‘www.how-to-be-a-better-burglar.com’

An exploratory study of online burglary guides.

By Matthew Durrant[1]

Abstract

The Internet was originally designed to provide a means of information sharing, universal networking and communication in which it has excelled. However, the unforeseen costs of the globalization of a freely accessible environment that lacks any kind of appropriate formal control has eventually succumb to those who wish to exploit its relative vulnerability and naivety as a secure community. One example of this vulnerability is the ability people from all over the world are afforded to disclose information which may prove to be harmful to others. Some well documented examples of this we have seen in recent times are online terrorist representation and the disclosure of information such as that on bomb making, the use of the Internet by white racialist groups, pages which are perceived to promote anorexia and websites which provide information on and encourage suicide.

[1] This dissertation was submitted in part-fulfilment of the degree of Bachelor of Arts (Honours) Criminology at Nottingham Trent University

Introduction

This study examines the ways in which the Internet is used as a means of information sharing and disclosure which relate to how to commit burglary more effectively and whether the techniques shared are likely to provoke copycat behaviour in the offline world. In order to gain an understanding or the accessibility and availability of relevant information online to the 'curious surfer' (Sutton, 2007), this study includes findings from an online empirical study which attempts to replicate the behaviour of such Internet users.

It is the aim of this chapter to explore the genuine potential for serious harm and how easy it is to find potentially harmful materials online by entering burglary related terms into the popular Internet search tools, Google and YouTube. Discussions will also take place regarding the possible motivations behind those who choose to disclose this sort of online information. Finally, this study provides a number of recommendations for the future which could facilitate reducing the damage this information is causing and make it less accessible to Internet users worldwide.

Literature Review

One of the most widely recognised and commentated upon problems regarding the Internet is that it is still a relatively new phenomenon and for this reason, it remains somewhat under researched. Many loopholes exist within the law regarding the Internet which can afford people the ability to offend in cyberspace in ways that would not be possible in the offline world. By utilising such loopholes, people are able to offend in ways that are beyond the reach of law enforcement agencies (Grabosky et al, 2001). The issue this research will address however is not one of crime, rather one of "harms" seeing as the problem of information disclosure currently has no reference point in law (*ibid.*). Beyond the plethora of terrorist-type "cookbooks" etc., not very much literature, if any, focuses directly upon the issue of the Internet as a source of knowledge for general offending techniques. This is one reason why the Internet is currently so under policed and is an area in which little formal regulation takes place.

Due to the growing dangers that are becoming apparent that it is presenting to society, the Internet has increasingly become recognised as an area in desperate need of study. However, studies that have been conducted tend to concentrate almost exclusively upon the direct harms that can be caused as opposed to the ways in which risk can be increased which becomes apparent during a brief review of the contents of almost any published literature on Internet crime. For example David Wall, a leading author on the subject of Internet crime, highlights four main areas of concern; 'cybertheft', 'cyberobscenity', 'cybertresspass' and 'cyberviolence' (Wall, 2001). All of these areas involve crimes that are committed online, and tend also to create victims online. This inability of criminological studies of the Internet to account for the link between the online and the offline world was drawn upon by Franko (2007) who attempts to explain the omission;

> The relevant reluctance of criminologists to incorporate the subject of cyber life into their research and writing may partly stem from some central theoretical dualisms and binary oppositions between beings and things, and technology and society, which define the conceptual apparatus of criminology (Franko, 2007 in Jewkes, 2007, p. 162).

Here, Franko (2007) suggests that criminologists are still having difficulty defining the Internet and incorporating it into our everyday traditional ways of thinking and theorising. This is partly due to the fact that we are still in a relatively early stage with regards to our learning and understanding of the capabilities of the Internet and where the dangers lie, but is mainly due to

the entirely different, seemingly lawless environment it has created which has come all at once and is accessible globally.

So what *does* the research tell us about the Internet?

Commentators in the past have purported that the use of the Net for facilitating crimes has been merely another moral panic of the kind described by Cohen (1980) (Sutton, 2007), only this time related to Internet activity. More recent, tragic events such as the Brick Lane Bombings and the terrorist attacks of 11/09/2001 and 07/07/2005 have directly challenged these views. Arguably, before these events, the link between online and offline activity was not taken seriously by academics, policy makers and law enforcement which resulted in harmful information about how to join terrorist groups, how to make bombs, and other unrelated damaging issues such as how to commit suicide and how to buy guns being freely available to anyone in the world who wished to view it. Of these, only the bomb making sites and the terrorist representation on the Internet have been made illegal and such sites have been closed down, or at least made harder to find.

