Internet Journal of Criminology © 2012
ISSN 2045-6743 (Online)

TO WHAT EXTENT HAS FACEBOOK BECOME A CONDUIT FOR CRIMINAL ACTIVITY?

By Victoria Loizou[1]

Abstract

The wide availability of the internet has brought massive changes in the ways by which communication can be achieved and in many instances have replaced traditional methods of correspondence. Increasingly popular is the use of social network sites which are one of the many ways by which computer mediated communication can be achieved. The massive growth of this sort of interaction has consequently attracted a large amount of media attention particularly following incidents of criminal activity that came to light. The aim of this dissertation is to explore the extent and nature of criminal activity of most popular social networking site, Facebook, and to determine whether the risks and warnings highlighted in the news and other media regarding the use of social network sites are justified. The main approach adopted for this purpose is a combination of both qualitative and quantitative collection.

Qualitative data was collected through 20 semi-structured interviews and in support of this; quantitative data was sought from individual police forces through Freedom Of Information requests which were sent to 32 police forces in England. The findings drawn from the interviews and data provided by 15 police forces which responded to the request, was compared and discussed in relation to existing literature and previous studies.

The findings of this project indicate an increase in reporting offences which are in some way related to the social network site Facebook. The several factors which contribute to this increase, as well as the limitations of the data supplied by the police forces, illustrate the need to explore the nature of criminal activity which linked to the social network site. By doing so, it was found that more that 100 categories of crime were recorded by the police, in which Facebook was mentioned during the report. These offences varied significantly in severity and prevalence.

This study has found that there is a definite need to enhance Facebook users' awareness in regards to the available security and privacy options the social network site provides. Many of the offences reported to the police, could potentially be the result of individuals making personal information available to online perpetrators who grasp the opportunity to commit an offence. Although tackling online criminal activity is a challenging task, many of these offences can be prevented, by enhancing the knowledge of individuals using the social network as to the risks to which they may be exposing themselves in their extended public self – presentation.

[1] Submitted in partial fulfilment of the requirements for the degree of ba (hons) criminology with psychology, Department of Social Science, University of Hull

Contents

Acknowledgments

It is a pleasure to thank those who have made this dissertation possible. Many thanks, to all participants in this study who took the time to share their personal experience with me. Also, I would like to thank all police forces who responded to my Freedom Of Information request and who provided me with valuable material. I am heartily thankful to my dissertation supervisors, Professor Keith Tester and Professor Majid Yar for their support and guidance throughout the duration of this project.

To what extent has Facebook become a conduit for criminal activity?

Chapter 1: Introduction

The extensive growth and availability of the internet has brought about massive changes to our familiar ways of living. What was previously unthinkable is now easily achieved with just one click of a mouse. This has changed the ways in which people communicate, work, educate and entertain themselves. However, along with the positive changes this technological innovation has brought, new opportunities and methods for criminal activity have emerged.

This study will focus on criminal activity which occurs on, or is mediated by the social network site Facebook. An attempt will be made to determine the extent and nature of criminal activity and provide an understanding as to the dangers users of Facebook are subjected to. This first chapter will outline the history of social network sites and Facebook in particular and explore the presentation of these sites in the media. This will assist us to draw a picture of the problem, before going on to explore the extent and nature of criminal activity related to Facebook in further detail in the following chapters.

Social Network Sites

Computer mediated communication (CMC) has become an increasingly popular method of communication particularly over the last decade, due to the rising accessibility to the internet and the rapid ways in which communication can be achieved. The exchange of electronic mail and instant messages using various software programs, hundreds of which are available on the World Wide Web, have in many cases replaced traditional methods of communication such as the exchange of letters. In addition, the ability to make cost free voice, video or even conference calls to people who may be thousands of miles away is another contributing factor to the large popularity of computer mediated communication. The only pre - requirement for this type of communication is that all parties have access to a networked computer.

The benefits of computer mediated communication have attracted the attention of many businesses worldwide, which adopted these methods as their primary means of communication. However CMC has also been implemented by millions of individuals who wish to communicate with friends, family and peers or desire to meet other people with whom they have common interests or beliefs (Boyd and Ellison, 2007). In addition to electronic mail, instant messaging and other CMC, Social Network Sites (SNSs) such as Facebook, Twitter, MySpace and Google Plus have become integrated into the daily lives of millions of internet users around the globe.

Social Network Sites are a form of virtual communities (Dwyer et. al., 2007), some of which are based on common features such as language, sexuality, religion or race, whilst others accommodate diverse audience (Boyd and Ellison, 2007). Social Network Sites allow their users to construct a profile, identify other users with whom they share offline connections with and navigate through their profiles (Dwyer et. al, 2007). Although it is possible for internet users to meet through the SNSs, this is not the primarily aim (Boyd and Ellison, 2007). A study on the motives and uses of Facebook, carried out by Joinson (2008) reveals that the most central use of Facebook tended to be for keeping in touch with peers.

The rise of Facebook:

The Social Network Site Facebook was first launched in February 2004 by Mark Zuckerberg and co-founders Dustin Moskovitz, Chris Hughes and Eduardo Saverin form their Harvard University dorm room (Facebook, 2011). Before expanding in September 2005 to accommodate high schools and corporate networks, Facebook was restricted to college based users (Joinson, 2008; Boyd and Ellison, 2007). A year later, in September 2006 Facebook expands once again allowing anybody to join the site (Phillips, 2007).

Less than a year after allowing everybody to sign up to the site, in April 2007 Facebook reached more than 20 million active users and by August 2008 the SNS accommodated more than 100 million active users. As of this writing, Facebook is the largest social network site with over 900 million active users (Facebook, 2012). According to Alexa Internet Inc. (2012), a global website metrics provider, Facebook is currently the second most popular website in the world, whilst the SNS Twitter ranks 9th and China’s largest Internet service portal QQ.com ranks 10th.

Social Network Sites in the media:

Most social network sites had attracted little media attention, particularly those which grew to become popular amongst non–English speaking communities. For instance Orkut was initiated in the United States as an English–only social network site, however Portuguese speaking Brazilians became the dominant user group in the early stages of the site’s development and it later became increasingly popular in India (Madhavan (2007) cited in Boyd and Ellison, 2007). Although sites such as Orkut and Live Spaces were just as large as MySpace, if not larger, they never received a vast amount of media coverage in the English speaking media (Boyd and Ellison, 2007, p.218).

MySpace only attracted immense media interest after being purchased by a large News Corporation for 580 dollars in July 2005 (Arthur, 2012). When the site was launched in 2003 in Santa Monica, California, few journalists had noticed as it emerged thousands of miles away from Silicon Valley. Not long after MySpace had been purchased by News Corp, accusations held the social network site to be implicated in a series of sexual interactions among adults and minors. According to Boyd and Ellison (2007) however, research had suggested that these accusations were exaggerated. Nevertheless, “a moral panic concerning sexual predators quickly spread” (Bahney (2006) in Boyd and Ellison, 2007, p.217).

"*Crime risk warnings to users of social networking sites*" (Barrett, 2007), is only one of the many headlines in the media featuring the dangers users are subjected to when engaging in various activities on social network sites. Concerns over privacy issues, fraud (Mail Online, 2007; Finkle, 2009), identity theft (BBC, 2011a), hacking (Williams, 2012; Holden, 2012), hate crimes (Channel 4 News, 2012) and so on, are often featured in newspaper articles. A study carried out by Dowland et. al. (1999) revealed that on average stories concerning computer related criminal activity was published two times a week during the period of their surveying of two UK newspapers (Cited in Yar, 2006).

Media coverage of Facebook

Due to the popularity of Facebook, it is not surprising that the social network site has not escaped media criticism. A browse through the online archives of popular news agencies over the last few years reveals the tremendous amount of coverage Facebook has been given. Many of the articles featuring the social network site aim at making the public aware of the possible risks they may be putting themselves in by sharing their personal details on the site (BBC, 2011a; Mail Online, 2007). Moreover, it has been alleged that the popular social network site has been used as an avenue for various other criminal activities. Offences ranging from stalking, hate speech, bullying (BBC, 2011b), to more serious offences such as '*sexting*' (Mail Online, 2011) and grooming (BBC, 2012) are increasingly being reported by the media. A number of incidents of sexual offences involving minors have caught a vast amount of coverage due to the sensitivity of the issue.

In addition to the crimes Facebook is accused to be engaged in, news items reveal unlawful activities that occur not on the social network site itself, but rather the ways by which Facebook was used to assist traditional forms of offending. One of the most recent examples is the use of Facebook to provoke disorder during the riots in England in August 2011. Although the riots took place in 'the real world', the news that two men were jailed for using Facebook to incite chaos, quickly made its appearance in international news agencies' articles which directed the blame towards Facebook and the other implicated social network sites (Green, 2011; Russia Today, 2011). The murders of Camille Mathurasingh (BBC, 2010a) and Emma Forrester (The Independent, 2008) over their Facebook postings, are two of the many high profile cases which as well, quickly made the round of the world through news reports which spread fear to users of the social network site, despite the fact that these took place in the terrestrial world.

Moral panic?

As the cyber community of Facebook grows and becomes further integrated into our daily lives, alongside this grows the threat to our familiar ways of living. The fear of crime and victimisation is a continuing phenomenon, particularly in Western societies. The ongoing over – reporting of potential or existing threats to users of social network sites by the media, provokes the already existing public anxiety about crime, resulting in a state of panic. Moral panic is defined by Cohen (2004) as "condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media..." (Cited in Garland, 2008, p.10). The furore over Canudos in Brazil, fear and prosecution of homosexuals in Boise, Idaho and the abduction of women in Orleans, France (Goode and Ben-Yehuda, 1994) are only some of the many incidences throughout history, which generate public fear associated with a particular group of people within those communities.

However, as in the above cases, moral panics refer to the fear generated by which evidence is largely out of proportion or in some cases nonexistent. This became the case with the emergence of the internet, following the over – reporting and over – inflating of the figures in regards to cyber criminal activity. According however to Yar (2010) "... [The] fear of crime often exceeds any objective measure of likely victimisation. In other words, public perceptions of risk are largely out of proportion to the actual chances of being a victim of any given form of criminal predation" (p.107).

