Investigating the Increase in Mobile Phone Evidence in Criminal Activities

Jack Euan Ross McMillan
University of Glasgow
Jack.euan.mcmillan@gmail.com

William Bradley Glisson
University of Glasgow
Brad.Glisson@glasgow.ac.uk

Michael Bromby
Glasgow Caledonian University
M.Bromby@gcu.ac.uk

Abstract

The magnification of mobile devices in everyday life prompts the idea that these devices will increasingly have evidential value in criminal cases. While this may have been assumed in digital forensics communities, there has been no empirical evidence to support this idea.

This research investigates the extent to which mobile phones are being used in criminal proceedings in the United Kingdom thorough the examination of appeal judgments retrieved from the Westlaw, Lexis Nexis and British and Irish Legal Information Institute (BAILII) legal databases. The research identified 537 relevant appeal cases from a dataset of 12,763 criminal cases referring to mobile phones for a period ranging from 1st of January, 2006 to 31st of July, 2011. The empirical analysis indicates that mobile phone evidence is rising over time with some correlations to particular crimes.

1. Introduction

The increasing amalgamation of mobile phones into all aspects of society makes such hand-held devices a primary mode of communication. In 2011, it was reported by the International Telecommunication Union (ITU) that there are 5.9 billion mobile-cellular subscribers of which they estimate is 87% of the global population [1]. Even though a Gartner press release states that sales of mobile phones declined by two percent, when comparing first quarter sales of 2011 and 2012, 419 million units were sold worldwide in the first quarter of 2012 [2]. MobiThink estimates that developed countries have reached a saturation point of a single subscription per person and that the next major markets are China and India [3]. Gartner goes on to indicate that smartphones are responsible for driving market growth with sales reaching 144 million units [2]. According to cellular-news, just over 50 % of the British population owns a smartphone [4]. It is interesting to note that the ITU estimates that the number of mobile broadband subscriptions increased annually by approximately 45% [1].

Mobile phones have evolved rapidly into devices that are relatively small, compact and, potentially, contain a vast amount of personal information, such as call history, text messages, contact details, images and videos. To complicate matters, smartphones offer a wider range of capabilities that include applications, Global Positioning Service (GPS) and email. They also provide access to the Internet allowing for information flows such as news feeds and social networking information exchange along with streaming video and cloud storage services. Coupling feature-rich mobile devices with ever increasing technical capabilities, such as storage size and processing power, encourages these devices to become an integral part of daily activities.

However, the same devices that provide benefits to society through increased communication and data activities can also be abused to initiate, sustain and even record criminal activities. The benefit to mobile phone forensics analysis is that there are potentially large amounts of information on these devices that can be retrieved and analysed.

Based on this information, it is hypothesized that the use of mobile phone evidence in court proceedings has been increasing and that it has played a critical role in securing convictions in the United Kingdom for the past five years. The hypothesis raises three principal questions:

- How much information can be obtained from appeal court judgments in reference to mobile devices? Is it possible to quantify this information?
- Is it possible to identify the types of data that were analyzed in these cases and what types of crimes involved mobile phones?
- Is it possible to determine to what extent this data was relevant in each case, and if it was crucial in maintaining a conviction following an appeal?

This research begins to explore the extent to which mobile phones, through a quantitative, non-

1530-1605/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2013.366

experimental, initial investigation into legal judgments, has become an integral part of a case. The research identified 537 relevant appeal cases from a dataset of 12,763 for a period ranging from the 1st of January, 2006 to the 31st of July, 2011. The original research contribution of this paper is the initial empirical report identifying the extent to which these devices are being admitted into evidence in court cases in the United Kingdom, along with an analysis of the types of crimes in which they are being used. The results provide the foundation for future research into both the technical and legal aspects of mobile phone investigations.

The structure of the paper is as follows. Section two discusses relevant work. Section three identifies the project details and methodology used to extract and classify data from the legal databases. Section four draws out the results and section five presents an analysis along with a discussion of the information impact. Section six presents conclusions and future work that will be conducted in this area.

2. Relevant work

Within academic research, there appears to be a growing interest in the mobile phone area. Specifically, research has examined the social impact mobile phone technology has made on mainstream culture [5]. This impact arguably has led many researchers to position their research at the psychological and behavioral consequences of such widespread use [6]. For example, Zhiling, et al, [7] examined user behavior when a mobile phone is lost. This study looks at ways in which users cope when they lose their mobile device, personal data, and access to social networks. This research does not mention the legal implications of the loss, nor does it examine the legal position where the device could be used to prosecute for theft or fraud.

Similar research has been conducted by Song, et al, [8] which examines the impact of mobile phone and social capital. This study examines correlations between different social networks and ways that users preserve these social networks through their mobile phones. This research was not designed to examine the potential of criminal networks to be part of an individual's social network. In other words, how illegal activities and communication between individuals, through a mobile phone device, could assist the legal system as part of a criminal investigation.

