefront of societal attention (see for example articles discussing the anonymizing online provision Tor - BBC News (2016a); BBC News (2016b) McGoogan (2016)). As a result, it would not take long for an individual, even with limited computing knowledge, to identify technology which could facilitate their acts of cybercrime.

Other prime examples include academic portals used to publish the latest strategies and techniques for crime fighting, practitioner driven forums and blogs. Whilst facilitating the development of the DF discipline through contributions of valuable knowledge to support practitioners, conversely it provides an insight into the principles and practices, even the investigatory limitations of those tackling cybercrime. This issue exists in many disciplines associated with the regulation and prevention of criminal acts, where there are limited solutions.

Often publications document the latest examination techniques and findings where a passive observer is free to gather reconnaissance to support any malicious purposes. Whilst this information requires a level of knowledge to successfully interpret and therefore utilize in a criminal capacity, it is not beyond possibility that such contributions to knowledge directly contribute to the intelligence of cyber criminals. This is acknowledged in Young et al's., (2007) survey of hackers in attendance of the 'DEFense readiness CONdition' (DEFCON) hacking conference, highlighting that educational resources are acknowledged as a source of information by those who have committed illegal hacking acts. Further, Bratus (2007) indicates that many of those carrying out acts of hacking acquire knowledge from both educational (textbooks) and practitioner based platforms (forums etc.). This aligns with comments from Radziwill et al., (2015) suggesting that those seeking to 'hack', in absence of education will simply self-teach using available resources. However, such potential issues are an inevitable byproduct of living in an information-rich society. Cronan et al's., (2006) historic survey indicating that 34% of university students respondents had committed a digital offence of software misuse/privacy, where those with a greater degree of exposure to computing more likely to commit an offence. The problem remains that those educating themselves may lack in-depth understanding of the associated ethical and legal issues in areas of computing which arguably increases the potential for abuse of this knowledge. This is often part of many formal educational institutes core computing syllabuses ensuring students understand the consequences of the misapplication of their actions (Radziwill et al., 2015).

The problem of available knowledge is one which cannot be controlled. Now, resources will always be available to educate those who seek it on almost any topic of their choosing. This can almost exclusively be put down to the Internet, a tool so powerful that in 2011 access to it was considered by the United Nations Human Rights Council (2011) to be a basic human right. However, eradication of online materials which could support criminal behaviour is impossible.

It would seem that we are reaching a time where reliance is placed on the consensus that perpetrators lack the drive to gather reconnaissance regarding a criminal act they plan to carry out in order to increase their chance of success. Morell worryingly revealed the following insight into these concerns in light of the Paris Attacks.

> *'First, ISIS went to school on how we were collecting intelligence on terrorist organizations by using telecommunications technologies. And when they learned that from the Snowden disclosures, they were able to adapt to it and essentially go silent ... And so, part of their rise was understanding what our capabilities were, adjusting to them so we couldn't see them. No doubt in my mind (Hirsh, 2015)'.*

These comments suggest that the exposure of weaknesses in current analysis methods are leaving society vulnerable. Further, it seems to demonstrate the anxiety underpinning phenomena such as ‘the CSI effect’.

2.1 The CSI Effect

The CSI (crime scene investigation) effect has spawned as a direct result of increased media coverage of criminal investigations, glamorised by popular television shows (McDonald, 2008; Overill, 2013). Often cited as having a negative effect on the expectations of juries with regards to forensic evidence, fears have emerged that it may also have an influence on criminal behavior and the use of countermeasures (Ferguson, 2013). Concerns have been raised by Overill (2013) who suggests that perpetrators are now more aware of the audit trails left behind by their criminal acts and may often take steps to remove these traces. Although the impact of the CSI effect continues to be monitored and evaluated, when coupled with the availability of resources online to educate individuals, it provides a tangible risk. Those who are aware of the evidence left behind by their actions and have the knowledge to effectively destroy it move one step closer to committing a ‘perfect crime’ type scenario, placing evidence beyond the grasp of current crime analysis techniques. Although such scenarios may seem confined to works of fiction, simple Google searching provides a number of resources documenting methods for digital evidence removal or obfuscation. To provide an example, Tor Metrics provides a means of estimating the number of users of the Tor Network. In January 2012, estimated user numbers are placed at around 530,000 (TorMetrics, 2016a). Now, In January 2016, numbers are approximately 1,900,000 (TorMetrics, 2016b). Further, usage increased to over 5,000,000 after the disclosures made by Edward Snowden in 2013 (TorMetrics, 2016c).