Is the over – reporting of criminal activity linked to Facebook an indicator that history is repeating itself once again? Is this phenomenon a state of 'moral panic' or are the mass media and public concerns over cyber-criminal activities on Facebook justified? Are the hackers, crackers and spies, who use the social network site to carry out unlawful activities, modern day Mods and Rockers? There is no doubt about the existence of cybercrime. As in all 'real world' communities, crime is somewhat expected and in many cases unavoidable. The potential threats we are exposed to however, on the cyberspace of Facebook might in fact be largely exaggerated by the news media who play on public fear in order to produce headlines. In order to establish whether public anxiety over the use of social network sites is justified, this study has primarily set out to find the extent of criminal activity that occurs on, or is mediated by, Facebook.

Chapter 2: Research methods

This study aims at casting light on the extent and nature of criminal activity, which occurs on, or is mediated by, the social network Facebook. It was decided that the best method to adopt for this investigation, was to conduct semi-structured interviews. The semi-structured approach was chosen as it is useful as a strategy for detection, particularly when researching new grounds (Fielding and Thomas, 2008). The versatility of this method will permit an in – depth understanding in regards to trends, patterns and issues that arise from the use of the social network site Facebook.

Despite the valuable information that can be provided through qualitative research, the very nature of this approach is simultaneously the reason for its limitations. This method of research provides the researcher with detailed information in regards to the issue at hand, however it restricts the identification of generalizable themes (Trochim, 2001). For this reason, quantitative data will be sought in support of the finding from the interviews. This type of data will be collected through Freedom of Information (FOI) requests from individual police force in England and will allow a more in depth understanding of the problems that arise and concurrently allow generalization basted on statistical projections.

In this chapter the methods used for the collection and analysis of both qualitative and quantitative data which will be used for the purposes of this study will be outlined.

Interview method

Prior to commencing the study, research ethic approval was sought from the Department of Social Sciences' Research Director. Following ethical clearance, this study began with two pilot interviews. These were conducted in order to gather basic information in regards to trends and identify the extent of participant's knowledge regarding criminal activity on Facebook. The pilot interviews were conducted informally and formed the basis for the structure of the main study.

20 subjects were recruited, using advertisements posted on the social network site Facebook (Appendix 1). Participants were selected on a first come first served basis. The sample comprised of 12 males and 8 females aged between 19 and 69 years old (Mean age = 28.9). The interviews with students at the University of Hull took place in private study rooms in the university's library. Non student participants and students of other academic institutions were either interviewed over the phone or Skype. All interviews were conducted formally and the data was recorded on a digital audio recorder and transcribed manually.

The interviews encompassed some demographic questions, such as age and sex, alongside with some measures of Facebook use, for instance, time spent on the social network site and main activities subjects engaged in. Following this, participants were asked to answer a series of questions regarding their understanding in relation to the possible threats they are subjected to when using the social network site Facebook. Furthermore some questions were included to capture the influence of the media on usage of Facebook and the frequency of victimization on the cyberspace of Facebook.

Freedom Of Information request

Qualitative data is a valuable tool for social science research. By acknowledging however the limitations of this method, particularly when the sample size is small and literature or previous research is limited due to the newness of the subject, the need for further information in order to satisfy the needs of this project became apparent. Hence it was determined that quantitative measures could be used, which would usefully supplement and extend the qualitative analysis.

It was decided that information will only be sought from police forces in England for several reasons. Firstly, the inconsistency in recording practices as well as in crime classification can vary significantly between jurisdictions. The National Crime Recording Standard (NCRS) commence in 2002 (Simmons et. al., 2003) and the Perks Committee before that in 1967 (Maguire, 2007), aimed at promoting greater consistency in recording and classification of crime between police forces in England and Wales. Although discrepancy in recording methods remain to this day, these regulatory mechanisms introduced over the past years make it less probable that these inconsistencies in recording practices will have a significant impact on the data collected.

On the other hand, the purpose of this study is to shed light upon the extent as well as the nature of criminal activity which is in some way relates to the social network site Facebook. In order to identify patterns in reporting criminal activity, as well as to develop an in depth understanding in regards to nature of criminal activity that emerges on, or is mediated by the social network site, the qualitative data collected from the interviews must be comparable to the quantitative data. This would not be achievable where the interview sample does not fall under the jurisdiction from which the quantitative data is derived from.

In England and Wales, Facebook related crimes are not recorded separately from terrestrial criminal activity. Consequently official statistics published by the Home Office do not reveal the nature or extent of cyber criminality on the social network site Facebook. Therefore for the purposes of this study, the information as to the number of reports and the nature of criminal activity brought to the attention of the police was sought through Freedom Of Information (FOI) requests to individual police forces in England.

Further to establishing the needs of for this project and identifying the means by which the data required would be obtained, FOI requests were sent to 32 individual police forces in England. To ensure maximum consistency in responses, an identical request was sent to all forces. The request was sent via email or through an online FOI request form, where available, and required information on the following matters:

a) The number of reports made, which in some way relate to the social network site Facebook.
b) Where it is possible a breakdown of the nature of these crimes. For example, if they were complaints of harassment, assault, sexual offences, theft, burglary and so forth
c) and the outcome of these reports. For instance whether they resulted in a conviction.

This information was asked to be provided separately for 2009, 2010 and 2011.

Of the total 32 police forces from which the information was requested, 15 satisfied some or all aspects of the request. 8 police forces refused to provide any information, whereas 6 forces acknowledged the receipt of the request but as of this writing, have not yet provided nor refused to provide the information requested. Finally 3 police forces have yet to make any contact in regards to the request for information (Appendix 2).

Although the number of reports relating to Facebook in 2008, was not requested, nevertheless 4 police forces made this information available. No information however was given as to the outcome of these reports received that year. The number of incidents recorded in 2009 was made available by 14 police forces. Of those, one included reports from September 6th of that year onwards. In both 2010 and 2011 records of reports received, were made available by 14 individual forces. However of those 14 forces which provided records for 2011, one included reports up to August 31st whilst another made available the number of reports received up to November 30th that year. All forces provided a breakdown of the nature of reports received in 2009, 2010 and 2011. Three police forces provided figures which included reports made that mentioned both social network sites Facebook and Twitter. As the number of reports in which the social network site Facebook was mentioned during the report was not recorded separately, this affected results gathered for years 2009, 2010 and 2011.

The findings from both FOI requests as well as from the interviews conducted will be presented in chapters 3 and 4, in which they will be discussed and compared to existing literature and previous studies. Following in chapter 5, this study will be evaluated and limitations of this research project will be outlined.

Chapter 3: The extent of Facebook crime

As shown in chapter one, Facebook has attracted a vast amount of media attention. Warnings regarding the risks that users of social network sites are subjected to are often featured in the in news articles, internet blogs and television programs. The purpose of this chapter is to examine whether the concerns of the media are justified and if so to what extent. Are the threats to users of social networks the product of media exaggeration or has Facebook become an actual crime hazard? To establish the extent to which the social network site Facebook has become a conduit for criminal activity, this chapter will present the findings from the current study and draw upon existing literature and previous studies.

Reporting Facebook crime

A quantitative analysis of the data gathered through the Freedom Of Information (FOI) requests sent to individual police forces in England, reveals a massive increase in reporting criminal activity which in some way implicates the social network site Facebook between the years 2008 and 2011. In 2008 the number of reports received by the police, were relatively trivial compared to those received the following years. The lowest number of incidents, mentioning the social network site in 2008, was recorded by the Humberside Police which received just 1 report in which Facebook was mentioned. On the other side of the scale, that same year Hertfordshire Police records indicate 31 incidents where the social network site was mentioned during the report (Appendix 3).

The following year, in 2009 the same four police forces received 443.7% more reports in regards to criminal activity which in some way the social network site Facebook was involved. Similarly to the previous year, the smallest number of reports was received by Humberside Police. Of the 14 police forces which made available the number of reports they received in 2009, Suffolk Constabulary had the largest number of recorded incidents, those being 568.9% more than Humberside Police which only recorded 6 reports that year (Appendix 4).

In contrast to 443.75% increase in reporting between 2008 and 2009, there was a significantly smaller increase between 2009 and 2010, with a raise of 229%. Out of the 14 police forces which provided data for 2010, the lowest number of reports was 17 which were received by Derbyshire Constabulary. Once again the largest number of reports was made to Suffolk Constabulary. The 1545 incidents reported to Suffolk Constabulary are 8988.2% more than those reported to Derbyshire Constabulary that same year (Appendix 5).

The rise in reports between 2010 and 2011 is yet again comparatively lower than the massive increase between 2008 and 2009. With the decline in reporting Facebook related crimes to 3 police forces in England in 2011, there was only a 27.5% increase from the previous year. Decrease in the number of reports between 2010 and 2011 was evident in the data provided by Hertfordshire Police, Norfolk Police and South Yorkshire Police with -13.6%, -96.4% and -86.5% respectively. Similarly to 2010 the lowest number of incidents was reported to Derbyshire Constabulary and the highest amount of reports was to Suffolk Constabulary. According to the data provided by Suffolk Constabulary they received 1814 reports that year, 7786.9% more than Derbyshire Constabulary which received 23 reports involving Facebook related incidents (Appendix 6).

Increase in reporting

Observing the data provided by 15 police forces in England, it is evident that there is a large increase in reporting crimes in which the social network Facebook was mentioned during the report. Although the increase appears to reduce over time, the high numbers of incidents relating to Facebook are a source for concern. There are however several factors which contribute to these elevated numbers in recorded incidents by the authorities, which need to be taken into account.