Policy makers have noted the dangers that technology such as the Internet can pose to society and the ways it can provide a "breeding-ground" for terrorism ideals. The Terrorism Act 2006 made provisions for the 'distribution or circulation of a terrorist publication' (s. 2(2)[b] Terrorism Act 2006). S. 2(2)[d] made it an offence to 'provide a service to others that enables them to obtain, read, listen to or look at such a publication' and 2(2)[e] states that a person engages in conduct failing with this subsection if he 'transmits the contents of such a publication electronically' (Office of Public Sector Information, 2008). Here we see clear signs of the recognition of high tech crime possibilities regarding terrorism and the Internet yet the remaining aforementioned issues continue to be accessible to Internet users despite having caused damage in the real world. For example, 'the teenage boys who carried out the Columbine Massacre killings in a USA high school, were said to have found support and information on the WWW' (Sutton, 2007, p. 31). Although the online/offline link is beginning to be taken more seriously in some cases such as terrorism, it seems to be doing so too slowly and the issue explored by this research is merely another example of the dangers this link can cause that has not yet been recognised by policy makers.

Another important issue that requires focus is that of offender motivation. In order to discover why it is that people wish to share information about burglary techniques possible answers can be found in the literature which discusses the motivations behind the crime of hacking, for which Sutton (2008) described a 6-fold typology. Of these, the ones which could apply to those who disclose burglary techniques and seek out such information are the urge for curiosity, enjoyment of feelings of power and peer recognition (Sutton, 2008). Although no literature explored has yet attributed these specifically to this research focus, they could all be offered as explanations and this research will attempt to add validity to this theory during the analysis of data stages.

It is also important to look at the issues regarding the Internet in general and the problems its unique nature poses for crime prevention, crime reduction, and law enforcement. One of the main issues was illustrated by Jewkes (2007) during a review of other harmful content on the Internet, 'Although these sites contravene the obscene publications act 1959, the UK authorities have no powers to shut them down because they are hosted by service providers in other countries' (Jewkes, 2007, p. 4). This limitation of law enforcement is a common problem with many online crimes and there exists no obvious way around it. It seems impossible (or at least a very long way off) that in the future we will have a law that all Internet users worldwide have to abide by due to the fact that 'a congruence of values across international boundaries exists only infrequently' (Grabosky and Smith, 2001, p. 38). This concern is relevant to this research because it may be offered as a reason why harmful information sharing is allowed to continue, or

at least why it has not yet been regulated. Before successful eradication of harmful content on the Internet worldwide is achieved, UN style international agreement is necessary which occurs far too infrequently for notable progress to be made.

One of the aims of this study is to identify the difficulties we face in controlling content on the Internet and express a need to establish tighter security. Various other limitations to this goal have been highlighted by the literature including the debates over who should be responsible for regulating the Internet and its content (Grabosky et al, 2001), inconsistencies in laws from one jurisdiction to another (Wall, 2001), and the anonymity that can be adopted while using the Internet (Denning, 1999). Perhaps the most relevant of these issues is the current legality of my main research focus; the fact that disclosure of information about how to commit burglary more effectively, and learning these disclosed techniques is not illegal as long as a disclaimer or illegality warning is provided by the source in some form. This poses political questions in that perhaps we should be looking to deal with these issues at an earlier stage than simply dealing with them once they have resulted in tragic or irreversible consequences in the real world. This issue will be discussed further in the discussion chapters of this study.

Literature from other areas of criminology can also be used to aid understanding of this issue such as that which explores the reasons why people offend or why they seek out such information, such as rational choice theory (RCT). Central to this theory is the nostrum that crime is an outcome of the opportunity to offend (Hopkins-Burke, 2005). In relation to the issue of this study, this theory would suppose that the key to reducing the damage caused by this problem is in removing the availability of the information before it motivates a rational actor to replicate it which will, in turn, reduce the incidence of burglary. The problem confronted by this theory when relating it to the central concern of this study is that unless the information was neither found accidentally, nor the casual surfer was directed towards it by another user or website, a person generally needs to be motivated (i.e. they want to seek out such information) *before* they become aware of the opportunity (i.e. the existence of such information) as it generally requires an active search to be conducted. In other words, it is probable that this theory is only attributable to the minority of cases in which this information has been viewed and used.

It therefore becomes necessary to consider the rational actor model (RAM). The contentions of this theory argue that it is the threat of a fair and proportionate punishment that can deter the 'rationally calculating, reasoning human being' (Hopkins-Burke, 2005, p. 48). The limitations outlined above, regarding the lack of congruence in values across international boundaries and the inconsistencies in laws binding Internet users globally (see Grabosky et al., 2001; Wall, 2001, above), is the reason why RAM would suggest such websites are prevailing and why people are allowed to continue to seek out such information. They are not being prevented from doing so by an adequate threat of punishment. A common criticism of this theory on the other hand exists in it's relatively naïve presumption that all those involved are rationally calculating human beings. The reality is that not all human beings are equal or function in the same way, and to assume that all those involved are rationally calculating or even aware of the lack of punishment regarding their actions is farfetched. While RCT advocates too little acclaim to the idea of the rational thinking human being, RAM appears to do so too much for what is realistic in the case of this research.