Again, the CSI effect only forms part of the bigger problem posed by education. Providing knowledge is only an issue when participants are encouraged to abuse it, which remains a situation that we are now starting to encounter on a frequent basis. The term ‘cyber-warfare’ frequently enters the media’s lexicon and groups such as ‘Anonymous’ and ‘Lulzec’ continue to force deviant behaviour into media headlines. Claiming responsibility for a number of high profile attacks on organizations such as Sony and Amazon, these groups glorify hacking and digital crime. This presumed acquisition of fame cannot be discounted as a driving force for individuals to escalate their involvement in digital criminal acts, desensitizing them from the potential penalties of their actions. The perception of cyber criminals has significantly changed since Gary Mckinnon’s exploits of US government computers, where they are now perceived through various media sources and social media platforms to be commendable and admirable individuals. It cannot be said that all individuals are compelled to replicate these exploits, but on some level, particularly in the younger generation, individuals are likely to be persuaded to partake and follow in their footsteps.

3 Fundamental limitations with digital data

The characteristics of digital evidence also provide a unique set of challenges to the DF practitioner; particularly its level of volatility, arguably acting in favor of the digital criminal. Although all forms of evidence, both digital and non-digital, are volatile; it is the ease of which digital evidence can be destroyed that presents a significant threat. To provide context, the lengths taken to destroy non-digital forms evidence must be considered. To destroy DNA evidence requires the use of chemicals such as bleach (Beauregard and Martineau, 2014). Even in cases of severe trauma, DNA evidence demonstrates its

resilience, for example where scientists are still able to identify victims from the September 11 attacks from DNA fragments found in the vicinity of the incident almost 15 years after the event (Robinson, 2014). In comparison, digital evidence is arguably not so robust.

The process of eliminating DNA itself is not straight forward, and requires the perpetrator to methodically process the site given DNA profiling can now be performed on small sample sizes, which cannot be seen easily by the naked eye. Further, the very act of destruction may lead to additional evidential touch DNA traces being left behind (Daly et al., 2012). As a result, it is unlikely that investigators will encounter a completely sanitized crime scene; free from DNA evidence which may prevent the identification of a suspect or offence. In comparison, the destruction of digital evidence is arguably simpler. In terms of destruction, reference is made to overwriting, where currently (at the time of writing) there are no known effective digital forensic techniques, which can be used for recovering overwritten digital data, even through the use of an electron microscope (Wright et al., 2008). Further, Wright et al. (2008) confirm that a single pass wipe is enough to securely remove data from digital storage media, meaning that there is no need to rely on schemes such as the Gutmann 35 pass wipe (Behr, 2008). This problem is aggravated by the range of applications and methods to overwrite content, many free of charge with support for multiple platforms and devices, downloadable after a simple search engine query device (see for example CCleaner: https://www.piriform.com/ with over 1 billion downloads reported). These applications are often easy to install and easier to operate, with many effectively placing digital data beyond the capability of the DF practitioner in a fraction of a second and pre-configured to remove those artifacts which are central to many DF investigations. There are limited ways to tackle this. It is unlikely that the foreseeable future will bring techniques for recovering overwritten data. Prohibiting the use of these tools is not feasible. As a result we are seeing the backlash of such positions where government powers are enforcing surveillance legislation (for example, the Draft Investigatory Powers Bill in the United Kingdom) in an attempt to increase the potential data set available to law enforcement and associated agencies for recognisance purposes and prosecution.

It is pertinent at this point to highlight Locard's (Kirk, 1953) exchange principle, which when distilled suggest that in theory, every criminal act leaves an evidential trace behind, where through the use of appropriate forensic analysis techniques, it is possible to establish a chain of events. Locard's principle helps to confine theories of the potential to commit a 'perfect crime' (a scenario where-by the detection of the perpetrator of an act is not possible) to works of fiction. Yet there are increasing signs that the concept is being treated with more respect in the digital realm as we edge towards a time where digital crimes are becoming harder to detect and police. Although effective deletion does not remove traces of activity maintained from service providers online, it does leave behind a limited opportunity to detect a crime in the first instance. In some cases, effective deletion may allow a suspect to operate outside of the current law, where reference to the UK illegal imagery legislation. There is no current offence of viewing therefore, and as a result, where all traces of indecent imagery are effectively removed from a device, there is limited scope for prosecution.