This impact of mobile phone technology seems to have particularly affected teenagers and young adults, who are increasingly considering a mobile phone as part of their self-identity [9]. For example, a recent study by Shambare and Mvula [10], examined South African students' use of social networking websites through their mobile phone. This study reveals that they spend at least three hours every day on their Facebook accounts using mobile phones. It also indicates that more females are "facebooking" then males.

Mobile phone forensics has advanced considerably over the last few years. The National Institute of Standards and Technology (NIST) defines it as "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods" [11] . As Casey et al note [12], the overall objective is to find and extract data that is pertinent to an investigation. They also note that investigators should incorporate as much case information as possible in their search strategy. This should include information such as time lines, locations, the criminal act and items of interest to aid in the search. The ability to document the extraction of data is critical in any digital investigation [13]. This is due to the fact that it impacts upon the integrity of the investigation and the overall admissibility of the evidence in a court case [14].

Evidence admissibility is critical in criminal proceedings. Admissibility of evidence within UK courts may be subject to legislation, case law and the legal conventions of the three different jurisdictions that forms the United Kingdom [14]. The legal position regarding admissibility is different in each of the distinct legal jurisdictions of England and Wales, Northern Ireland and Scotland. Within England and Wales and Northern Ireland, the Civil Evidence Act, 1968 and the Police and Criminal Evidence Act, 1984 collectively set out the legal requirements for digital evidence to be admissible within criminal law.

In Scotland, the admissibility of electronic evidence is governed by the Civil Evidence (Scotland) Act, 1988. The interpretation of the legislation permits digital copies to be considered a true copy [15]. The case *McIlveney v Donald* [16] highlights the importance of this issue when evidence was deemed inadmissible due to a lack of authentication by the person making the copies [15]. The chain of custody helps to decrease the possibility that data integrity is compromised during the examination process through maintenance and documentation [17].

The increase in smartphone usage coupled with the expansion of capabilities makes the extraction of data a more complicated issue from an admissibility perspective [18]. What is actually extractable from a device will depend largely on its individual capabilities and the extraction process that is implemented. The main purpose of the admissibility rules is to ensure that data stored on the device is left unchanged [19]. However, this is problematic as simple activities such as switching mobile phones off and back on again has

shown to make changes to dates stored on the device [19]. The current methods used for mobile device memory extraction focus on extracting information from the phone by using either a physical cable, infrared or Bluetooth [20].

Grispos, et al, [21] argues that there is no universal file structure for mobile devices which, frustratingly, means that the method of storing data on such devices differs between manufacturers. This means that files will most likely be stored in different formats and in different locations according to the different manufacturers [20]. Due to variances across mobile phone devices, forensic acquisitions are normally conducted in one of two ways; physical or logical [21].

A physical acquisition of a mobile phone device exacts all of the memory contents from the phone through a communication port [12]. A logical acquisition interacts with the operating system on the mobile device to extract accessible data thought the use of protocols like Attention (AT) commands and Object Exchange (OBEX) [12]. To assist in the extraction of mobile device evidence, several forensic software packages are available to investigators. Some of these software solutions include: Paraben Cell-Seizure [22], Oxygen Phone Manager [23], XRY Complete [24] and Cellebright [25].

In order to gain this information, some phones have to be rooted or jail-broken. Rooting a mobile phone acquires administrative access to the phones file system. The closest method to a physical acquisition for an iPhone has been developed by Jonathan Zdziarski [26]. This technique allows the digital investigator to obtain a bit-by-bit raw disk image of the user's partition on the iPhone flash memory. This process involves accessing and modifying the system partition on the device to image that area of the device. Both rooting and jail-breaking involve modifying evidence which directly disagrees with the general recommendations by the Association of Chief of Police Officers (ACPO) for handling digital evidence [27] and the NIST [11] guidelines for handling mobile phones.

Moreover, other information that can be significant in securing a conviction is cell-site information which can be extracted and analyzed as part of evidence within a case. Cell-site data can contain information about a device's communication, movements and online activities [28]. Cell-site analysis is the ability to locate the geographical origin of where the mobile phone was located at the time calls were placed or SMS messages were sent. This can be traced either via real time or historical analysis. Tracing can be conducted through the combination of data from various cells, networks and examining signal strengths to narrow down mobile phone usage locations [29]. The ability to determine a suspect's location through a mobile device during a period of interest is arguably a powerful investigative capacity [30] and such data has proved critical in many criminal cases as it can be presented to show an individual's general location, movements and possibly actions [31].

In this paper, the authors suggest that there is a lack of substantial, empirical research into how law enforcement is trying to tackle the growing issue of mobile phones within crime. One hypothesis put forward by McEwan [32], argues that, globally, law enforcement agencies are increasingly focusing their limited resources on mobile phones as they appear to have become a master tool in the hands of those involved in organized crime.