Routine activities theory (RAT) is another helpful theory which warrants noting in this context. The theory is based upon the proposal that for a crime to occur there must be in existence at the same time and place a motivated offender, a suitable target and an absence of capable guardianship (Cohen and Felson, 1979). Attributing the contentions of this theory to online crime is more complicated as it involves the removal of the concept of the need for a congruence of

place and time in the same form as the theory was originally designed for. The Internet however, arguably provides the place and time in a new form where people can virtually be in the same place at the same time, while they may physically be on opposite sides of the world. The relevance of this theory to this research exists in the third of the three necessary components, the absence of capable guardianship. As aforementioned, (see Grabosky et al, 2001, above), this is a common characteristic of the online world which is why the theory could also be helpful in explaining the prevalence of online crime. This issue will be addressed after the data collection stages where its value can be properly assessed.

Methodology

Due to the insufficient research which endeavors to answer the same questions as those addressed in this study, it was decided that primary research was the most appropriate method due to the apparent strengths that are often associated with its use. Seeing as there is such a diminutive volume of empirical work that has been conducted on this issue, the only way to gain an accurate picture of social reality was by conducting research first hand which can provide a more up to date picture of the issue at hand and will increase the authenticity of the results (Bryman, 2004). It can allow the aim of the research to be directly addressed (Bryman, 2004), and considering the area is such an under researched issue it can make an original contribution to knowledge (Bryman, 2004). This could then be used in the future as a base from which to conduct further research on the issue in a more detailed and thorough manner than this researcher had the resources to achieve.

Considering the primary objective of this research was to investigate the extent, type and availability of information that is being viewed and used online, the researcher attempted to replicate similar behavioural patterns to those of the curious surfer. It has been noted that the problem with such a method of data collection is that 'we do not know enough about how young people use the Internet' (Sutton, 2007, p. 35). Such a hindrance could have also played an influential role in this case due to the differences between the author of this study and those whose behaviour it was attempting to replicate. These differences are unclear without further research into the issue than is possible in this case yet one possible such example could be that many of the people who seek out this information may have become accustomed to criminal terms and techniques if they have past experience with burglary. This knowledge would inevitably affect their ability to navigate through useful and unhelpful sources. The author himself, being from a small, middle class town in the South East of England, has encountered the crime of burglary far less than many and is likely to be far less experienced with the terms than many of those whose behaviour the research is attempting to replicate.

In order to balance up this divide it was necessary to conduct a small amount of research on the issue before the main exploratory research was conducted in order to gain a more realistic understanding of the relevant issues. This helped the author formulate a list of the search terms which were used during the main primary data collection stages. From this prior-research, it was decided that the terminology used in the searches would consist of the words "burglary", "burglary tools", "break in to a house", "vibrating lockpick", "lock-picking kit", and "bump keys" being entered into both Google and YouTube both singly and in random groupings with the terms "how to use", "buy" and "how to commit" proceeding them. It is important here to add a note regarding this term, "bump keys". Bump keys are keys that are cut in a certain way so as to enable the owner (as a result of the technique commonly referred to as "bumping") to open almost any "Yale" or "Chubb" lock (most notably the kind commonly used on front doors of

houses). The technique appears to be very successful and can be said to appeal to burglars as it leaves very few signs of forced entry.

During the data collection phases of research, it was decided that there were various guidelines which needed to be observed in order to maximise the probability that the research was replicating the behaviour of the curious surfer as much as possible. For example, the list of terms that was devised were entered systematically into Google and YouTube as it was decided that these two would maximise the range of data which was collected whilst preventing data from being used in the study that was located through a less commonly used source. Seeing as information disclosure on the techniques of burglary and supply of burglary tools can be in the forms of websites, videos or products which are being sold, the use of these two databases to search for information gave a suitably comprehensive range. The research method consisted of spending two time periods of two hours each, entering the random groupings of terminology into the popular search engines. Anything found within each of those two hour sessions deemed by the researcher to be relevant to the study was noted and recorded for later analysis. It was decided that the time period of two hours spent researching issues such as this 'represents a reasonably significant, but not too highly motivated, effort to find material on a particular subject' (Sutton, 2007, p. 26). Failure to do this would have decreased the probability that the research was addressing the same material as the curious surfer and therefore decrease the validity and replicability of any of the results that were found.

One of the early criticisms to note of this study is that the data collection phases required a great deal of personal discretion on the researcher's behalf when deciding which terms to enter, which sources to consider relevant, how to interpret the information and which internal links to follow. This seems unavoidable however due to the lack of resources available to the researcher and the consequential lack of a realistic ability to conduct prior research into online behaviour which would have undoubtedly helped focus research. This negative effect was minimised in various ways by ensuring certain practices were observed during the data collection period. Examples of this included ensuring that not too many internal links were followed and by only using results which appeared in the first few pages of each search which was launched. Following these simple precautions ensured that the behaviour of the curious surfer was being replicated more accurately and the likelihood that the same information is being viewed was increased. However, following these precautions could have compromised the richness of the information that was studied by reducing the size of the pool of information that was being viewed. After consideration of these associated strengths and weaknesses, it was decided that the precautions were to be observed due to the priority of the research being to study the range of information which is being *used* as a source of information and tutorage as opposed to the range of information which is *available* but is possibly not being used as extensively to ensure that behaviour was replicated as much as possible. This was decided to be imperative, at the expense of the possibility of studying a wider range of information.