It is also necessary to consider the impact of physical destruction of data. Despite overwriting data placing data beyond recovery, the physical destruction of devices can be just as effective. We now have a concept of a disposable device, where costs are so low that it is now feasible to consider that perpetrators will physically destroy a device once it no

longer has a use. For example, mobile handsets can now be acquired for around £10 (Sainsburys, n.d.). Despite data recovery specialists possessing the ability to potentially repair devices which have experienced acts of abuse, the effective use of a hammer and similar tools common to most households can often place data beyond their grasp. Fundamentally the issue of data destruction, both physical and via overwriting methods is one which the field of DF has known about since it was first established, and is an issue which will continue to be faced for the foreseeable future.

4 Actually detecting a crime has taken place

As digital crimes become more complex, the digital crime scene has evolved into a minefield of issues ranging from the detection of crime to the extraction and interpretation of evidential data.

4.1 Identifying that there is a crime scene

Before an analysis can take place, relevant authorities must be alerted to the commission of a digital crime, where action can then be taken. Yet the digital crime scene is a complex entity and does not always present obvious indications of foul play, with attention draw to the previous discussions above. To illustrate this, a comparison is drawn between a hypothetical traditional offence, for example a murder crime scene and that of a digital offence. Where tangible evidence manifests itself (for the benefit of this example, a body), both detection and reporting is relatively straightforward, where symptoms of the crime are easy to spot and harder to ignore (Bryant and Bryant, 2014). Further, witness reports or standard societal processes (victim misses work, family report them as lost etc.) often lead to relevant authorities being alerted and the crime scene being identified and processed. Within the digital realm, identification of an offence is not as simple and is arguable a cause of increased digital crime.

The first scenario to consider is that of the direct victim of a digital crime where the crime scene involves their digital devices which may have been subject to, for example, attack or intrusion. Here, law enforcement is reliant on the victim to identify that they have been subject to an offence and therefore report it. However, given the complexity of digital crime and potential for victims to lack the necessary knowledge, signs that they have been the victim of a digital crime may go undetected for some time (for example in cases of hacking or online fraud), by which time identification of an offender may no longer be possible. In addition, as evidence of a crime takes the form of intangible digital content, a lack of understanding may lead to failure to report a criminal act or to even understand that they have indeed become a victim of cybercrime. Where evidence of crime exists within a digital device, arguably it is easier to ignore, (demonstrated above with crime reporting figures from the House of Commons (2013b)), the result being the absence of a criminal investigation into the incident, leaving perpetrators free to continue, indirectly encouraging the behaviour.

The second scenario to consider is the perpetrator who commits a digital crime from the comfort of their own home. From the millions of people who own a digital device, identifying those who are using it to commit a digital crime is not simple task. Here, there are no witnesses to alert police of the crime and proactive policing strategies are required. Reliance is placed on an individual to fall victim of an online sting or equivalent operation, or that their act is traceable. Yet when we consider the sheer volume of Internet traffic which must be monitored in order to identify the offence and the potential for a smart digital criminal, we now have an environment facilitating criminal acts where detection is significantly harder

given available resources. Therefore digital crimes may go undetected for significant periods of time or potentially never be uncovered.

Even where a crime scene is identified and accessed, competence plays a key role in the success of an investigation. Crime scene evidence can be destroyed by both a suspect and a first responder, should ineffective evidence collection methods be used. However, it is often reported that these individuals lack the knowledge, expertise and training to carry out the task (Bryant and Bryant, 2014). The problem is aggravated if they are required to triage devices at the scene. Albeit, even where the crime scene is one which contains prosecutable data, we risk failing to deal with it correctly.