The Organized Crime and Corruption Reporting Project (OCCRP) [33] reports that law enforcement agencies around the world are trying to prevent criminals from utilizing mobile phone technology. This threat is countermanded through policies such as eliminating the option for owners of pre-paid phones to remain anonymous and by blocking mobile phone signals in prisons. OCCRP also highlighted that mobile phone users in countries such as Mexico, Greece and South Africa, are now required to show a form of identification which is recorded in a national register, similar to gun purchases common in many jurisdictions. These identity checks are deemed necessary by authorities to try and limit the increasing practice among suspects who buy mobile phones anonymously, use them for a short period of time, and then dispose of them [34]. However, it has been argued that such protocols may violate the privacy rights of the citizens [34], an issue which extends beyond the scope of this paper.

Other research into mobile phone use and crime has been conducted regarding the recording of police e-crime data within Australia [35]. This quantitative research is an analysis of an e-crime police database of the South Australian Police force that tracked requests for analysis of electronic information of devices and other related information. The figures presented in this research show the number of mobile phone exhibits analyzed by type of investigation and type of device. This research [35] highlights and discusses several crimes independently, namely drugs, fraud and pornography. Within drug use, for example, in 2004-2005 and onwards to 2008; there were significant increases in mobile phones being analyzed as part of drug use. This ranged from 2.6% in 2004/05, to 11% in 2005/06 to 64% in 2007/08. Moreover, in the years of 2006/07 and 2007/08, 64% of all drug-based analysis came from mobile phones. The paper also reports that, approximately, 15% of all requests were related to illegal pornographic images. The drawback to this type of research is that it is based on police statistics from

one part of Australia. It does not examine the evidence from the perspective of the fact-finder or arbiter of law, namely the judge and or the jury.

There is currently minimal substantive academic literature, which examines the link between criminal activity and technology use. Studies such as Vacca [36] have indicated that mobile devices have the potential to be involved in a large variety of crimes, ranging from white-collar, to terrorism and murder.

3. Methodology

This study used the three major UK legal databases: Westlaw [37], Lexis Nexis [38], and the British and Irish Legal Information Institute (BAILII) [39] to conduct research on mobile phone involvement in criminal court cases. These databases were selected because they each offer an online legal research reference point for lawyers and academics within the UK. Moreover, these databases typically contain most, if not all, of the judgments handed down from the appeal courts in full text format with case notes, headers and keywords commonly added.

The research was conducted in three stages. In the first stage, cases were identified and the facts, details and decisions were retrieved from the legal databases. Only cases that occurred in the last five year were selected from the legal databases. In the second stage, a research database was created and relevant case details were entered into this database for subsequent analysis. Finally, the details of the legal representatives who were conducting each case (counsel for the appellants and for the Crown) were captured as part of the research. These details were further sourced using external legal directories as required.

3.1. Research scope

This paper focuses on mobile phones that have been referred to as evidence within criminal courtrooms and recorded in appellate judgments. The legal databases each have limited coverage of criminal law, as cases of first instance are typically not reported unless they are particularly significant. Appellate judgments may be considered the tip of the iceberg with many more incidences of mobile phone evidence unreported either due to acceptance of the evidence or a lack of any possible grounds of appeal.

The decision to limit the search to three databases was a pragmatic decision based on available resources. Relevant cases were extracted from these database records. Hence, cases that were either not recorded in these databases during the search period or reported elsewhere are considered to be out-of-scope for this research.

A second constraint is the legal jurisdiction. This research only covers criminal appeal cases that have been heard in England and Wales, Scotland or Northern Ireland. It does not include cases that arise from the Republic of Ireland, British Overseas Territories, the Channel Islands or other Commonwealth or indeed common-law countries. A further constraint on this paper is that analysis of the mobile phone evidence is limited to the information given within the judgments written and handed down by the appeal court judges.

3.2. Research process

The acquisition of legal judgments in this research was obtained through the following process:

1. Each database was accessed through an Internet portal; a subscription is required to access two of these sites (BAILII is an open access resource).
2. Once access has been granted, the ‘cases’ section of the database was selected. This section contains information on reported cases and excludes legislation, journal articles and other sources of law.
3. Within the ‘case’ section of the database, the keyword field was used to populate queries. The keywords that were used in the search process are provided in Table 1 - Keywords. It should be noted that the database searches each time started with LexisNexis, then BAILII, and then Westlaw. A total of thirty-two searches were conducted in each legal database; two parent and thirty children. The parent key words used in the search were ‘mobile phone’ and ‘mobile telephone’. As noted in Table 1 Lexis returned the highest number of cases followed by BAILII and Westlaw. An additional thirty searches were conducted using additional key words to help clarify the results.
4. Once a query search had been conducted, cases that related to criminal law were selected; this was normally indicated by the use of the term (Criminal) in brackets.
5. All cases returned in the search query were opened up and read to identify the context of the keywords and to determine whether or not it was relevant to the purposes of the research. If it was deemed relevant, the information was copied into the Microsoft access database under appropriate headings. If the judgement was not relevant the information was not recorded. For example, discarded judgments included civil cases, extra-territorial judgements and cases where mobile phones were not instrumental to a case. In other

words, a mobile phone was stolen but not recovered, for example, or a mobile phone was used to dial 999 for help or other such purposes. Case judgements in this category were not recorded in the database.