Results

The first stage of research was conducted on the 3rd January 2008. During the first hour of research an abundance of relevant data was located after the search term "lock picking kit" was entered into Google. On the first page of 233, 000 results, the first (ukbumpkeys.com/lockpicks), second (topsecretmagic.co.uk/lockpicks), and sixth (lockpickshop.com) results provided links to websites which sold guides on how to use lock picks, sold lock picking kits themselves, offered and sold tutorial videos, sold practice locks and a also sold a variety of other tools and products designed to break or pick a range of different designs of lock. Two out of three of these particular

websites also provided forums in which discussions could take place between customers. All three of the websites appeared to cater for the "beginner" as specialist beginner sets were also sold (ukbumpkeys.com/lockpicks), books, video guides and practice locks were available (lockpickshop.com). The amount of users each website had, or the number of "hits" each received was unclear from this level of research but one of the websites, (ukbumpkeys.com/lockpicks), had 844 registered users. This gives an indication as to the extent of custom the website receives and the popularity of the discussion forum which contained over 20, 000 posts offering mechanical support and discussions regarding how to get the most out of the products which were being sold by the website.

Despite the fact that two of the three websites in question recommended that their products should be purchased for professional use only and to those over the age of 18 (ukbumpkeys.com/lockpicks and lockpickshop.com), neither of these websites requested any proof of profession or even age before the purchase of a product was authorised. The final observation to note regarding these three websites is that although no explicit evidence was apparent that the information was being used for illegal purposes, it was certainly being practiced in the offline world, 'Cheers UK bump keys it finally makes sense, I've done four locks today and I'm totally freaked out, what a product!', (feedback left by one customer who purchased a "BMW/Peugeot inner groove pick", a lock pick specifically designed to aid entry to BMW and Peugeot vehicles) (ukbumpkeys.com/lockpicks). Although no explicit illegality is mentioned here, it seems unlikely to the researcher that this particular customer owns four BMW's or Peugeots themselves.

For the next 20 minutes, results were studied that were produced after entering the search terms "lock picking kits" and "lock picking sets" into the YouTube database. The vast majority of the results were video tutorials demonstrating how to use lock picks and explaining the various kinds of lock picks available. The videos on YouTube are free to view, can be viewed by anyone of any age and do not contain warnings regarding using the techniques shown for illegal purposes. No proof of profession is required to view the videos and there is space for comments to be left below questioning or discussing the techniques shown. A handful of the videos appear to be promoting their business throughout, presumably in order to increase custom and product awareness (e.g. the video "new lock picking kit" (14/08/2007) frequently advertises the website "www.lockpicks.com" throughout the demonstration). The amount of views that the videos have received reveal worryingly high numbers. To name a few examples the first three results of the search term "lock picking kits" revealed that the first result, "new lockpicking kit" (14/08/2007) had been viewed 1, 248 times, the second result, "lock picking a padlock" (20/03/2007) had been viewed 497 times, and the third result, "learn how to pick combination master lock" (02/11/2007) had been viewed over 12, 000 times. There was no evidence to suggest that viewers of any of the videos studied had practiced the techniques shown for illegal purposes yet there were numerous comments left by people offering praise for the skill required for each and enquiring about the specifics of some of the details that were not made entirely clear by the video, which suggests that they are being practiced.

There were 26 results displayed after the search term "burglary tools" was entered into the YouTube database. The 12th result displayed was a video called "20 second real cylinder lock picking" (27/10/2006) and was a similar tutorial video to those described above. This particular video had been viewed 2, 320 times and was of particular interest because of the search term it was locatable by. This was the only source of relevant information (both on Google and YouTube) which was locatable using the explicitly open term "burglary" in the search term which immediately implies illegal purpose.

There also exists an abundance of information on the YouTube website after entry of the term "how to break into a house" which was studied in the research for the next 70 minutes. Although this term does not specifically imply illegal purpose, the information that was found can of course be used for such a purpose. From 1, 160 results available, many more tutorials were available demonstrating how to pick locks, more specifically those which can gain entry to a house. Although some of these videos provide legality warnings, the majority of these take the form of diminishment of responsibility. For example, the comment 'now everyone can be a criminal', which was left as a response to the video "paperclip door lock picking" (14/08/2007), rendered the response 'yes, if you want, but like it says in the video, I'm not held responsible' by the creator of the tutorial. This particular video had received over 40, 000 views which seemed to be an average amount for many of the videos located in this category. One video located, ("how to pick locks (the beginners guide)", 04/09/2006), had received over 150, 000 views at the time research was conducted.