4.2 The crime scene: size related issues

The next issue for consideration relates to the size of a digital crime scene and the implications this can have on a digital investigation. Continuing with our example, in traditional crimes, evidence of an incident can often be confined a dwelling or catchment area, where even the defendant themselves maintain evidential traces. Almost all of a perpetrator's acts will leave some form of tangible data, ranging from fingerprints to DNA, which are difficult to effectively sanitise. The digital crime scene cannot be so easily quantified in terms of size. On one hand, it can be seen as significantly smaller, where in many circumstances practitioners are dealing with evidence existing on devices such as computers or mobile handsets of that may be located on a suspect or in their vicinity. As Oluwasegun et al., (2014) suggest, digital devices play one of three roles in digital crime. They are either a target of crime, a device to commit a crime or finally a repository for evidence, essentially making the crime scene the digital device itself. Unlike traditional crimes involving DNA evidence where multiple traces may be left, it becomes a lot easier for perpetrators' to destroy digital evidential content, as it predominantly exists in the device. This evidence cannot be leaked onto or left behind on other surfaces or removed via touch alone, therefore, wherever the device goes, so does the evidential data. Devices can be easily picked up, hidden or physically removed and destroyed; leaving behind minimal sign of their existence, therefore sanitisation of the digital crime scene is arguably easier.

Conversely, the digital crime scene can also be significantly greater in size than traditional offences where illicit acts were facilitated via an Internet connection, bringing with it its own set of challenges. The Internet and computer-network technologies have now facilitated extensive digital crime scenes, blurring the boundaries of international jurisdictions, providing a seemingly borderless method of communication (Akdeniz, 2013). Here, the crime scene can potentially involve multiple jurisdictions, devices and device types, requiring the cooperation of all involved parties to ensure an effective examination is carried out. However, where the crime scene spans multiple nations, it becomes vulnerable to inconsistencies in examination and legal processes, potentially jeopardising an investigation. International collaboration also poses an issue despite attempts to facilitate this with the Council of Europe's Convention on Cyber Crime (Council of Europe, 2001). However, not all parties have adopted the measures of the convention and as a result, countries such as Russia have failed to acknowledge the convention and are posing issues in their failure to co-operate when tackling criminal activity such as the distribution of illegal imagery (Pyshkina et al., 2004), effectively harbouring those carrying out this criminal activity. Simply put, communication between relevant jurisdictions in digital crime investigations is often ineffective (Brown, 2015).

5 Concluding thoughts - So where does this leave us?

Digital crime is the result of a natural evolution of acts that have been occurring for years. Where perhaps once, offences such as theft were an invasion of one's personal space to remove physical chattels, it can now be a faceless crime, carried out from almost anywhere, where intangible digital assets are often a target. The challenge for DF is to support the regulation of crime that now present traits that lack the tangibility of more traditional offences. Further, new digital crimes emerge daily requiring the constant development of specialized examination approaches (Bryant and Bryant, 2014). As the pressures mount upon DF to support criminal investigations into digital crimes, it is necessary to question whether it can continue to do so effectively.

Unlike the human body, all of which are fundamentally similar and subject only to the limited changes brought about by evolution, many digital devices and cyber-offences are dissimilar, subject to rapid rates of change. Where universally accepted procedures can be applied, for example, to the analysis of blood, the diversity of digital devices and services mean that there is no standard approach which can be applied to every device, or in some cases an effective examination technique may not exist. As devices change or digital artifacts are manipulated as a result of new software releases, procedures for recovering or parsing data quickly become redundant, maintaining a lifespan parallel to the life span of the technology it is designed to examine, which is often short. This requires significant investment in terms of research and development in order to cultivate new investigative procedures, which in practical terms is largely unsustainable. Commercial forensic organizations release updates to their software packages at specific intervals throughout the year, yet new technological releases occur on a daily basis.

DF and associated organizations constantly operate in a reactive state where it is impossible to match pace with the rate at which new devices enter the market for consumers to potentially abuse. This leaves the real possibility that practitioners are likely to incur an increasing number of cases which they are ill-equipped to tackle. This issue alone raises serious concerns for the continued effectiveness of DF. This problem provides stark contrast to current techniques for traditional forms of evidence, such as the analysis of blood, which have remained similar for around 150 years due to the stability of blood structures (Bevel and Gardiner, 2008). This consistency of application has allowed techniques to be honed, increasing the reliability of evidence and allowing evidence recovery in most cases. Inconsistencies in digital evidence structures and type have not afforded this luxury and often analysis techniques have a limited lifespan of applicability before the technology or service they were designed to interrogate is further developed or superseded by newer technology. What this leads to is essentially placing DF's ability to effectively examine crimes out of their hands and in many cases, into those of the software developer. An apparent solution lies with a call for developers to adopt standardization of development protocols so that DF examination techniques have a longer lifespan and can be developed easier. However competition between organizations is likely to prohibit the practical implementation of this strategy.