One of the possible reasons for the apparent rise in reporting online criminal activity could be attributed to the increase of Facebook users. Facebook has grown massively since its emergence, particularly after its expansion in 2006 allowing anybody to join the site. As in every society, the growth of the population results in the rise of criminal activity within the particular community. This does not exclude cyber communities which are very much structured and run in the same way as those in the terrestrial world. On the 1st of July 2008 there were 11,171,540 Facebook users in the UK. By the 1st of July 2010 the number of Facebook users in the UK reached 26,543,600, an increase of 137.6% (Burcher, 2010). The growth in popularity of Facebook however can only partly explain the increase in reporting, as the number of reports between 2008 and 2010 was significantly larger than the increase in Facebook users between those years.

A further assumption that could partially explain the immense increase in reporting Facebook related crimes to the police, is the ease by which reporting of non emergency crimes can be achieved. In 2006 a small number of police forces in England and Wales piloted the 101 police non emergency number. By 2011 all police forces in England and Wales introduced the new number. Sheffield, one of the 2006 pilot areas, showed to have an 11% increase in call volumes following their campaign activity (Home Office, 2011). This however is unlikely to have affected the number of reports as only a small area of South Yorkshire Police provided this service out of the 15 forces which responded to the Freedom Of Information (FOI) request. Nonetheless, several police forces now provide an online crime reporting system which allows anybody with access to a computer and internet to report an offence with relative ease and in a quick manner. In addition, many police forces have made their websites accessible to users of Smartphones and other wireless devices. Although a relationship between the ease in reporting with the elevated number of incidents recorded by the police may exist, this cannot be confirmed as there is no available information as to when these methods have been adopted by each police force.

Additionally noteworthy is the fact that only four police forces made available the number of incidents they have recorded during 2008. Although there is no doubt about the increase in reporting offences relating to the social network site Facebook, it is perhaps rational to presume that the pattern that emerged could have been significantly different provided that information in regards to recording trends that particular year were available.

Of particular concern however are the large numbers of incidents recorded by Suffolk Constabulary. In 2009 the lowest number of incidents was recorded by Humberside Police which received just 6 reports, 562 less than those received by Suffolk constabulary. Similarly in 2010 and 2011 Suffolk Constabulary received the largest amount of reports. In 2010, 1545 reports were made to Suffolk Constabulary followed by only 258 to Hertfordshire Police. The following year there were 1814 incidents reported to Suffolk Constabulary, followed by 359 reports to Leicestershire Constabulary. In all three years that Suffolk constabulary has provided data on, the number of reports were significantly higher in comparison to reports made to other police forces in England.

Although it is difficult to explain why Suffolk Constabulary appears to receive such a large number of reports regarding Facebook, this could yet again be attributed to the ease by which the public can report non emergency crimes to the particular force. Suffolk Constabulary is one of the forces in England which provide the online crime reporting service. However, a vast amount of police forces such as Devon and Cornwall Constabulary and Merseyside Police have also introduced the online crime reporting service, without however having received such large number of reports. It seems possible that this is due to the layout of Suffolk Constabulary's website. The link which leads to the online reporting service is located on the front page of the force's website, accompanied by a colourful image beside the link. It is possible that this makes the link to reporting more apparent to those who wish to report a particular offence.

A further explanation for this is the fact that Suffolk Constabulary's website is available on mobile phones, as well as PDAs and other wireless devices. In 2010 the British Crime Survey found that just over 50% of the public knew how to contact their local authorities if they wished to report a crime (Home Office, 2011). The widely available methods to contact Suffolk Constabulary, allows those who do not have access to a computer to seek information in regards to reporting an offence using alternative means. In addition, the difference in recording practices and the misinterpretation of the FOI request could also, be possible explanations for the high number of reports received by Suffolk Constabulary. This however can neither be confirmed nor refuted and hence it remains unclear, what the causes for the large number of reporting Facebook related offences.

The dark figure of Facebook crime

As it is the case with all official statistics, what they reveal is important, though what they hide is crucial. Therefore, having looked at the factors that could have contributed to the increase in reporting, we shall now turn to the dark figure of Facebook crime. There is no doubt that statistics on crime disclose only a fraction of the true extent of criminal activity (Coleman & Moynihan, 1996) and Facebook crime is no exception. In order to provide a greater understanding in regards to the extent of criminal activity that is in some way linked to the social network site Facebook, the reasons for under reporting of such activity must be taken into account.

Similarly to traditional forms of criminal activity, there are several possible explanations for the under-reporting of cybercrime (Wall, 2005). Often victims are reluctant to bring an offence to the attention of the authorities as this is a time consuming procedure. Therefore in many cases victims of online criminal activity choose to seek alternative way with dealing with an issue rather than resorting to the police. However the severity of a crime has a great impact on whether or not a particular offence will be reported to the police (Coleman & Moynihan, 1996).

In the same way 'real world' offences are more likely to be reported if thought to be more serious, the same applies to online criminal activity. This was confirmed through the data collected from the interviews which were carried out for the purposes of this study. All participants who reported to have been a victim of an offence on the online environment of Facebook, stated that they did not report the transgression to their local police authorities. John, 26, explained the reason "I'd feel that I was wasting their time if I did that... [I would go to the police] if it involved money but in case of hate I would probably tell Facebook first ...".

An additional reason for the under-reporting of cybercrime which reflects on the figures of cyber criminality can also be attributed to the victim's unawareness of a crime being committed (Maguire, 2007). There is a large ambiguity as to what consists of a cybercrime and hence this has a great impact on the likeliness of an offence being reported. During the course of this study, it became apparent that in many instances victims were at least at first, unaware that an offence had been committed. This was particularly the case of victims of online spying which will be discussed further detail in the following chapter. This sort of criminal activity however, is generally seen as acceptable behaviour and hence not considered by the victim as a being crime.

To complicate the matter even further, in some instances there is no identifiable victim (Coleman & Moynihan, 1996). This is the case with internet trolling and hate, which in most instances are not directed towards a particular individual, but rather aims to cause alarm and distress on a larger scale. Although this behaviour can cause a vast amount of psychological distress to its recipients, it can often go unreported due to the very fact that this behaviour is not directed towards a specific user of the social network site.

Over-reporting of cybercrime

Because of the seemingly apparent indications as of the large amount of criminal activity that occurs on or is mediated by the social network site, Facebook is often portrayed in media reports as a hazardous online environment. The over – inflating of cybercrime figures is often the result of the various methodologies used in order to calculate the extent of online criminal activity, producing questionable 'guesstimates' as to the risks users of social networks are subjected to. The inflation of cybercrime problems, often serves the interests of various actors, such as internet security providers, who use these extravagant figures for their own purposes (Wall, 2007).

At the same time as the inflated figures are used to point the finger of blame at the social network site Facebook for being the cause or carrier of criminal activity, these allegations are over – reported by the media, who too, play on public fear for their own reasons. The over – reporting of this activity is evident through this study as all but one of the interviewees, report having read a news article featuring the danger associated with the social network site. Although such reports, found in the news media, on internet blogs and through television programs are not necessarily exaggerated, the methods used to gather and present this information are dubious.

One of the numerous reports regarding Facebook claims that "The Facebook crimewave hits 100,000 in the last five years" (Gill, 2010). Further, the author of this article claims that 16 police forces have received 7,545 calls between them, within a year of that writing. The author of this particular article however fails to take into account the fact that the calls were made does not necessarily denote that a crime has in fact been committed.

Facebook: A hazardous online environment. Fact or fiction?

As discussed above, the data collected through the FOI requests indicates to an enormous increase in reports, in which Facebook was mentioned, received by the police since 2008. Nevertheless there are several possible explanations for this apparent increase in reporting such as the growth of the social network as well as the ease by which reporting can be achieved. Despite however the factors that to some extent contribute to the elevated number of reports received by the police, it becomes apparent that criminal activity on Facebook is existent and growing.

Caution must be drawn however to the fact that; police forces to some extent employ diverse recording practises, which consequently would lead one to be sceptical in regards to the accuracy of the extent in reporting behaviour. In addition, the responses to the FOI request include incidents in which the word 'Facebook' was mentioned during the report. It cannot be therefore assumed that in all instances, the social network site was a contributing factor to the offence.

At the same time much of the criminal activity connected to the social site is being under – reported to the police, we observe an over – reporting of this activity by the news media. This study however, has found that the excessive reporting of criminal activity relating to Facebook, has not had a significant impact upon the users of the site, which in the majority claim to be aware of the risks and dangers reported in the media, but nevertheless, carry on using the social network without fear of the possible outcomes.

"The apparent simultaneous over-reporting and under-reporting of cybercrime is actually a symptom of cybercrime being simultaneously over - problematised and also misunderstood" (Wall, 2010, p.89). Wall's account regarding the misapprehension of cybercriminal activity is evident through the exploration of public understanding regarding criminal activity on Facebook carried out for the purposes of this study. The interviews have shown that there is a common perception amongst participants that illegal activity on Facebook is associated with particular users of social network sites, such as young people. Most subjects who are aware of some crimes associated with the social network site, do not consider themselves being at risk of victimization.

Since is not possible to determine the exact extent of criminal activity in which Facebook is a contributing factor, in addition to the ambiguity that exists in regards to the nature of these offences, it is therefore necessary to further examine the problem from a different perspective. The following chapter of this dissertation will explore the nature of criminal activity caused or carried by the social network site in order to draw a conclusion as to the level of risk users Facebook are subjected to.

Chapter 4: The nature of Facebook crime

The pervious chapter has examined the problems that arise in determining the extent of criminal activity associated with the social network site Facebook. The over –reporting of Facebook related criminal activity by the media and the under – reporting of these activities by the public to the police, indicate that Facebook crime has been both over – problematised and misapprehended. The purpose of this chapter is to examine the nature of offences which occur on, or are mediated by, the social network site in order to produce a lucid picture of the problem posed by the use of Facebook.

The data collected through the Freedom Of Information (FOI) requests which were sent to individual police forces around England, has provided valuable information in regards to the types of criminal activity reported to the police which are in some way associated with Facebook. More than 100 categories of offences were identified and recorded between the forces, with Hertfordshire constabulary alone recording 75 different offences between 2008 and 2011. It is not possible however in this study to examine all categories of offences recorded by the police. Therefore in attempt to provide an understanding in regards to the nature of criminality linked to Facebook, this chapter will focus on some of the mostly recorded offences as well as offences which were identified through the interviews conducted for the purposes of this study.