One of the most controversial sources of information found was located after the search "vibrating lockpick" was entered into the Google search engine. The webpage ("inventgeek.com", 01/06/2006) appeared to be very popular and widely viewed as not only was it one of the first results displayed by Google, but the next 15 results were websites either advertising this contraption, discussing it, or providing links to it. The page contained a guide of how to create a vibrating lockpick using household objects. The reason why this contraption is so controversial is because is cannot claim to be designed for use by professionals as it shows people how to make the contraption using an electric toothbrush and is given a difficulty rating of "novice". The author of this guide gave details of how to build the device, how much it will cost and which materials will be needed.

The final two hour session of research was spent entering the search terms "bump keys", "how to use bump keys", "how to make bump keys" and "buy bump keys" into both Google and YouTube. Many sources were found during these two hours were similar to the websites and tutorials discussed located with entry of the other search terms discussed above. Amongst only the first page of approximately 644, 000 results for the term "buy bump keys", were numerous websites which sold, promoted, contained advice, offered forums and provided tutorials for how to use bump keys. A similar volume of results were achieved with the remaining search terms used in these two hours. Many of the websites amongst these which were viewed by the researcher gave similar warnings regarding the use of their products and information for illegal purposes, yet all categorically failed to acquire any form of proof of age or profession when the researcher attempted to purchase any of the products that were on offer. The term "how to use bump keys" entered into YouTube produced 46 video tutorials, again, showing how to use the tool to break into locks using the "bumping" technique. Similar issues of note were found with all of the results of these search entries to those of the lockpick results discussed above.

Analysis of Data.

Of all the various search terms entered during the data collection phases of this research, a distinct divide in the volume of content which was located became apparent. There were many sources of information, (predominately websites or videos), that were easy to find after the search terms for various techniques for lockpicking or types of lockpicking devices were entered, such as "how to use bump keys" or "vibrating lockpick" for example. Perhaps unsurprisingly, the search terms which were not so successful were those which contained the word "burglary" in them such as "how to commit burglary" and "burglary tools". This is despite the fact that whilst the former may not insinuate or specify illegal purpose, they are essentially examples of the latter.

This seems to suggest that many of the people who have created and chosen to share the material this study has observed are happy to continue to do so in full knowledge of what it may be and in all likelihood predominately is being used for. While on many occasions the disseminators offer a warning against illegal use of the information, the question arises of why they do this; is it because they genuinely don't want this information used for illegal purposes? Or is it because they wish to cover their own backs and deflect any blame for illegal use of the information away from themselves?

The vast majority of the material found online was either explicitly designed for, or suitable for use by the "beginner", or "novice". For example, the majority of websites that constituted the first few pages of the results page of a Google search under "vibrating lockpick", contained links to the same website (inventgeek.com). Despite numerous voiced concerns from various viewers of this information regarding what it may be used for, the author of this particular guide justified his actions by claiming that it is for security purposes, or for use by professionals only, 'I do not condone anything nefarious or criminal in nature ever' (Final thoughts, inventgeek.com, 2006). It is possible to infer from such a reply that this is not in fact entirely true because why a professional would use such a device, and how it could be used to protect oneself are highly questionable. It can only be derived that the author in this case is motivated to disseminate the information for personal gain, (i.e. perhaps the 'enjoyment of feelings of power', or for 'peer recognition' motivations (see Sutton, 2008 above)), or that he simply doesn't care what it is used for.

It became evident during data collection that both of the enjoyment of feelings of power and peer recognition typologies may explain motivation in many cases due to the fact that the majority of the facilitators identified themselves in some way whether via a pseudonym or by disclosing their real name. Having said this, of those who choose only to adopt a pseudonym it is important to point out that they may have had no choice but to do so in order to become a member of the website in the first place (e.g. as is necessary for membership of the website www.youtube.com). For this reason it could be misleading to include such examples amongst those who may be choosing to disseminate information for the aforementioned motivations, as pseudonyms alone are not instantly recognisable to those who are not established members or frequent visitors of these particular websites.

What could be argued, however, is that these motivations could apply to those who choose to only go by a pseudonym in the online world as the credit, recognition, respect, power or heroism that they may receive becomes attributed to their online equivalent, or their alternate online persona - their pseudonym. The same rewards can be experienced by this pseudonym so long as they exist in a community amongst which other Internet users have become familiar with their pseudonym. Others will learn to associate certain actions, behaviours, traits, characteristics and personalities with them in much the same way as we do in the real world with the names and faces of those around us. Only in this sort of environment could such a motivation account for this form of information dissemination due to the fact that websites which do not possess such a community, where viewers can come and go and access the information anonymously, for free and without any sort of membership requirement, the discloser of the information will not receive the same credit and association as they would in these online familiar communities.