It is at this point, that the combined impact of education, crime scene difficulties and data volatility on DF effectiveness is demonstrated. Rao et al., (2015) suggest that privacy in computing is now an increasing concern. In recent years, the emergence of privacy

enhancing applications (both locally and online) has and will likely continue to pose issues to DF analysis, ranging from private browsing facilities to applications like Snapchat (2015) and device sanitization provision. Individuals now possess a greater awareness of the benefits of these applications. The implications of their use will likely mean that the digital crimes scene may now frequently maintain less evidential data for extraction by a practitioner due to the ease in which it can be removed. The inevitable impact of this is the inability to successfully prosecute those who break the law in a number of cases due to a lack of evidence. Government responses in the United Kingdom have taken the form of proposals to ban technology which prevents law enforcement from effectively analyzing digital content, such as encryption on messaging clients like WhatsApp. Yet it remains debatable as to what this will achieve. The competing interests between the organization and their need to maintain the trust of their customers in order to survive, and that of law enforcement conflict. This is apparent with Apple Inc CEO Tim Cook's latest public message in February 2016 indicating Apple would not adhere to FBI requests to embed a back-door into apple devices to allow access to encrypted content (Apple, 2016).

Further, is it realistic to think that encryption can be prohibited or that it would even matter, after all, knowledge of techniques such as encryption methods is publically available and therefore subject to redesign? Targeting major encrypted platforms will only likely seek only to drive those who abuse these services to lesser known methods, making detection even harder. With this in mind, practitioners are arguably stuck between a hypothetical rock and a hard place, where driving crime to lesser-known platforms due to the invasive regulation of known applications could be seen as disastrous. In such circumstances, law enforcement loose complete control over criminal behavior and are left wondering where criminals are operating and through what means. Conversely, it could be suggested that this is no worse than current scenarios where reports suggest illicit acts are regulatory committed on known applications, yet protected by encryption.

Digital crimes are now some of the easiest illicit acts to commit. Further, it is similarly arguably that we do not know the volume of digital crime currently taking place, with organizations such as the Office of National Statistics (2014) highlighting the difficulties faced with quantifying this type of crime. As long as technology continues to play a major role in society, there will be a need for DF analysis. It is difficult to consider a time where it becomes wholly ineffective, yet it is not beyond possibility. Minor changes in user behavior (in some instances, having already been witnessed) could lead to significant restrictions for investigatory processes jeopardizing the detection of prosecution of criminal behavior, and at present there appears to be no obvious viable solutions. If individuals want to destroy or prevent traces of their digital acts, we are powerless to prevent these actions. Most individuals now possess both the tools and can easily acquire the knowledge to do so, with the volume of informed digital criminals likely to rise. Although there will always be those who are caught for engaging in acts which are detectable using currently techniques, those who seek to evade capture, possibly those engaged in more severe digital crime can and do frustrate current investigations.

Ultimately we are subject to the inventiveness of the criminal mind and how far individuals are willing to go in their attempts to commit an undetectable digital offence, where the influences of disclosures from individuals like Edward Snowden and Julian Assange cannot be underestimated. Detection of criminal behavior will become more difficult as it diversifies

in its methods, away from traditional methods. To provide an example, rumors spread post Paris attacks suggesting communication had taken place across gaming platforms (Farmer, 2015; Tassi, 2015). Although never definitively established it raises some concerning points. Communication protocols exist in abundance and it is unlikely that all can be effectively regulated. Therefore, we will likely miss or failed to detect content which may prevent an illicit act from taking place. Further, it raises issues over non-traditional forms of digital communications. Methods such as 'dead-drops' have been publicized (saving messages as drafts then sharing user login details to access the content to prevent interception whilst sending (BBC News, 2013b)), but what about using inbuilt games graphics to send messages? It seems a far-fetched idea, but when you consider the penalties associated with many criminal acts if caught, it is not beyond the realms of possibility that such techniques could be implemented. In such cases, these acts are almost beyond regulation.