6. If the judgement was relevant, each piece of mobile phone evidence was classified as High, Medium or Low. The classification is based on the significance of the evidence, and the language used within the judgement in relation to the conviction of the defendant. The classifications are explained as follows:
   - **High**: This designation indicates that the digital evidence presented within court proceedings was vital to the outcome of the case. In other words, the conviction was brought solely or principally on the evidence contained within the mobile phone e.g. cell-site analysis. In other words, the sole use of evidence was stated in the decision part of the transcript e.g. *the call records* were *'vital'* in the case and terms such as *'critical', 'vital' or 'crucial'* were used.
   - **Medium:** This designation indicates that the digital evidence strengthened or contributed towards the outcome of the case, either to disprove or prove the named defendant committed the crime. In this instance, the transcripts generally state that this evidence, along with other forms brought about an outcome in the case. In this instance, the evidence is part of a larger collection of evidence stated in the decision e.g. the prosecution *'relied'* on the images, and terms such as *'relied', 'reliance', 'supporting' or 'circumstantial'* were used.
   - **Low:** This designation indicates that the digital evidence was mentioned in the court transcript but there was a lack of analysis or discussion surrounding it. It appeared that such evidence presented had little or no significance to the outcome of the case. For instance, the only reference to the mobile phone evidence appears as a statement such as *'texts from the appellant's phone appeared to show he was in contact with a co-defendant'*. In this instance, there was a lack of reference to the mobile phone usage in the transcript and no active terms towards the reliance of the evidence
7. Legal representative information was located using external legal sources for completeness. This depended on the jurisdiction, the type of criminal case and the role of the representative in conducting the case.
8. Relevant case information was extracted out of the judgment and placed into an Access database in order to create the final dataset. If an existing case within the database was identified as a duplicate, the case was skipped to prevent duplicates within the research.
9. This database was backed-up and stored in a secure location on a daily basis.

Table 1. Keywords

Keywords (Parent)	DB	Cases
1. "mobile phone"	LexisNexis BAILII Westlaw	L=397 B=43 W=29
2. "mobile telephone"	LexisNexis BAILII Westlaw	L=43 B=25 W=0
Keywords (Child)		
"evidence"		
"examined" or "examination"		
"text messages"		
"analysis" or "analyse" or "analysed" or "analyst"		
"photographs"		
"camera"		
"seized"		
"expert"		
"criminal"		
"handset"		
"report"		
"video"		
"images"		
"forensic"		
"cell-site analysis"		

4. Results

From the databases that were used, 12,763 cases were identified in total as containing the mandatory keywords, of which 537 cases were identified as relevant and rated as High, Medium, or Low. The first significant finding is that the majority of these cases are from the jurisdiction of England and Wales, with only a few cases arising from other parts of the UK. These findings are illustrated in Figure 1 - Relevant Cases by Jurisdiction.

The data showed that 496 were from England and Wales (15 originating from Wales), 23 were from Scotland and 18 cases were located from Northern Ireland. Out of the cases from England, 129 cases were from London. Analysis of the data indicates that in 2006, 51 cases were prosecuted that contained and/or relied on mobile digital evidence.

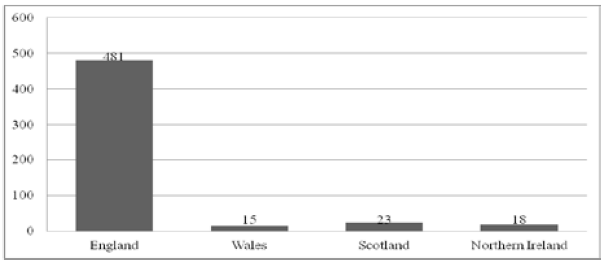

Figure 1. Relevant Cases by Jurisdiction

In 2007, the number of relevant cases dropped by one to 50. In 2008, this increased by eleven cases to 61 and steadily increased year-on-year to 111 in 2009 and 157 in 2010. The number of relevant cases at the end of July, 2011 had already hit 107. These findings are presented in Figure 2 – Incidence of Mobile Phone Evidence.