Harassment

Given the nature of interactions that occur on social networking sites, the fact that harassment is the most common category of reported crime relating to Facebook is not surprising. Out of the 15 police forces which responded to the FOI request, 8 forces reveal that the highest number of reports they received concerned harassment. A further 5 police forces indicate that harassment was one of the top three most recorded offences relating to the social network site.

According to the Crown Prosecution Service, English law does not contain a specific definition of harassment, however "*it can include repeated attempts to impose unwanted communications and contacts upon a victim in a manner that could be expected to cause distress or fear in any reasonable person"* (The Crown Prosecution Service, n.d.). The Protection from Harassment Act 1997 governs a variety of acts such as stalking, bullying, hate speech and so forth (Finch, 2001). Although legislation regarding such conduct is relatively recent, harassment is by no means a new kind of behaviour. The internet however has created a large range of possibilities for cyber harassment.

Throughout the nineties cyber harassment primarily involved spamming and the sending of computer viruses (Ellison and Akdeniz, 1998). The later emergence of social network sites produced all the more opportunities for such acts. Distance is no longer an obstacle to harassment and the massive growth in popularity of social network sites has made direct forms of harassment a global phenomenon. One of the interviewees, Emilia, age 36, shared her experience of harassment on Facebook. She said: "I faced some harassment before because of a group I created on Facebook. People I didn't even know constantly threatened me because they didn't agree with my views."

Cyber stalking

Cyber stalking according to Joseph (2002) can be defined as "unwanted, threatening or offensive email or other personal communication over the computer that persists in spite of requests by the victim that it be stopped" (p.106). Although there is no specific legislation in English law against stalking, the Protection of Harassment Act 1997 offers both criminal and civil measures against stalking (Ellison and Akdeniz, 1998). Though 'traditional' and online stalking only differ by the means used to gather information or contact the victim, there is much debate as to whether it should be conceptualised as an addition to 'real world' stalking or as a new type of unlawful behaviour (Roberts, 2008).

As with terrestrial stalking there is no easy way to determine the prevalence of cyber stalking as it is not an offence in its own right (Finch, 2001). However the high number of harassment cases reported to the police could be the result of stalking on the virtual environment of Facebook. The social network is a heaven for stalkers who are able to identify and target their victims through sites, such as Facebook, with ease. Personal information about users is extensively available on social network sites and this is often used as a tool for online stalking (Roberts, 2008). "The real fear, however, is that offensive and threatening behaviour that originates on-line will escalate into "real life" stalking" (Ellison and Akdeniz, 1998, p.31). Consequently this leads to a further issue in regards to the social network site which is privacy.

The amount of personal details users of social network sites make available, have attracted the attention of scholars such as Gross and Acquisti (2005) who argue that users of social network sites are putting themselves at risk, both online and offline (Cited in Ellison et. al., 2007). Although Facebook allows its users to select what information is shared and with whom, the large number of harassment reports brought to the attention of the authorities could be considered as evidence of the users ignorance in regards to security options available to them. This study however has found that the majority of users, particularly the younger users of Facebook, are to some extent familiar with the privacy settings the social network provides. Of the 20 Facebook users who participated in this study, 8 reported having changed the privacy settings, enabling only 'friends' to view personal information they share on the site.

This however does not eliminate the possibility of becoming a victim of cyber stalking for several reasons. The first question that should be asked is who our Facebook 'friends' are? Although the main function of Facebook is to maintain offline relationships, this does not prevent new connections from occurring. While there are provisions that allow users to include or exclude particular 'friends' from viewing certain personal information, this requires quite extensive knowledge of Facebook's privacy settings. Additionally, creating a Facebook profile account providing false personal details is relatively easy to accomplish, hence it is not always possible to be certain who is hiding behind a Facebook profile. Therefore many users may be putting themselves at risk by providing sensitive personal information to strangers. On the other hand, personal information such as telephone numbers and addresses can often be found through online databases such as 192.com (Ellison and Akdeniz, 1998). The problem that derives from this is rather alarming, as the amount and nature of personal information available over the internet may be beyond our own control.

Hate speech

Moving on to another form of harassment which is, hate speech, it is notable that this is perhaps the only form of harassment which is not specifically directed towards a particular individual but rather, it is hate directed towards the group the victim affiliates with. According to Nielsen, (2002) hate speech is defined as "speech that (1) has a message of racial inferiority, (2) is directed against a member of a historically oppressed group, and (3) is persecutory, hateful and degrading" (Cited in Yar, 2006, p.99). Hate speech is a relatively new offence, which emerged as a consequence of public pressure for legal action to be taken against discriminatory language, exclusion and violent behaviour (Yar, 2006).

What is distinct about online hate speech is the fact that there are no geographical boundaries. This allows such ideologists to promote their ideas on a far larger scale than previously possible and with far less consequences (Jewkes, 2002). Moreover, social network sites act as a tool for recruitment and confederation of those sharing analogous views (Jaishankar, 2008), allowing them to promote their hate propaganda and extremist ideologies, whilst "...facilitating the creation of a collective identity and empowering sense of community" (Perry (2001) in Jewkes, 2002, p.22).

In recent years many hate groups have made their appearance on Facebook, promoting hate towards particular ethnic, religious and other minority groups. According to the news agency Reuters (2009) "the most often targeted groups in these social networking sites are Jews, Catholics, Muslims, Hindus, gays, women and immigrants" (Cited in Jaishankar, 2008, p.17). Following public pressure, Facebook has removed a number of groups which used the social network site as a medium to spread hatred.

26 year old John, a victim of hate speech on the social network site Facebook said: "[Hate groups] were rife a few years ago. You could search for anti-gay groups and you would find them very easily, hundreds of them. Some with just two in them, some with thousands of members in them". Despite however the efforts to eliminate racism and discrimination from Facebook, much of this hatred persist to exist under the guise of politically orientated groups.

Trolling

Internet trolling according to Yar (2012) '*...refers the actions of individuals who deliberately seek out opportunities to post abusive commentary online, with specific intention of causing alarm and distress*' (p.10). This behaviour poses a huge problem, as the targets of trolling are often tribute sites, which are set up by relatives and friends of the recently deceased. This can cause a great amount of distress and suffering to the families and friends of the deceased, who are already suffering a loss (BBC Tree, 2012). This activity which is an offence under the Malicious Communications Act 1988, does not feature in the data collected for the purposes of this study. However, it was decided that to be discussed in this chapter because of the all and more cases of this phenomenon that are brought to the attention of the media.

Recently, a page set up on Facebook to allow relatives and friends to write tributes, to a recently deceased teenage girl who died from leukaemia earlier this year, had become the target of internet trolls (Harding, 2012). In yet another case internet trolls, added pictures on Facebook of a girl with Down's syndrome, adding sexual and derogatory captions to the girl's photo (The Sun, 2012). This online behaviour, illustrates once again how the open nature of Facebook leaves us vulnerable to unwanted and inappropriate communications. This is particularly concerning however, when the target of these unwelcome communications are individuals who are already suffering because of the loss of a loved one or another misfortune. Further problematic with internet trolling is the fact that perpetrators often create fake accounts which they use to carry out their post offensive commentary. This not only does it allow trolls to avoid detection, but it also enables them to continue posting abusive messages using a different Facebook account after one account has been blocked.

Assault

A large number of reports to the police by Facebook users are in connection to assault occasioning actual bodily harm. It is not possible however to examine each case individually in order to determine if these are actually the result of online interactions and if so how this online behaviour provokes violent actions in the terrestrial world. In attempt to explain this phenomenon one may look at other categories of crime reported to the police that could provoke violent attitudes, such as the various forms of harassment discussed above.

Cyber bullying is yet another form of harassment which has been associated with violent behaviour and hence could be a product of assault. The negative effect of cyber bullying is featured in Anti – Social Network, a documentary by Richard Bacon (BBC Three, 2012). Although this presents one of the most extreme cases, where a teenager takes his own life as a result of him being bullied on Facebook, it is not hard to imagine that in less acute cases this could result in violence. According to Willard (2008) incidence such as cyber bullying that occur away from school, can influence in school behaviour, for instance school violence (cited in Kraft and Wang, 2009).

In yet another extreme case, a man attacked and killed his wife following an update the woman posted on the social network Facebook subsequent to the couple's separation (BBC, 2008). The cases however that come to the attention of the news and other media are the most extreme of cases and therefore must be treated with caution as the incidents which lead to excessive violence only comprise a fraction of computer mediated crime. Moreover one should be cautious in interpreting these results, at it remains unclear whether the user's offline relationships are what influence online behaviour or vice versa.

Sex offences

The vast number of media reports in regards to sexual offences over the internet, have created the perception that such activity has become a common phenomenon. The exact occurrence however of sexually motivated crimes is difficult to determine, particularly when these involve young people (Bryce, 2010). Responses to the FOI request indicate that sex offences, which in some way relate to the social network site Facebook, are relatively low. However, great concern over the safety of children on social network sites remains, as this has a great impact on their psychological and physical wellbeing.

The all and more active engagement of children in computer mediated communications through social network sites raises many worries in regards to a variety of potential threats they are subjected to in the online environments they engage in. Perhaps one of the most extensive problems that derives from young people's use of social network sites is in regards to sexual grooming. In English law sexual grooming is defined as "A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes" (Home Office (2002) cited in Chase and Statham, 2005, p.12). In other words, sexual grooming is the preparatory stage, for a planned face to face sexual abuse of a minor.

Social network sites have become the new hunting ground for paedophiles, who use the sites to identify and attempt contact their prospective victims. Typically the offender will first attempt to establish an online relationship with the victim. When intimacy and trust are established between the victim and offender, the perpetrator will attempt to meet the child face to face and suggest sexual contact (Yar, 2006). There is extreme difficulty however in determining the prevalence of this offence. This is because it is largely dependent on the victim's awareness and recognition that an offence has been committed. Consequently it is believed that sexual grooming is likely to be under-reported (Bryce, 2010).