To provide a tentative prediction, ten years from now it is perceivable that we will detect and prosecute far less individuals involved in crimes containing digital evidence. Although it may seem like an obvious statement, it is often one which is unacknowledged. Those operating at the less severe end of the spectrum may always provide lowest-hanging fruit for law enforcement, but high-end crimes will provide regulatory challenges, as they currently do. Yet as even basic acts of digital crime migrate to technologies capable of protecting a criminal's identity or the act itself, questions of the redundancy of DF are raised. It is difficult to see this can be evaded without major regulatory overhauls which are simply unlikely. Technology is largely uncontrollable, as are the users of it.

References

Akdeniz, Y Internet Child Pornography and the Law: National and International Responses (1st, Ashgate Publishing, 2013) 326 2.

Alazab, M., 2015. Profiling and classifying the behavior of malicious codes. Journal of Systems and Software, 100, pp.91-102.

Apple (2016) 'A message to our customers' Available at: http://www.apple.com/customer-letter/ [Accessed February 18th 2016]

Balogun, Adedayo M., and Shao Ying Zhu. "Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology." arXiv preprint arXiv:1312.3183 (2013)

BBC New (2011) 'Michael Jackson: I didn't Available at: http://www.bbc.co.uk/news/world-us-canada-15193077 [Accessed September 20th 2015]

BBC News (2013) 'Lostprophets' Ian Watkins: 'Tech savvy' web haul' http://www.bbc.co.uk/news/uk-wales-25435751 [Accessed September 20th 2015]

BBC News (2013b) 'How do terrorists communicate?' Available at: http://www.bbc.co.uk/news/world-24784756 [Accessed February 8th 2016]

BBC News (2014a) 'Oscar Pistorius girlfriend Reeva Steenkamp: You scare me' Available at: http://www.bbc.co.uk/news/world-africa-26711618 [Accessed September 20th 2015]

BBC News (2014b) ‘Police ‘overwhelmed’ by number of child abuse images’ Available at: http://www.bbc.co.uk/news/uk-29470001 [Accessed September 20th 2015]

BBC News (2104c) Police 'overwhelmed' by number of child abuse images Available at: http://www.bbc.co.uk/news/uk-29470001 [Accessed September 20th 2015]

BBC News (2015a) ‘Banning Tor unwise and infeasible, MPs told’ Available at: http://www.bbc.co.uk/news/technology-31816410 [Accessed September 28th 2015]

BBC News (2015b) ‘MI5 boss warns of technology terror risk’ Available at: http://www.bbc.co.uk/news/uk-34276525 [Accessed September 28th 2015]

BBC News (2015c) ‘Paris attacks: Silicon Valley in crosshairs over encryption’ Available at: http://www.bbc.co.uk/news/technology-34855462 [Accessed January 26th 2016]

BBC News (2016a) ‘Tor: 'Mystery' spike in hidden addresses’ Available at: http://www.bbc.co.uk/news/technology-35614335 (Accessed 1st June 2017)

BBC News (2016b) ‘FBI resists call to reveal Tor hacking secrets’ http://www.bbc.co.uk/news/technology-35924859 (Accessed 1st June 2017)

Beauregard, Eric, and Melissa Martineau. "No body, no crime? The role of forensic awareness in avoiding police detection in cases of sexual homicide." Journal of Criminal Justice 42, no. 2 (2014): 213-220.

Behr, Darrin J. "Anti-Forensics: What It Is? What It Does and Why You Need to Know?." New Jersey Lawyer Magazine 255 (2008): 4-5.

Bjelland, Petter Christian, Katrin Franke, and André Årnes. "Practical use of Approximate Hash Based Matching in digital investigations." Digital Investigation 11 (2014): S18-S26.

Bratus, S., 2007. Hacker curriculum: How hackers learn networking. IEEE Distributed Systems Online, 8(10), pp.2-2.

Brown, Cameron SD. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice." International Journal of Cyber Criminology 9, no. 1 (2015): 55.

Bryant, S and Bryant, R. (2014) ‘Policing Digital Crime’ Ashgate Publishing

Code Club (2014) ‘About Code Club’ [online] Available at: https://www.codeclub.org.uk/about [Accessed
September 20th 2015]

Cronan, T.P., Foltz, C.B. and Jones, T.W., 2006. Piracy, computer crime, and IS misuse at the university. Communications of the ACM, 49(6), pp.84-90.