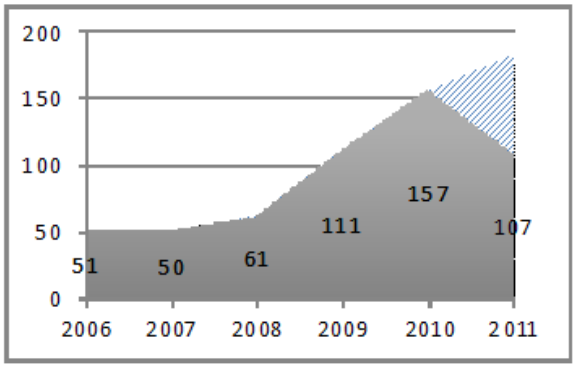

Figure 2. Incidence of Mobile Phone Evidence

The data collected provides insight into the type of mobile phone evidence being introduced into court cases. From the 537 cases that were extracted from the legal databases, 18 categories of relevant forensic evidence were identified.

The different evidence categories were, generally, coupled with another type of evidence, e.g., cell-sites were coupled with call records and presented together to the court for consideration within the proceedings of the case. An illustration of the different types of forensic evidence found within the case data is presented in the Figure 3 - Evidential Categories.

The data shows that the leading types of evidence retrieved from a forensic examination and discussed in court were call records. There were 217 cases that contained call records on the mobile devices. This was followed by 145 SMS cases, 67 cases involved images and 51 cases involved calls and cell-site analysis.

The age of the appellants was also captured. Out of 537 cases, 282 cases had their ages recorded. The age range was between 10-87 years old. The data reveals that the age range of 20 to 24 year olds contained the most with 55 cases. The second largest age group was 25-29 year olds with 52 cases.

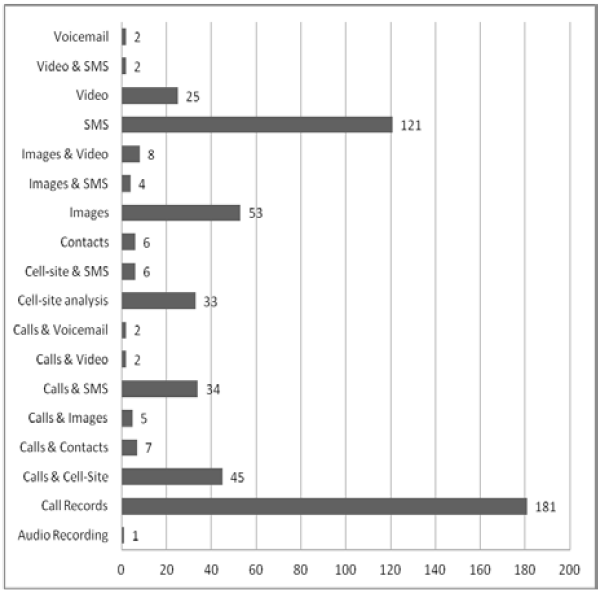

Figure 3. Evidential Categories

The information on appellant age ranges is illustrated in Figure 4 – Age Ranges. The age of the appellant relates to the time of the original trial and conviction. It is also worth noting that the appellant may or may not have been the owner of the mobile phone, and that these figures are reported for interest rather than statistical significance.

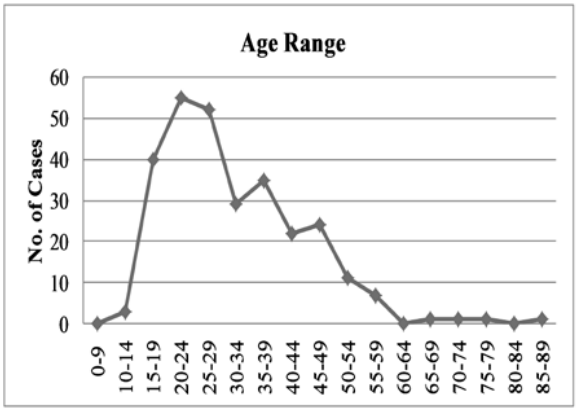

Figure 4. Age Ranges

5. Analysis

The analysis of the appeal judgments supports the hypothesis that mobile phone evidence, within criminal court cases, has indeed been increasing over the past five years. The trend in Figure 2 shows an early plateau and then an increase from 2008 onwards.

When the data for the 7 month period for 2011 (n=107) is extrapolated to give a 12 month period (n=183, on estimate) assuming an even distribution of cases over a year. If this trend were to continue, further cases would be expected for the period 2012. While mobile phone evidence is playing a role in the courts, most of the cases were weighted with a low significance, not a high significance, on the outcome of the court case.

5.1. Information Obtained

The first research question inquired as to how much information can be obtained from the judgments in reference to mobile devices and whether it is possible to quantify this information.

The lack of recording of technical data within the judgments was another significant finding. Very little information is actually recorded relating to the technical details or the actual technological device. On reading the judgments in full, it is typically reported that the mobile device was analyzed or seized and information was retrieved or evidence was found with no further analysis given.