Sex offences mediated by social network sites however are not limited to sexual grooming despite the fact that these cases attract the majority of media attention. Online exportation of children can include 'cyber-rape', sexually explicit conversations and 'fantasy enactment' of sexual scenarios (Yar, 2006). Yet again there is no easy way to determine the prevalence of these online behaviours as figures are subjected to limitations. However, "given the potential difficulties associated with recognition and reporting of associated behaviours, it seems likely that recording figures represent only a small proportion of sexual offending against young people which involves the Internet and related technologies" (Bryce, 2010, p.332).

Frape a growing trend

Moving on from the most serious of crimes regarding Facebook, we now turn to the other side of the scale. Much of the activity users of the social network site engage in, are not perceived to be illegal. These acts however are in many cases highly intrusive as they invade the privacy of their victims. As a consequence of Facebook's growth in popularity, new trends have emerged. Some of the new trends have become so popular amongst Facebook users, that new names have been adopted for them. These trends are by no means new behaviour on cyberspace, however the terms are used to describe old behaviour, with the exception these are carried out on the social network site Facebook.

One of the newly emerged trends is 'frape', which literally means Facebook-rape. This refers to the unauthorised access to an individual's Facebook account. Frape, most commonly occurs as a consequence of devices, such as computers and smart phones, left unattended while logged-on Facebook accounts. Frapers take the opportunity to access a Facebook account, in order to change the victim's personal information, or use the victim's account 'poke' or message strangers. A previous study has found that over a third of snoopers between 18 – 24 years old, thought that doing so would be cool or humorous (Yar, 2011).

There is general misconception that this sort of online activity is permissible by law. More than half of participants in this study report to have been fraped or have fraped someone themselves at least once. This is particularly the case amongst the younger users of the social network site, who claim to engage in this activity for fun. 19 year old Valery explained: "me and my friends frape each other all the time, you know we just do it for fun... I don't think there is anything wrong with that. There are no bad intentions we just do it for a laugh". This extremely intrusive behaviour however, is a violation of the Computer Misuse Act 1990 which prohibits the unauthorised access to a computer with intent to commit a further offence (Computer Misuse Act 1990). The further offence here being fraud by false representation governed by the Fraud Act 2006 (Fraud Act 2006).

Privacy

Privacy is perhaps one of the most controversial issues in relation to social network sites. As in the case of stalking discussed above, privacy has a significant function in users' safety, both online and offline. Much of the criminal activity that is mediated by the internet is primarily due to the availability and accessibility of excessive personal information being posted on social network sites. According to the routine activities theory, a crime takes place as a result of the accordance of three elements, a) there is a person willing to commit an offence, b) a there suitable target and c) the absence of someone to prevent the offence (Yar, 2012).

The results from the FOI requests reveal a large number of offences involving burglary, criminal damage and so on. These may well be the result of individuals making themselves visible to online offenders who 'loiter' in online communities waiting for a suitable target. The public sharing of personal activities and real time locations, on social network sites provide offenders an array of opportunities to carry out an offence. However, those who engage in these acts are not always the modern day 'folk devils' the mass media makes them out to be. A recent study on the motivations of social network users, found that

30% of adults in the UK use social network sites to spy upon others. These snoops and spies are often partners, friends and colleagues who out of curiosity most commonly, secretly access our personal information (Yar, 2011). "The findings suggest that we have a culture in which privacy is increasingly fragile, with many of us at the risk of our personal information and communications becoming available to people we wouldn't necessarily want" (Yar, 2011, p.19).

Hacking

Hacking is perhaps the most commonly associated with the internet criminal activity. This is most probably due to the fact that this type of criminal activity has over the years caused large corporations and government agencies many millions of pounds in losses. The primary aim of hacking according to Wall (2007) is "to breach the security of a networked computer by assaulting its integrity" (p.53). After gaining access to a personal computer, a range of further criminal activities become possible. Although motivations for hacking vary, activities following a computer intrusion can include theft of computer resources, system sabotage and so forth (Yar, 2006).

Facebook hacking refers to the unauthorised access to an individual's account. Unlike 'frape' which is relatively harmless, Facebook hackers, gain access to an account and use it to commit further offences such as fraud, trolling and so on. Additionally, Facebook hackers may 'mine' sensitive personal information that is available on the site which can potentially be used for blackmailing the rightful owner of the account (Yar, 2011). This increasingly popular online behaviour could be a possible explanation for the high number of fraud reports received by the police, in which the social network site was mentioned during the report.

Detecting and convicting Facebook crime

Detecting and convicting Facebook related criminal activity, can be a significantly difficult task for law enforcement agencies. Although little information was provided by the police through the FOI requests in regards to how the reports were resolved, the data that has been made available shows that a large number of reports remains undetected. This is particularly evident in the data provided by Suffolk Constabulary. Out of the 3927 reports received by the particular police force between 2009 and 2011, 2454 remain undetected. Similarly, out of the 614 reports received by Devon and Cornwall Police between 2009 and 2011, only 90 resulted in a conviction.

The difficulties in detecting cyber – crime and other criminal activity in which the internet was used as an avenue for the committing of offences lies in the fact that, there are no physical boundaries. Often the offender is thousands of miles away from the victim, consequently they do not fall within the same jurisdiction the complaint was made. Although some international agencies such as Interpol and Europol do investigate crimes occurring across police forces, these tend to deal with the most serious of internet – related criminal activity. Furthermore, police forces are subjected to budgetary restrictions and therefore, "a common complaint made by the police and law enforcement agencies is that they do not have the facilities to keep up with criminals" (Wall, 2005, p.11).

Noteworthy however is the fact that the same qualities of social network sites which create opportunities for offending are often the same merits used by the police for investigation and provide new sources of evidence with which prosecutions and convictions can be established (Wall, 2005). Several police forces have now set up their own Facebook pages, in which they post appeals for help. This public visibility of the police and the accessibility to the information and appeals police forces post on the social network site has become an increasingly popular way of investigating and solving crime. Following an appeal put on the Facebook site of North Down Police in Chicago, the force with help of citizens who saw the appeal on the social network site, found a stolen car (BBC, 2010b). As well as in the United States, this new tool for tackling crime has become increasingly popular in the UK, which is evident from the fact that all forces England now have their own Facebook page.

A further way by which police forces can use to social network site Facebook for investigating and collecting evidence is by monitoring the activity on the site. This method of intelligence - gathering has proven to be effective further to an incident last year were a teenage boy pleaded not - guilty for flooding Portsmouth's central library causing £150,000 damage, changed his plea after being presented with a transcript of a Facebook conversation, in which he admitted to a friend that he was the one who caused the flood (Travis, 2011). This latter method however used by the police and other agencies, according to Yar (2012), "raise[s] real concerns about the extent of state intrusion into users' communications, and the potential violations of privacy rights that might arise in consequence" (p.15).

Who are the victims of Facebook crime?

Unlike previous studies (Marcum et. al., 2010), this study has found no significant correlation between the time spent on Facebook and the chances of becoming a victim of a criminal activity. 80% of subjects access the site at least once a day, many of whom report to spend more than 2 hours a day on the social network site. However, excluding frape, only 2 of the 20 subjects reported to have been a victim of some form of criminal activity that relates to the social network site. Furthermore, the age of the user does not appear to have a significant impact on the chances of becoming victimised on or through the online environment of Facebook. There is however the need for further investigation in order to draw a lucid picture.

The nature of criminal activity on Facebook

The discussion throughout this chapter focused on criminal activity that has been associated with the social network site Facebook. Through this discussion it became apparent that offences mediated by the social network site or took place on the online community of Facebook vary significantly in severity. The majority however of these offences are by no means new behaviour that emerged since the emergence of the site. Stalking, harassment, bullying and so forth, are behaviours that have a long history, despite the fact that much of the legislation which covers them is relatively new.

The internet and specifically social network sites such as Facebook, have in recent years provided new means by which such offences can be carried out. However, these offences are no more than an extension of already familiar offences. What is distinct about online criminal activity is that previously known offences can now have a significant impact on people's lives, due to the lack of geographical borders. Such criminal activity can now be carried out on a far larger scale than could ever be imagined prior to the internet.

Although new offences have emerged post internet era, these types of criminal activity do not seem to have a significant impact on social network sites. Offences such as hacking and spamming, which are often presented as the main threats of online criminal activity by the media, do not appear to have a significant impact on users of Facebook, although they are not distinct from the site.

What is problematic about online criminal activity is difficulty by which perpetrators can be identified and convicted. Although Facebook's policy prohibits the creation of an account using fake personal information, this is easily accomplished. Consequently, the ease by which perpetrators can remain anonymous reduces the chances of being identified and convicted for their acts. In addition, it is often the case that victim and offender are hundreds or thousands of miles apart. This does not only pose a problem in identifying the offender, but what it is rather problematic in establishing a conviction. This is due to the fact that laws covering cyber criminal activity can vary significantly from one jurisdiction to another.

Noteworthy however is the fact in many cases of offences committed on, or mediated by the social network site Facebook, the offender is known to the victim. This is particularly the case with frape and snooping, however it can include offences such as harassment, bullying and so forth. Much of the activities users of the social network engage in are influenced by existent offline relationships between two parties. In many instances of violent acts, the social network site is used only to provoke already existent problems which may explain the increased number of offences of assault occasioning actual bodily harm.

Despite the over – reporting of the online risks by the media and the extensive reporting in regards to privacy issues on the social network site, there is much evidence that the public remain unaware of the possible risks they are subjected to. There is a clear need to increase awareness to users of social network sites and those who engage in online activities in general, as to the available options to ensure safe online interactions. Enhanced knowledge of the risks users are subjected to, as well as awareness in regards to online privacy options, may not eliminate criminal activity, it could however largely reduce the likelihood of becoming a victim of online and offline criminal activity.