It was found during the research stages that amongst many YouTube users there exists certain "regulars" who have numerous videos on certain subjects. For example, whilst searching for videos under the term "how to break into a house" the researcher came across a group of videos which had been uploaded in competition with each other. This competition appeared to have begun with a video which demonstrated a method of picking the front door of a house using only

a paper clip by the user ("Miles shows us how to break into a house!", 15/10/2006). The method shown was subjected to heavy criticism by other members each claiming that they knew a more effective method of breaking into a house. This instigated a series of around 8 videos being uploaded by a handful of different users who each demonstrate how to commit this act more effectively than that demonstrated in the previous video. This is an example of such a community where users have familiarised themselves with each other, by pseudonym only, and have learnt to associate each other with actions and ideas they had portrayed in their videos without even knowing their offline personas. As a result of this particular series of videos, a hierarchy was formed amongst the members of this small guild which was determined by ones level of knowledge of how best to break into a house. Apart from the obvious implications this kind of published material can have on impressionable viewers and wider society, it is also possible for the motivations mentioned above to play a significant role despite the fact that potential rewards of fame, heroism, credit and respect that may result may only be attributed entirely to a fictional, representation of oneself. This can have the same positive reinforcement effects on someone's online equivalent (their pseudonym) in the online world, as it can have on someone in the offline world if those same rewards were given to someone who had disclosed their real name or address. If this kind of reinforcement is in fact what is being sought by this group then they can quite clearly be categorised under the typologies discussed by Sutton (2008).

Of the websites and sources studied, approximately one third of the authors found on the Google searches had no reservations about either using their real name or even making their address or contact details readily available. Assessing the possible motivations behind acts such as this are more straightforward. What can be said about these cases with a certain degree of confidence is that either they are operating with the motivations in mind outlined above, or they simply see no wrong doing in their actions and show a similar disrespect for any criminal consequences that may occur to that of the author of the example described above. One example to demonstrate that this particular type of dissemination may be for the two motivations outlined above exists firstly in the fact that they allow their name and contact details to be accessible, and secondly in the amount of pride some of them take in their contribution. For example, a response to the vibrating lockpick guide discussed above read 'I'd like to get mine working again just to show off, but I'm also working on a new pick with a motor that can handle nine volts.' (Makezine.com, 11/01/2006). Here exists a blatant example of someone seeking the credit, recognition, heroism, fame or power amongst their peers for what they claim they are able to achieve. They are attempting to climb a similar hierarchy of knowledge and power to the one mentioned above, yet this time they disclose their real name which renders the need for an online familiar community less necessary, yet at the same the basic principles of motivation apply.

Another typology that these disseminators can be categorized amongst are those who act as they do with financial gain as their primary objective. This category requires either of the two belief systems outlined in the previous paragraph, or another belief that they are aware of the moral boundaries they may be crossing, they know of the dangers it may pose to certain areas of society yet they consider the possibility of it directly effecting themselves to be very small and therefore the potential rewards of financial gain outweigh the threat of legitimate punishment. It became apparent from the research that a fairly large portion of the websites which include material relevent to this study do so for financial gain which can take many different forms. The ways in which money is being made by these websites can be through advertising or by selling products. Of the 35 (approx.) websites which were studied from searches entered into the Google database, approximately 65% of them contained advertising of some form (for which the question of whether or not they receive additional funding for this remained unclear) and the vast majority of them sold products on their website designed for lockpicking. While the majority, (21 of approximately 35), of these websites were keen to stress that they were designed specifically for

professional locksmiths and that their products were not designed to be used for illegal purpose, merely 3 of the websites which were located required the buyer to be over the age of 18 *or* requested proof that they were a professional locksmith before the "enter payment deatails" phase of making a purchase was achievable. This negligence portrays a clear message that although these particular websites may be keen to deflect any incurring blame away from themselves, profit ultimately takes priority over community safety and consideration for who is actually purchasing their products. Seeing as these websites represented such a large majority it seems crime prevention, law enforcement agencies and policy makers need to take a far more active role in issues such as this.

Discussion

As aforementioned in the literature review, there are many characteristics of the Internet which have resulted in the creation of a "place" which is severely under regulated which results in many examples of crime and deviance being able to flourish and prevail. One of the most damaging of these characteristics is the global reach the Internet affords people the ability to achieve. If the issue is examined from the perspective of those who view this information online, this global reach has many advantages and attractive qualities. The first of these is that the Internet offers a way of connecting people together who share the same dangerous and harmful ideologies and views in a way which cannot be achieved with the same amount of ease in the offline world. For example if you want to have underage sex, commit cannibalism or learn how to make bombs the chances are that somewhere on the Internet exist like-minded individuals who will share your thoughts, a far higher chance than the resources such an individual is confined to in the offline world. It has been suggested (Jewkes, 2007) that individuals 'might be drawn to the Internet to facilitate their desires, particularly if their behaviour receives support from communities of other people who are sympathetic to their thoughts, values and behaviour' (Jewkes, 2007, p. 5). Surrounded by similar people who share these deviant values or thoughts, there exists a very real danger that individuals are going to become accustomed to believe that they are equally as socially acceptable in "meatspace" (Pease, 2001) as it is in this close knit online community. Familiarisation with unlawful behaviour can occur in these communities as they are only receiving praise, recognition, support and justification with few negatives to rebalance their morals.