The judgments are unsurprisingly lacking in technical detail and leave many unanswered questions regarding the technical framework of the mobile device and the techniques used for analysis. Additionally, hardly any information is given regarding the chain of custody, the type of hardware/software used to extract the data and the outcome of the analysis. For instance, within the dataset only seven cases refer to the product name of the device that was analyzed and these were identified as Blackberry, Nokia, Samsung and iPhone.

Furthermore, no further device details are given, such as the model of the phone or the features of the mobile device that were exploited in order to commit or assist in the criminal activity. There is an absence of detail regarding the evidential value of the device as there appears to be little or no discussion or analysis of the data by either the defense or prosecution in terms of challenging the authenticity of this data. Hence, it is observed that arguments relating to admissibility or evidential value are settled in the courts of first instance, and these issues are not raised on appeal.

It is interesting to note that the details relating to the digital forensics expert witness were equally lacking. Out of 537 cases, only 21 experts were named in the judgments and could be identified and located from the reports. Ten of these were identified as being police officers who had the expertise to analyze and present the evidence, typically evidence of fact rather than expert opinion. Eleven of these individuals were named as independent contractors working within the area of digital forensics and no information was provided on the remaining experts.

5.2. Evidential Value

The second question inquires about the ability to identify the types of data that were used in crimes along with the types of crimes that involved mobile phones. As noted in Figure 3 - Evidence categories, the most referenced artifacts were Call records, followed by SMS evidence, then calls and cell-site analysis.

Further detailed analysis of these findings indicates that there is a link between the type of evidence and the type of crimes for which the appellants are standing trial. For instance, an appellant could be standing trial for sexual offences and images are extracted from the appellants mobile phone claim to prove the individuals innocence, guilt or motive within a crime. Within the case results, there appears to be several links where digital evidence is used to establish the criminality of the appellant(s) being charged. This type of evidence could be text messaging, video and images and cell-site analysis, etc.

From the dataset, it appears that SMS evidence gathered from the case analysis is predominantly drug themed, where users contact dealers regarding the purchase of drugs. The data show that at least 40 cases out of the total number of 121 contained SMS evidence and had a drug element. Similarly, when analyzing judgments for video or image related evidence, at least 48 of the 86 image and video cases had a sexual undertone to them and were predominately used in sexual offence proceedings. 163 out of 181 cases indicate that call-record evidence is largely to confirm connections to link co-conspirators to their collective actions, or to establish intent to commit criminal acts.

The analysis of the case data shows that cell-site analysis evidence is largely used to trace movements and to confirm the location of the appellant's mobile phone at the time of the crime. For instance, cell-site analysis has been used to help disprove an appellant's witness statement or their alibi of events that happened during the time of the criminal act. From the analysis, at least 20 out of 33 cases contained cell-site analysis as illustrated below in Table 2 – Evidence Type.

Table 2. Evidence Type

Evidence type	Total cases	Evidence category	Correlating cases
SMS Evidence	121	Drug Use	40
Image & Video	86	Sexual Offences	48
Call records	181	Link Co-Conspirators	163
Cell-site analysis	33	Confirm location or disprove statements	20

5.3. Evidential Weight

The third question inquires about the potential to determine the extent mobile device evidence was relevant in obtaining a conviction. As discussed in the methodology, the weight of evidence was categorized as high, medium or low. The findings indicate that digital mobile evidence, in this dataset, was not relied upon to support a conviction. 345 of the 537 cases were assessed as having a low significance towards the outcome of the criminal case. 181 of the cases involved evidence that had a medium impact on outcome of the case. Only eleven of the cases had a high impact on the court ruling. The results of this assignment are illustrated in Figure 5 – Evidential Weight.

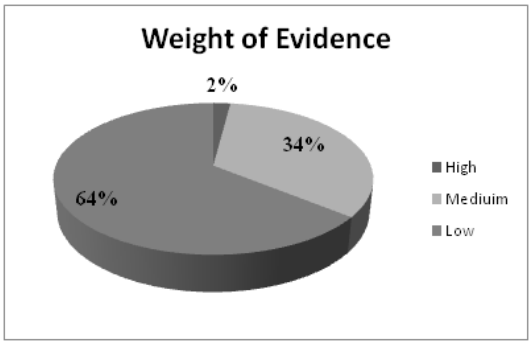

Figure 5. Evidential Weight

5.4. Legal Analysis

The most significant finding within the body of cases is the lack of detail in the judgments in relation to digital and forensic data. This lack of recording is clearly illustrated within many of the judgments and consists primarily of evidence that is accepted by both parties and remains unchallenged and subsequently not commented upon by the judges in the appeal courts. These findings may suggest a lack of specialist knowledge on the part of the legal teams when dealing with digital data as there appears to be little questioning or interrogating of mobile phone evidence on appeal. It may well be that these issues are dealt with at the initial trial, although the very existence of appeal court judgments suggests that the relatively new field of mobile forensics is still yet to become a mainstream part of investigations or form evidence in criminal trials.