Chapter 5: Conclusion

Limitations and further research

A number of caveats need to be noted regarding the validity and reliability of the data gathered for the purpose in this study. Data collected by oral or verbal responses is inevitably a subjected to inaccuracies. This is because "people sometimes lie or elaborate on the 'true' situations to enhance their esteem, cover up discreditable actions or for any of a whole gamut of motives" (Fielding and Thomas, 2008). One of the most important limitations however, lies in the fact that the sample size was relatively small and the majority of subjects in this study were university students. The implication of this is that the findings may not be transferable to the general population as it has been shown through this study that, students spend more time on Facebook than non students. Further this study has found that students were better informed about the risks users of social networks are subjected to. Subsequently we may have observed very different patterns in victimisation, had the sample comprised of more non student subjects.

Furthermore, the small sample size has an impact on the accuracy measuring the effect and significance of correlations. This study has found no correlation between the time spent on the social network site and the chances of becoming a victim of a criminal activity, despite the contrary findings from previous studies. This may be the result of the small sample size used in this research. Further, this study was unable to identify whether a large number of Facebook 'friends' has an impact on the chances of becoming a victim of unlawful acts on Facebook. It is suggested that the association of these factors is investigated in future studies.

In addition, the subject group of this study consisted of participants over 18 years old. Therefore important information in regards to the use of Facebook by younger age groups; as well as possible criminal activity involving minors, has not been addressed in this study. Teenagers are often the target of cyber bullying, sex offences, sexting and so forth. This could be the result of differences in the online activities younger people engage in. It would therefore be interesting to see in further studies the motives and uses of Facebook by younger users of the social network site and how these may influence the high level of victimisation of this group of individuals.

Furthermore, the data gathered from the Freedom Of Information (FOI) requests to individual police forces, must be treated with extreme caution for several reasons. Firstly, although identical requests were sent to all forces in order to ensure maximum consistency in responses, the request could have been interpreted in a different way by each recipient. A further drawback of the data collected from the FOI requests lies in the fact that recording practices vary across police forces. This is problematic as it does not allow a comparison to be made between the data collected from different police forces. In addition, the records provided by the police, include incidents in which the social network site was mentioned during the report. It remains unclear however, as to what role Facebook played, if any, in the committing of these offences.

Nevertheless, the qualitative method used in this study has produced valuable knowledge in regards to how users of the social network site perceive the threats their online activities exposed them to. This knowledge can be used in the future, to form the basis for the development of quantitative research methods, which would allow the exploration of the nature and extent of criminal activity on Facebook on a larger scale. Furthermore, this information can form the basis for the development of victimisation survey, which would produce a clearer picture of victimisation levels as well as susceptible groups of individuals of Facebook related criminal activity.

Conclusion

This study set out to find the extent to which the social network site Facebook has become a conduit for criminal activity. The discussion throughout this dissertation has provided explanations for the large number of reports received by the police in relation to criminal activity which are in some way linked to Facebook. Despite however the factors that contribute to the elevated number of reports received by the police, it becomes apparent that criminal activity on Facebook is existent and growing. For this, it is safe to say with serenity that Facebook has indeed become a conduit for criminal activity, although there are extreme difficulties in assessing the exact level of risk the social network site poses to its users.

This dissertation has elaborated a number of offences associated with Facebook, in order to draw a conclusion regarding the level of risk users of the social network site are subjected to. This investigation has shown that many of the offences linked to Facebook are simply an extension of terrestrial criminal activity, though the internet has allowed these offences to occur on a much larger scale than previously possible. Despite the fact that these online activities are by no means new behaviour, this study has found that Facebook users are ill informed about the risks they are putting themselves in.

The very nature of social network sites raises concerns about privacy. "...participation in social media, with the extension of personal lives into quasi–public spaces that it necessary entails, brings as its inescapable counterpart a vulnerability to a wide range of criminal victimisation than previously seen" (Yar, 2012) Without doubt however, some of the risks users of Facebook are subjected to, may be reduced significantly by enhancing the knowledge of individuals using the social network site, as to the risks to which they may be exposing themselves in their extended public self – presentation.

We may therefore conclude that to some extent the news media is justified in highlighting the potential threats that emerge by participating in online communities. However, these reports must be taken with caution as often the figures presented are largely exaggerated and often, perpetrators are not the modern day 'folk devils' they are made out to be by the mass media.

As with any technological innovation "There will always be people who see only the potential to do good, while others see new opportunities to commit crime or make money" (Standage, 1998 cited in Wall, 2010, p.88).

Appendix 1

Interview sample group

Name*	Age	sex	employment status	Time spent on Facebook	no of FB friends
Emilia	36	F	Unemployed	several times a day	574
Chris	21	M	Student	once or twice a day	552
Paul	29	M	Student	once a day	248
Barbara	19	F	Student	several times a day	238
John	26	M	Student	several times a day	221
Anna	47	F	Full time	Once a month	21
Julie	69	F	Retired	4-5 times a week	15
Mark	45	M	Full time	2 hours a day	53
Andy	24	M	Part time	1 hour a day	511
Simon	21	M	Student	several times a day	715
Valery	19	F	Student	several times a day	514
Alex	22	M	Student	several times a day	260
Mary	21	F	Student	once or twice a day	171
Susan	31	F	Unemployed	most days	58
Philip	27	M	Full time	once a day	365
George	39	M	Full time	once a day	175
Peter	19	M	Student	several times a day	348
Laura	20	F	Student	once or twice a day	960
William	19	M	Student	several times a day	987
Tom	24	M	Full time	most days	341
	28.9				366.35

*In order to ensure confidentiality subjects names have been changed

Appendix 2

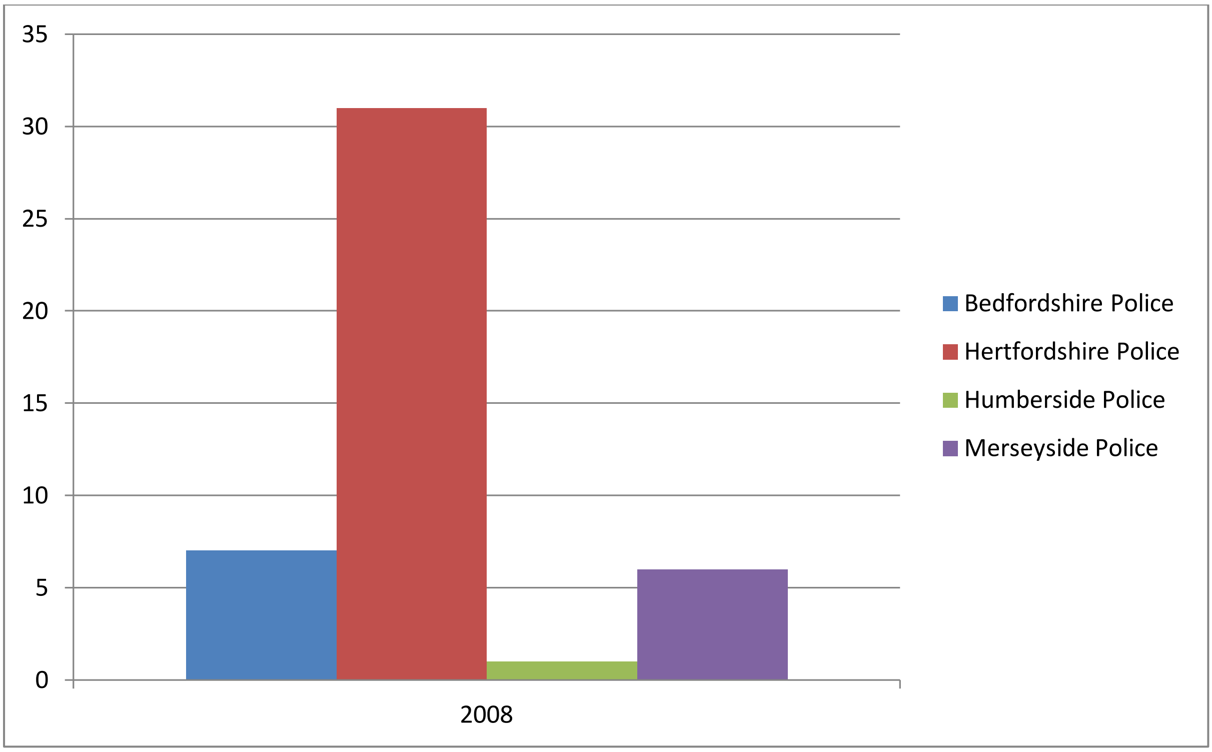
Responses from police forces

1	Metropolitan Police Service	Refused
2	Bedfordshire Police	Provided
3	Essex Police	Not Responded
4	Hertfordshire Constabulary	Provided
5	Norfolk Constabulary	Provided
6	Suffolk Constabulary	Provided
7	Sussex Police	Pending
8	Thames Valley Police	Refused
9	Avon and Somerset Constabulary	Refused
10	Devon and Cornwall Constabulary	Provided
11	Dorset Police	Pending
12	Gloucestershire Constabulary	Provided
13	Derbyshire Constabulary	Provided
14	Leicestershire Constabulary	Provided
15	Lincolnshire Police	Pending
16	Northamptonshire Police	Refused
17	Nottinghamshire Police	Provided
18	Staffordshire Police	Not Responded
19	Warwickshire Police	Refused
20	West Mercia Police	Refusal
21	West Midlands Police	Pending
22	Cleveland Police	Not Responded
23	Durham Constabulary	Refused
24	Humberside Police	Provided
25	North Yorkshire Police	Pending
26	South Yorkshire Police	Provided
27	West Yorkshire Police	Provided
28	Cheshire Constabulary	Provided
29	Cumbria Constabulary	Pending
30	Greater Manchester Police	Refusal
31	Merseyside Police	Provided
32	Lancashire Constabulary	Provided

Refusals:	08
Information give:	15
Awaiting response:	06
No response:	03
Total	**32**