Council of Europe (2001) ‘Convention on Cybercrime’ Available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185 [Accessed September 20th 2015]

Daly, Dyan J., Charlotte Murphy, and Sean D. McDermott. "The transfer of touch DNA from hands to glass, fabric and wood." Forensic Science International: Genetics 6, no. 1 (2012): 41-46.

De Santis, Alfredo, Aniello Castiglione, Giuseppe Cattaneo, Giancarlo De Maio, and Mario Ianulardo. Automated construction of a false digital alibi. Springer Berlin Heidelberg, 2011.

Farmer, Ben (2015) ‘Paris attacks: Terrorists could have used PlayStation4 to plot’ Available at: http://www.telegraph.co.uk/news/worldnews/europe/france/11997976/Paris-attacks-Terrorists-could- have-used-PlayStation4-to-plot.html [Accessed 2 February 2016]

Ferguson, Christopher J. "The CSI Effect." In Adolescents, Crime, and the Media, pp. 69-80. Springer New York, 2013.

Garfinkel, Simson L. "Digital forensics research: The next 10 years." Digital Investigation 7 (2010): S64-S73.

Graham, Ian (2011), Forensic Technology, Evans Brothers, 2010

HC Deb, 12th June 2013a, vol 564, col 397

HC Deb, 4th July 2013b, vol 565, col 1142

Hirsh, Michael (2015) ‘It’s All Back in Snowden’s Lap’ Available: http://www.politico.com/magazine/story/2015/11/paris-attack-isis-snowden-michael-morell-interview- cia-213373?cmpid=sf#ixzz3rnU95dKu Accessed (26th January 2016)

Houses of Parliament (2015) The Darknet and online anonymity, Postnote 488

Kanazawa, Satoshi (2008) ‘Why Criminals Are Less Intelligent than Non-Criminals’ Available at: https://www.psychologytoday.com/blog/the-scientific-fundamentalist/201006/why-criminals-are-less- intelligent-non-criminals [Accessed 9 February 2016]

Kirk, P. L. (1953). Crime investigation. New York: Interscience Publishers

Lang, Anthony, Masooda Bashir, Roy Campbell, and Lizanne DeStefano. "Developing a new digital
forensics curriculum." Digital Investigation 11 (2014): S76-S84.

McDonald, Aubri Fair. A CSI Effect Investigation: Media, Curiosity, and the Pursuit of Closure. ProQuest,
2008.

McGoogan, Cara (2016) ‘Dark web browser Tor is overwhelmingly used for crime, says study’ Available at: http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/ (Accessed 1st June 2017).

McGuire, M. And Dowling, S. (2013) ‘Cyber crime: A review of the evidence’ Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75 - summary.pdf [Accessed 19 September 2015]

Moore, D. and Rid, T., 2016. Cryptopolitik and the Darknet. Survival, 58(1), pp.7-38.

National Crime Agency (2016) ‘NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016’ Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file (Accessed 1st June 2017).

Office of National Statistics (2014) ‘Discussion paper on the coverage of crime statistics’

Oluwasegun, Sogbaike, Okene Ese David, Esemuede Esther, and Oweh Victor. "Computer forensics for law enforcement." Journal of Emerging Trends in Engineering and Applied Sciences 5, no. 1 (2014): 35-38.

Overill, R. E., and Jantje, A. M. S. (2010) ‘Digital Meta-Forensics: Quantifying the Investigation.’ Proc. 4th International Conference on Cybercrime Forensics Education & Training (CFET 2010), Canterbury, UK.

Overill, Richard E. "The'inverse CSI effect': further evidence from e–crime data." International Journal of Electronic Security and Digital Forensics 5.2 (2013): 81-89.

Phelps, Amy, and Allan Watt. "I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia." Digital Investigation 11.4 (2014): 261-272.

Pyshkina, Tatiana, Iosif Gurvich, Maia Rusakova, and Anna Yakovleva. "The Commercial Sexual Exploitation of Children in St. Petersburg and North-West Russia: The Russian Legislation and Activity of Law Enforcement Authorities." Crisis Centres and Violence Against Women. Dialogue in the Barents Region. Femina Borealis 9 (2004): 109-126.