From the results of the findings, it is observed that the vast majority of cases were originally conducted in the Crown Courts in England, Wales and in Northern Ireland. The Crown Courts heard 485 out of the 537 cases. In Scotland, 21 cases were heard at the High Court of Justiciary. These courts deal with indictable offences and are typically serious offences. This raises the question: is mobile phone evidence predominantly used in high-profile criminal court cases such as murder, sexual offences and drug possession rather than low-level or petty crimes? On the data presented in this study, the answer would appear to be affirmative.

Defence counsel details were extracted from the judgments and entered into the research database. This information was captured for completeness. The legal representatives were predominantly barristers rather than solicitors. An analysis of the appellant's ages revealed that out of 537, 282 contained the age recorded within the judgment. Criminological research indicates that the age group 14-25 is the peak age group for criminal activity [40]. An analysis of the data in this study appears to be in slight disagreement with general research findings elsewhere with a total of 106 cases in the 14-25 age range. The highest age range for criminal activity within the dataset was between 20-29 years with a total of 107 cases. The majority of the appellants were in the age group between 15 and 29 with a total of 147 cases.

The general background of criminology research goes on to indicate that after age 25 there is a decrease in criminal activity as people take-on new roles such as parenthood [41]. However, the results of the dataset appear to differ of this overall trend. It has also been reported that criminal activity is more likely to be conducted in urban areas [41]. It is interesting to note that the majority of the cases in this dataset were prosecuted in London, although this is the most heavily populated part of the UK. The results were not analysed for other urban areas as Crown Courts are by default located in urban areas and would hear local rural crimes.

The results illustrate that 337 cases out of the 537 appeals raised were refused or eventually dismissed by the appeal court judges. The remainder of these cases contained reductions of sentences for the appellants, other amendments to the punitive element, or a quashing or the original conviction. Finally, from the analysis of the case information, no correlation was evident between the appeals that were dismissed and the type of crime that was committed.

6. Conclusions and Future Work

The increased integration of mobile phones into society is beginning to show in the text of the appeal court judgments. An initial empirical investigation indicates that the filtration into court proceedings is a multifaceted subject in an increasingly complex atmosphere. The initial results indicate that mobile

phone evidence within criminal court cases has been increasing since 2008. However it should be noted that there is relatively minimal information on the specific of the mobile device that is available in the judgments used for this research.

From the results outlined in the case data, it can be argued that mobile phone devices are, potentially, a growing facilitator in criminal activity. The trends that were noticed in the data indicate a general correlation where drug-related crimes utilized SMS evidence. It also indicates a correlation between images and video and sexually related crimes. Call records were generally used to establish connections between individuals. Cell-site analysis was used to trace device movements and confirm locations at particular times of interest.

Future research needs to investigate the level of understanding and knowledge of mobile phone forensics terminology, techniques and procedures by members of the legal profession. A quantitative and qualitative investigation could accomplish this goal through the implementation of Web surveys and semi-structured interviews.

Future work will conduct further in-depth research into the forensic reports generated for individual cases to obtain a more detailed understanding of technical problems in mobile phone forensics. This data could also be used to establish common repeatable problems and potentially used to develop solution patterns.

The same research should be conducted in other countries to see if the same pattern of mobile phone integration exists and how they compare. Future work will examine mobile devices like Global Positioning Systems (GPS) devices and tablets. Specifically, mobile devices will be examined from court proceedings and forensic reports in conjunction with specific modes of transportation, i.e., air, water, rail, and motor.

7. References

[1] The Wold in 2011 ICT Facts and FIgures, http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf, accessed 19/05, 2012.

[2] Gartner Says Worldwide Sales of Mobile Phones Declined 2 Percent in First Quarter of 2012, http://www.gartner.com/it/page.jsp?id=2017015, accessed 19/05/, 2012.

[3] http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats, accessed 19/05, 2012.

[4] http://www.cellular-news.com, accessed 19/05, 2012.

[5] Shambare, R., Rugimbana, R., and Zhowa, T., "Are Mobile Phones the 21st Century Addiction?", African Journal of Business Management, 6(2), 2011, pp. 573-577.

[6] Aoki, K., and Downes, E.J., "An Analysis of Young People's Use of and Attitudes toward Cell Phones", Telemat. Inf., 20(4), 2003, pp. 349-364.

[7] Zhiling, T., and Yufei, Y., "Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft", System Science (HICSS), 2012 45th Hawaii International Conference on, 2012, pp. 1393-1402.

[8] Song, Y., Kurnia, S., and Smith, S.P., "The Impact of Mobile Phone Use on Individual Social Capital", System Sciences (HICSS), 2011 44th Hawaii International Conference on, 2011, pp. 1-10.

[9] Hooper, V., and Zhou, Y., "Addictive, Dependent, Compulsive? A Study of Mobile Phone Usage", 20 th Bled eConference eMergence: Merging and Emerging Technologies, Processes, and Institutions, 2007

[10] Shambare, R., and Mvula, A., "South African Students' Perceptions of Facebook: Some Implications for Instructors", African Journal of Business Management, 5(26), 2011, pp. 10567-10564.