Another effect this can have is that the availability of such information allows these individuals to share and improve each others knowledge and skills at committing crimes to become more effective and successful. This effect is similar to the way many criminologists and politicians have for decades been referring to prison as being a closed university of crime within which criminals can learn not only how to improve their current skills, but can also learn new techniques of committing crime (Cavadino and Dignan, 2002). From this perspective, the Internet too can be viewed as a place where dangerous like-minded individuals can meet and share information which can have the same, if not more, harmful effects on society. In other words the Internet can be seen as an open university of crime upon which damaging information is being disclosed, yet this time it is being circulated amongst free innocent people of all ages from anywhere in the world and is no longer being confined merely to the walls of a prison or to ones immediate surrounding offline community.

The Internet is a tool which can empower small agents the ability to act in ways which, before the turn of the Internet, only knowledgeable experts were able to. To relate this to the issue at hand, anyone can obtain the necessary skills required to pick locks or commit burglary by using search engines on the Internet to locate tutorage on how to do so. Added to this is the fact that the

Internet also possesses the bonus incentives of eliminating the majority of the deterrents that would usually exist in the offline world, such as a suitable form of law enforcement and legal intervention, surveillance, identity and public retribution (Jewkes, 2002).

An issue which will remain debatable and relatively unanswerable after this level of research is just how much of an influence this sort of information and spending time in these online environments will have on the behaviour of people in the offline world. The answer to this issue will inevitably vary depending on the susceptibility of every person who is exposed to it. The question must be asked of whether, after viewing this type of information online, these people are going to be more likely to replicate these methods themselves in an illegal manner? Jewkes (2007) suggested that this is perhaps not necessarily the case, 'Like wider debates about the effects of harmful media content, much mediated public discourse about computer-related crime is underpinned by a strong technological determinism (that is, overstating the power of the Internet and underplaying the importance of the individual actor)' (Jewkes, 2007, p. 5). Here, Jewkes warns of the dangers of ignoring the Rational Actor Model (RAM) with regards to computer-related crime. Although after consideration of the contentions of this theory and relating them to the issue at hand, we can purport that the perceived risks could be considered to be lower by many due to the apparent absence of capable guardianship which exists online, although this of course depends on the subjects awareness to this fact. We can also suppose that the perceived risks may be lower due to the effect that this information may have on someone viewing it as it may enable them to become better at committing burglary, or at least increase their confidence to this conception, and they will therefore view the risk of them being caught as far lower. Bjorgo's (1993) research, which was based upon interviews with perpetrators of racist violence, reached the following conclusion:

> It often seems that journalists believe, with the best of intentions, that the extreme opinions of confirmed racists will reveal their nasty faces and have a deterrent effect upon readers. Although this may be the effect on most readers, there is also a small section who may find such extreme and taboo-breaking views exciting and attractive. This is the small group the extremist groups are seeking to reach (Bjorgo, 1993, in Sutton, 2007, p. 34).

The fact that here Bjorgo (1993) is obviously discussing a far more extreme issue than that of this research speaks volumes. If such a conclusion is reached regarding such a serious crime, can't we logically assume that this 'small section' of impressionable readers is going to be far larger for a seemingly less serious and "taboo-breaking" issue? It is likely that the readers and viewers of information online regarding burglary techniques are going to be far more impressionable and easily persuaded than those researching far right views on the Internet for example, due to the fact that they are breaking far fewer social norms and taboos by doing so which could play a major role during the process of weighing up the risks and the rewards discussed by RAM. Jewkes (2002) highlighted her concern for this point, 'if the moral, ethical and legal boundaries that usually constrain our behaviour are indistinct or unenforceable in the virtual world, what forms of regulation exist to define and curb 'excesses' of behaviour? Is it a case that 'anything goes' in cyberspace?' (Jewkes, 2002, p. 15).

Essentially, the issue that is being explored by this research is the online, or virtual equivalent of simply discussing with another person in the offline world how to commit burglary which is of course by no means illegal. Seeing as the act of discussing such techniques of committing illegal acts is legal and one must assume that it is done so frequently in the offline world, the question remains of why it is that essentially the same act occurring on the Internet presents so much more of a danger to society? As mentioned above, one of the main problems that this evokes is the scale and scope of the people who can view the information, or who can discuss it in this virtual

world. The global reach the Internet affords people the ability to achieve results in the online equivalent of something that seems relatively harmless and unavoidable being potentially a lot more dangerous as it increases the frequency of these "discussions" taking place. Another characteristic of the Internet that has allowed this information to flourish is found in the accessibility of knowledge has been made far greater and is no longer restricted to surrounding communities because through search engines such as Google and YouTube, the Internet has provided disseminators the ability to publish information that ordinarily would not be allowed, by bookshops for example. This is mainly due to the infringement of civil liberties that limiting freedom of speech will have on those who wish to disclose information. The 'hackers ethic', outlined by Levy (1984) (Newman and Clarke, 2003, p. 71) describes one of the central belief systems that hackers live by being that all information should be freely accessible by anyone. Freedom to voice opinion, and for that opinion to be heard is central to the beauty and attractiveness of the Internet for many users and any attempts to eradicate this by authorities (who are mistrusted by the 'hackers ethic') compromises individuals' civil liberties.