Radziwill, N., Romano, J., Shorter, D. and Benton, M., 2015. The Ethics of Hacking: Should It Be Taught?. arXiv preprint arXiv:1512.02707.

Rao, Ashwini, Florian Schaub, and Norman Sadeh. "What do they know about me? Contents and concerns of online behavioral profiles." arXiv preprint arXiv:1506.01675 (2015).

Reilly, Denis, Chris Wren, and Tom Berry. "Cloud computing: Pros and cons for computer forensic investigations." International Journal Multimedia and Image Processing (IJMIP) 1, no. 1 (2011): 26-34.

Robinson, Belinda (2014) ‘Families of more than 1,000 victims from 9/11 may finally get closure as scientists hope DNA tests will unravel remaining unidentified bone fragments’

Available at: http://www.dailymail.co.uk/news/worldnews/article-2624062/Scientists-hope-DNA-tests-bone- fragments-finally-reveal-identities-1-000-victims-9-11.html#ixzz3mSkZ9ZYJ [Accessed September 10th 2015]

Sainsburys (n.d.) 'Samsung E1200' Available at: http://www.phoneshopbysainsburys.co.uk/pay-as-you-go-phones/samsung-phones/samsung-e1200-black.html?source=googleps&cmp=MBSPS&gclid=CjwKEAjw-lOwBRD1wrTC27fSjFISJABUDZ176rNZf0Zm7OzhUyKVlLLUdxjrB29RgoEvt6XjJsZ9UBoC9Lfw_wcB [Accessed September 20th 2015]

Scottish Police Authority (2015) Investment in new cybercrime hub for East of Scotland Available at: http://www.spa.police.uk/news/296903/ [Accessed September 20th 2015]

Shaw, A and Browne. A. (2013) 'A practical and robust approach to coping with large volumes of data submitted for digital forensic examination.' Digital Investigation 10: 2 pp. 116-128.

Snapchat (2014) 'Home' Available at: https://www.snapchat.com/ [Accessed September 20th 2015]

Sommer, P. (2004) 'The future for the policing of cybercrime', Computer Fraud & Security, (1), pp. 8–12.

Statista (2015) Number of worldwide internet users from 2000 to 2015 (in millions) Available at: http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ [Accessed September 20th 2015]

Tassi, Paul (2015) 'How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks [Updated]' Available at: http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis- terrorists-used-ps4-to-plan-attacks/#323daf6b731a [Accessed 2 February 2016]

Thompson, G (2015) 'Key Issues for the 2015 Parliament' House of Commons Library 53.

TorMetrics (2016a) 'Direct users by country' Available: https://metrics.torproject.org/userstats-relay-country.html?start=2011-01-01&end=2012-01-01&country=all&events=off [Accessed January 20th 2016]

TorMetrics (2016b) 'Direct users by country' Available: https://metrics.torproject.org/userstats-relay-country.html?start=2015-01-01&end=2016-01-01&country=all&events=off [Accessed January 20th 2016]

TorMetrics (2016c) 'Direct users by country' Available: https://metrics.torproject.org/userstats-relay-country.html?start=2013-01-01&end=2014-01-01&country=all&events=off [Accessed January 20th 2016]

Turner, P. (2007) 'Applying a forensic approach to incident response, network investigation and system administration using digital evidence bags.' digital investigation 4:1 pg. 30-35.

UNODC (2013) ‘Comprehensive Study on Cybercrime’ Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Accessed 19 September 2015]

United Nations Human Rights Council (2011) ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue’ A/HRC/17/27

Webbink, D., Koning, P., Vujić, S. and Martin, N.G., 2008. Why are criminals less educated than non-
criminals? Evidence from a cohort of young Australian twins.

Wright, Craig, and Dave Kleiman. "Overwriting hard drive data: The great wiping controversy." Information Systems Security. Springer Berlin Heidelberg, 2008. 243-25

Xu, Z., Hu, Q. and Zhang, C., 2013. Why computer talents become computer hackers. Communications of the ACM, 56(4), pp.64-74.

Young, R., Zhang, L. and Prybutok, V.R., 2007. Hacking into the minds of hackers. Information Systems Management, 24(4), pp.281-287.