[11] Jansen, W., Ayers, R., "Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology"2007

[12] Casey, E., and Turnbull, B., "Chapter 20 Digital Evidence on Mobile Devices", in (Casey, E., 'ed.' Digital Evidence and Computer Crime Third Edition edn., Academic Press, 2011

[13] Beebe, N.L., and Clark, J.G., "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process", Digital Investigation, 2(2), 2005, pp. 147-167.

[14] Rowlingson, R., "A Ten Step Process for Forensic Readiness", International Journal of Digital Evidence, 2((3)), 2004, pp. pp1-28.

[15] Motion, P., and Warren, S., "Electrical Storm on the Horizon?", Journal Online For members of the Law Society of Scotland, 2009,

[16] "Mcilveney V Donald ", 1995.

[17] National Institute of Standards and Technology, "Guide to Integrating Forensic Techniques into Incident Response"2006, pp. 121.

[18] Mccarthy, P., and Slay, J., "Mobile Phones: Admissibility of Current Forensic Procedures for Acquiring Data", Proceedings of the Second IFIP WG 11.9 International Conference on Digital Forensics,, 2006

[19] Breeuwsma M, D.J.M., Klaver Coert, Van Der Knijff Ronald, Roeloffsm., "Forensic Data Recovery from Flash Memory", Small Scale Digital Device Forensics Journal, 1(1), 2007,

[20] Willassen, S., "Forensic Analysis of Mobile Phone Internal Memory Advances in Digital Forensics", in (Pollitt, M., and Shenoi, S., 'eds.'), Springer Boston, 2005, pp. 191-204.

[21] Grispos, G., Storer, T., and Glisson, W.B., "A Comparison of Forensic Evidence Recovery Techniques for a Windows Mobile Smart Phone", Digital Investigation, 8(1), 2011, pp. 23-36.

[22] http://www.paraben.com/device-seizure.html accessed 22/09, 2011.

[23] http://www.oxygensoftware.ru/en/default.asp accessed 22/02, 2012.

[24] http://www.msab.com/xry/what-is-xry accessed 22/02, 2012.

[25] http://www.cellebrite.com/forensic-products/forensic-products/ufed-physical-pro.html, accessed May 12, 2011.

[26] Zdziarski, J., Iphone Forensics: Recovering Evidence, Personal Data, and Corporate Assets, O'Reilly, 2008.

[27] The Association of Chief Police Officers, "Good Practice Guide for Computer-Based Electronic Evidence"

[28] Furnell, S., Securing Information and Communications Systems: Principles, Technologies, and Applications, Artech House, 2008.

[29] http://www.mobilephoneforensics.com/cell-site-analysis.php, accessed 11/09, 2011.

[30] Casey, E., and Turnbull, B., "Digital Evidence on Mobile Devices", in (Casey, E., 'ed.' Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Elsevier Academic Press, 2004

[31] Tony Dearsley, "Mobile Phone Forensics – Asking the Right Questions", New Law Journal, 155(7187), 2005, pp. 1164-1168.

[32] Mcewen, R.N., "Tools of the Trade: Drugs, Law and Mobile Phones", Proceedings of the American Society for Information Science and Technology, 44(1), 2007, pp. 1-16.

[33] Organized Crime and Corruption Reporting Project, http://www.reportingproject.net/occrp/index.php/en/ccwatch/cc-watch-indepth/402-cell-phones-ideal-for-crime, accessed 20/05, 2012.

[34] Green, N., and Smith, S., "A Spy in Your Pocket? Monitoring and Regulation in Mobile Technologies", Surveillance and Society, 1(4), 2004, pp. 573-587.

[35] Turnbull, B., Taylor, R., and Blundell, B., "The Anatomy of Electronic Evidence - Quantitative Analysis of Police E-Crime Data", Availability, Reliability and Security, 2009. ARES '09. International Conference on, 2009, pp. 143-149.

[36] Vacca, J.R., Computer Forensics: Computer Crime Scene Investigation, Charles River Media, 2005.

[37] http://www.westlaw.co.uk/, accessed 05/06, 2012.

[38] http://www.lexisnexis.com/uk/legal/, accessed 05/06, 2012.

[39] http://www.bailii.org/databases.html, accessed 05/06, 2012.

[40] Tittle, C.R., Ward, D.A., and Grasmick, H.G., "Gender, Age, and Crime/Deviance: A Challenge to Self-Control Theory", Journal of Research in Crime and Delinquency, 40(4), 2003, pp. 426-453.

[41] Blonigen, D.M., "Explaining the Relationship between Age and Crime: Contributions from the Developmental Literature on Personality", Clinical Psychology Review, 30(1), 2010, pp. 89-100.