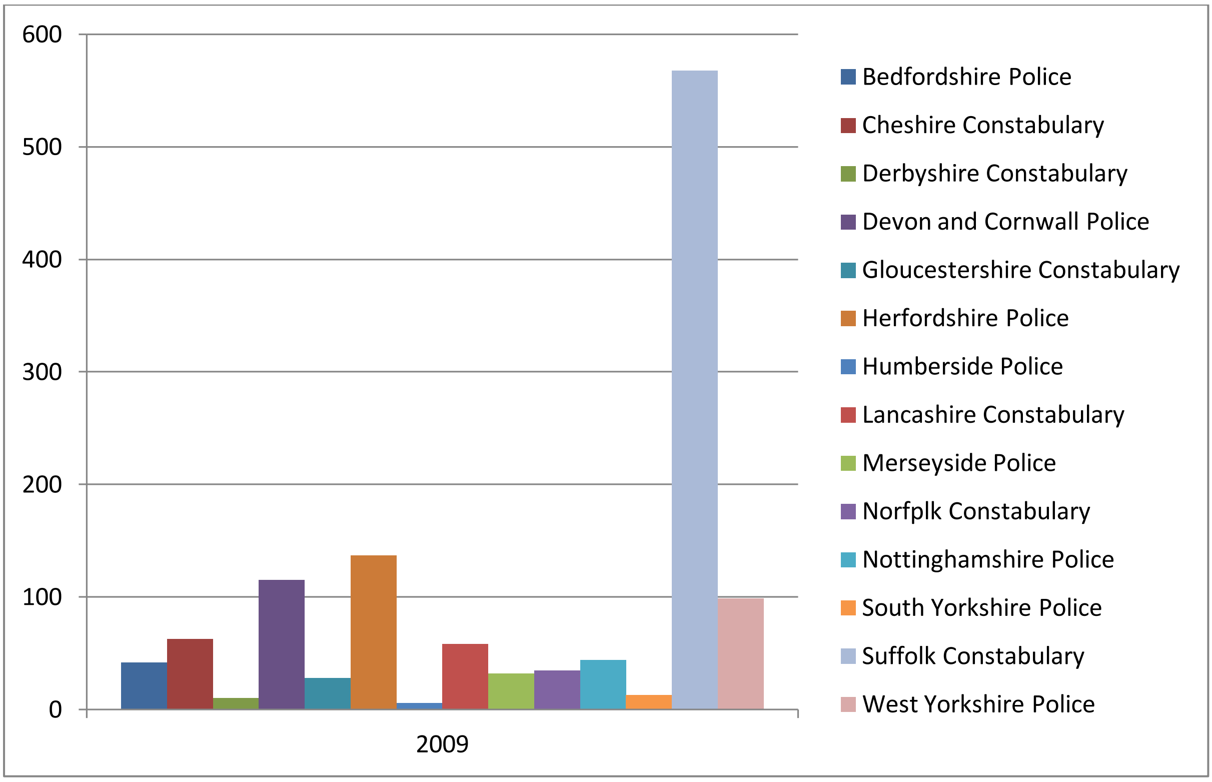
Appendix 3

Number of reports received in 2008



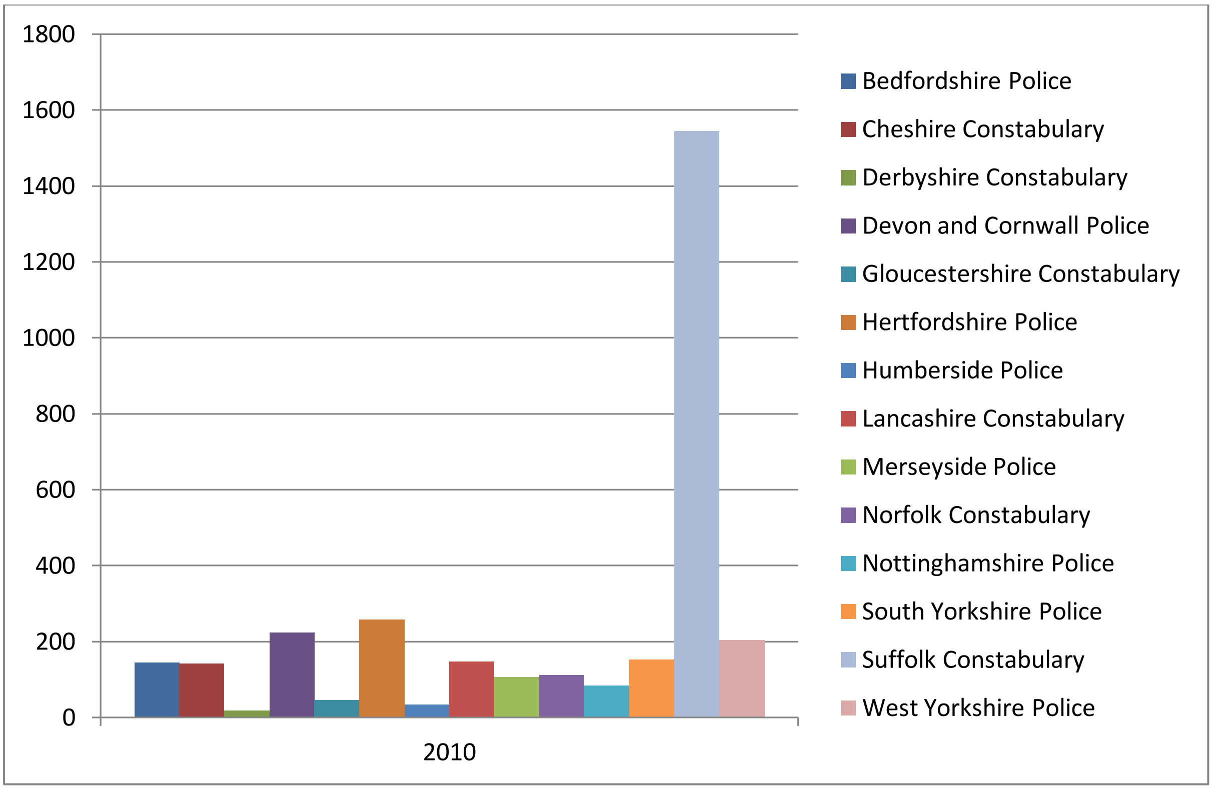
Appendix 4

Number of reports received in 2009



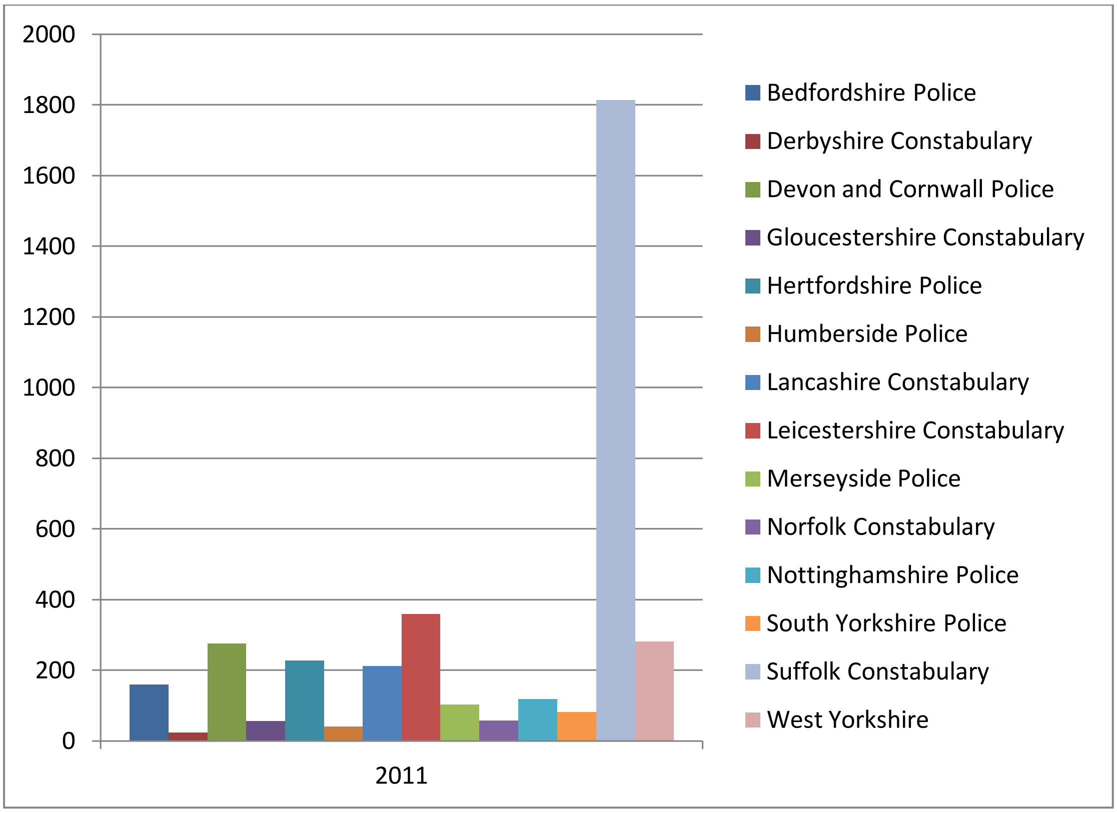
Appendix 5

Number of reports received in 2010



Appendix 6

Number of reports received in 2011



Bibliography:

Alexa Internet Inc. (2012) 'facebook.com' at: http://www.alexa.com/siteinfo/facebook.com (Accessed: 1 May 2012)

Arthur, C. (2012) 'From Instagram to MySpace: a guide to hip social startup acquisitions', at http://www.guardian.co.uk/technology/2012/apr/10/instagram-myspace-social-startup-acquisitions?newsfeed=true (Accessed: 1 May 2012)

Barrett, D. (2007) 'Crime risk warnings to users of social networking sites' at http://www.independent.co.uk/news/uk/crime/crime-risk-warning-to-users-of-social-networking-sites-400062.html (Accessed: 1 May 2012)

BBC (2008) 'Man killed wife in Facebook row', at: http://news.bbc.co.uk/1/hi/7676285.stm (Accessed: 30 March 2012)

BBC (2010) 'Jealous lover jailed over London Facebook photo murder', at: http://news.bbc.co.uk/1/hi/england/london/8557402.stm (Accessed: 15 September 2011)

BBC (2010b) 'Fighting crime on Facebook', at: http://news.bbc.co.uk/1/hi/northern_ireland/8646428.stm (Accessed: 1 May 2012)

BBC (2011a) 'Warnings to Facebook users over personal data' at: http://www.bbc.co.uk/news/uk-wales-14988579 (Accessed 14th November 2011)

BBC (2011b) 'Study finds third of teachers have been bullied online' at: http://www.bbc.co.uk/news/technology-14527103 (Accessed 15 September 2011)

BBC (2012) 'Child sex offender jailed for Facebook approach to mother', at: http://www.bbc.co.uk/news/uk-england-sussex-17614922 (Accessed: 11 April 2012)

BBC Three, *Anti – Social Network*, 18 April 2012

Bryce, J. (2010) 'Online sexual exploitation of children and young people' in Jewkes, Y. and Yar, M (eds) *Handbook of Internet Crime*. Devon: Willan

Boyd, D. M. and Ellison, N. B. (2007) 'Social Network Sites: Definition, History, and Scholarship', *Journal of Computer-Mediated Communication*13 (1), pp. 210 - 230

Burcher, N. (2010) 'Facebook usage statistics by county – July 2010 compared to July 2009 and July 2008' at: http://www.nickburcher.com/2010/07/facebook-usage-statistics-by-country.html (Accessed: 1 May 2012)

Channel 4 News (2012) 'Five arrested in UK over online race-hate crimes', at: http://www.channel4.com/news/five-arrested-in-uk-over-online-race-hate-crimes (Accessed: 1 May 2012)

Coleman, C. and Moynihan, J. (1996) *Understanding crime data, Haunted by the dark figure*. Buckingham: Open University Press

Computer Misuse Act 1990, Chapter 18, at http://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed: 20 April 2012)

Dwyer, C., Hiltz, S.R. and Passerini K. (2007) 'Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace' in *Americas Conference on Information Systems*. Colorado: Association for Information Systems

Ellison, L. and Akdeniz, Y. (1998) 'Cyber-Stalking: the Regulation of Harassment on the Internet', *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the internet, pp.29-48

Ellison, N. B., Steinfield, C. and Lampe, C. (2007) 'The Benefits of Facebook "Friends": Social Capital and Collage Students' Use of Online Social Network Sites', *Journal of Computer-Mediated Communication* 12 (4), pp. 1143-1168

Facebook (2012) 'Key Facts', at: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (Accessed: 1 May 2012)

Fielding, N. and Thomas, H. (2008) 'Qualitative Interviewing' in Gilbert, N. (ed.) *Researching Social Life*, (3rd edition). London: Sage

Finch, E. (2001) *The Criminalisation of stalking: constructing the problem and evaluating the solution*. London: Cavendish

Finkle, J. (2009) 'Cybercrime spreads on Facebook', at: http://www.reuters.com/article/2009/06/29/us-facebook-security-analysis-idUSTRE55S55820090629 (Accessed: 1 May 2012)

Fraud Act 2006, Chapter 35, at http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf (Accessed: 20 April 2012)

Garland, D. (2008) 'On the concept of moral panic', *Crime Media Culture 2008 4:9,* at: http://cmc.sagepub.com/content/4/1/9.full.pdf+html (Accessed: 15 November 2011)

Gill, C. (2010) 'The Facebook crimewave hits 100,000 in the last five years', at: http://www.dailymail.co.uk/news/article-1338223/Facebook-crime-rises-540-cent-3-years-police-chiefs-16-forces-reveal.html#ixzz1syzp2kWk (Accessed: 24 April 2011)

Goode, A. and Ben-Yehuda, N. (1994), Moral Panics: The Social Construction of Deviance. Oxford: Blackwell Publishers

Green, R. A. (2011) 'British minister discusses Twitter, Facebook bans' at: http://edition.cnn.com/2011/TECH/social.media/08/25/uk.social.media/index.html?iref=allsearch (Accessed: 1 May 2012)

Harding, E. (2012) 'Trolls target cancer victim on Facebook: Sick comments about girl who inspired William and Kate' at: http://www.dailymail.co.uk/news/article-2136230/Vile-internet-trolls-target-Facebook-tribute-page-girl-touched-Prince-William-Kate.html?ITO=1490 (Accessed: 28 April 2012)

Holden, M. (2012) 'Student jailed for "extensive" Facebook hack', at: http://uk.reuters.com/article/2012/02/17/uk-britain-facebook-idUKTRE81G1MF20120217 (Accessed: 1 May 2012)

Home Office (2012) 'Launching the 101 non-emergency number: Information for police communicators', at: http://www.homeoffice.gov.uk/publications/police/101-non-emergency-resources/launch-toolkit?view=Binary (Accessed: 1 May 2012)

Jaishankar, K. (2008) 'Cyber Hate: Antisocial networking in the Internet', *Internet Journal of Cyber Criminology*, Vol.2 (2), pp.16-20

Jewkes, Y. (2002) 'Policing the Net: crime, regulations and surveillance in cyberspace' in Jewkes, Y. (ed), *Dot.cons. Crime, deviance and identity on the internet*. Devon: Willan

Joinson, A. N. (2008) ''Looking at', 'Looking up' or Keeping up with' People? Motives and Uses of Facebook', *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, at http://people.bath.ac.uk/aj266/pubs_pdf/1149-joinson.pdf (Accessed: 23 August 2011)

Joseph, J. (2002) 'Cyberstalking: an international perspective' in Jewkes, Y. (ed) *Dot.cons. Crime, deviance and identity on the internet*. Devon: Willan

Kraft, E. M. and Wang, J. (2009) 'Effectiveness of Cyber bullying Prevention Strategies: A study on students' perspectives', *International Journal of Cyber Criminology*. Vol.3 (2), pp.513 - 535

Maguire, M. (2007) 'Crime data and statistics' in Maguire, M., Morgan, R. and Reiner, R. (eds) *The oxford Handbook of Criminology* (4th edition). Oxford: Oxford University Press

Mail Online (2007) 'Millions of Facebook users putting themselves at risk of online crime', at http://www.dailymail.co.uk/sciencetech/article-476866/Millions-Facebook-users-putting-risk-online-crime.html (Accessed: 20 August 2011)

Mail Online (2011) 'Mother banned from the internet after pleading guilty to 'sexting' 16-year-old son's classmate naked pictures of herself', at: http://www.dailymail.co.uk/news/article-2061100/Lori-David-banned-internet-sexting-boy-16-naked-picture.html?ito=feeds-newsxml (Accessed: 14 November 2011)

Marcum, C. D., Higgins, G. E. and Ricketts, M. L. (2010) 'Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine active theory', *Deviant Behavior*, 31, pp. 381 - 410

Phillips, S. (2007) 'A brief history of Facebook', at: http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia (Accessed: 1 May 2012)

Roberts, L. (2008) 'Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking', *International Journal of Cyber Criminology*. Vol.2 (1), pp. 271 – 285

Russia Today (2011) 'Gang profiling: UK council wants eye on social network', at: http://rt.com/news/social-networks-youth-riots-461/ (Accessed: 14 November 2011)

Simons, J., Legg, C. and Hosking, R. (2003) 'National Crime Recording Standard (NCRS): an analysis of the impact on recorded crime', *Crime in England and Wales 2002/2003*. London: Home Office

Chase, E. and Statham, J. (2005) 'Commercial and Sexual Exploitation of Children and Young People in the UK – A Review', *Child Abuse Review*, Vol. 14, at: http://onlinelibrary.wiley.com/doi/10.1002/car.881/pdf (Accessed: 1 May 2012)

The Crown Prosecution Service, (n.d.) 'Stalking and Harassment' at http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/ (Accessed: 1 May 2012)

The Independent (2008) 'Man murdered wife over Facebook posting', at: http://www.independent.co.uk/news/uk/crime/man-murdered-wife-over-facebook-posting-965056.html (Accessed: 23 August 2011)

The Sun (2012) 'Web trolls put picture of Down's girl on Facebook with vile caption' at http://www.thesun.co.uk/sol/homepage/news/4278427/Web-trolls-put-picture-of-Downs-Syndrome-girl-on-Facebook-with-vile-caption.html (Accessed: 30 April 2012)

Travis, J. (2011) 'Teenager faces jail after he admits flooding library', at: http://www.portsmouth.co.uk/news/local/teenager-faces-jail-after-he-admits-flooding-library-1-2616198 (Accessed: 30 April 2012)

Trochim, W. M. K. (2001) *The research Methods Knowledge Base* (2nd edition). Cincinnati: Atomic Dog Publishing

Wall, D. S. (2005) 'The Internet as a Conduit for Criminals' in Pattavina, A. (ed) *Information Technology and the Criminal Justice System*. California: Sage (Chapter revised March 2010)

Wall, D. S. (2007) Cybercrime: The transformation of crime in the information age, Cambridge: Polity

Wall, D. S. (2010) 'Criminalising cyberspace: the rise of the internet as a 'crime problem'' in Jewkes, Y. and Yar, M. (eds) *Handbook of Internet Crime*. Devon: Willan

Williams, C. (2012) 'Facebook criticised for 'hurting' cybercrime investigation', at: http://www.telegraph.co.uk/technology/facebook/9068166/Facebook-criticised-for-hurting-cybercrime-investigation.html (Accessed: 1 May 2012)

Yar, M. (2006) *Cybercrime and Society*. London: Sage

Yar, M. (2010) ‘Public perceptions and public opinions about Internet crime’ in Jewkes, Y. and Yar, M. (eds) *Handbook of Internet Crime*. Devon: Willan

Yar, M. (2011) *A New Age of Hackers.* Readings: PCTools

Yar, M. ‘E-Crime 2.0: The Criminological Landscape of New Social Media’, *Information Communication Technology Law*. Forthcoming 2012