Cyber-governance of damaging information online, which can create victims offline, is increasingly becoming recognised as problematic. Websites which disclose information on how to commit suicide and those which promote illnesses such as anorexia are two examples which have highlighted the damage that the availability of online information can cause to victims in the offline world. In terms of Internet crime, this delicate issue has until recently existed relatively unchallenged seeing as essentially, the issue of information sharing is not an illegal act. Extensive media coverage of these particular issues has served the purpose of highlighting the need for legislation to be brought in which would force Internet Service Providers (ISP's) to withdraw such websites from the Internet. This kind of threat to the offline world has existed for as long as the Internet has, yet before now it has been viewed more as an issue to do with the prevalence of anorexia and suicide as offline, psychological and societal issues which of course they are, yet tackling the source of such information has never before been viewed as being a possible way forward. Only recently after this extensive media coverage and the subsequent creation of a 'moral panic' (Cohen, 1980) has it been considered as an online issue for which the Internet is to blame.

As mentioned earlier, the Internet has created a world in which anyone can join a community and discuss issues free from the moral, ethical and legal boundaries that otherwise exist in conventional society, where like-minded individuals can encourage and sympathise, and "taboo" issues are considered less so. There exists very little research which addresses the issue of the online/offline link in this way but this seems to represent a shift in belief systems that blames the Internet, as a source of information, as one of the main problems because it is becoming increasingly understood that this is in fact an online issue. With the subject of this research in mind however, this remains more questionable. For example, we view terrorism to be an offline issue despite the fact that the techniques adopted may have been entirely learnt using information available online. To illustrate this point, the Brick Lane Bomber David Copeland learnt from the Internet how to make and use pipe bombs in April 1999. Despite the fact that this was almost 10 years ago, we did not see the creation of such sites being outlawed until after the September 11th terrorist attacks on the World Trade Center in 2001. The sad and alarming truth seems to be that it takes a disaster of tremendous scale, such before affirmative action is taken which seems to suggest that action is unlikely to be taken regarding outlawing the issue of this research until we witness a disaster of national scale or a burglary epidemic in this country.

Recommendations

The way forward in research.
As is the case with any constructive piece of research, it is important to summarize the issues which have been brought to the attention of the author as being areas which could have been conducted, could have been improved, should have been included or simply couldn't have been achieved with the resources available in this case. Only by reviewing the research in this way can future study in the area evolve for the better and formulate a more augmented contribution to knowledge.

The first issue to note was previously mentioned and deliberated over during the methodology chapter. The predicament this author found himself considering was an issue related to the priorities of this research. The first option was to place no limit on the time allocation which was decided research on each term would be bound by. Elimination of this restriction would have allowed more time to conduct a far more in-depth study of the volume of material available online as the researcher would have been able to follow more internal links and use a larger variety of search results. This would have given a more thorough review of what sort of information is available, albeit after perseverance. However, it was decided that the second option was the most suitable one to use in this case as it allowed the researcher the chance to shadow what he believed to be the behaviour of the casual surfer as accurately as possible. This second option involved limiting the amount of time spent researching each search term, limiting the number of search results that are to be used involved making a conscious effort not to follow too many internal links to other websites. This method was considered the more appropriate of the two due to the priority of the research being to provide a review of the kind of material that *is* being viewed online, as opposed to what *could* be being viewed. However, having chosen to adopt only one of these options, the research rejected the advantages that the other option could have offered. For example, by choosing to adopt only the second method, the research did not have the opportunity to view the same material as that of those casual surfers who *do* deviate away from the original search page by following a more complicated sequence of internal links.

In order to gain a more holistic picture of social reality, it would not have done any harm to conduct a period of research under both methods. By doing this, the results could have been triangulated so that the advantages of one could have compensated for the disadvantages of the other. The reason such action was not taken by this researcher was due partly to the lack of time that was available for research, but mainly due to the hypothesis which was originally made which involved the assumption that the casual surfer would also act in such a way as to not devote too much time to researching the issue, not follow too many internal links to other webpages and would only use the first few relevant results that Google and YouTube provide after each search term was entered. In other words, by using both methods of research the first one would have admittedly provided the researcher with *some* valuable information, yet the proportion of all information of this sort which is available online that is actually being viewed would presumably be a lot less if the hypothesis mentioned above is accurate.

Another issue which could have been addressed prior to the conduction of this research, resources permitting, is that of online behaviour. The successful completion of this task would have narrowed down the extent of the material studied because the researcher would be given a more accurate picture of the practices and habits of those who search out this information for real and for illegitimate purposes. For example, if it was possible to find out the percentage of those who use Google as a primary means of conducting an online search, then the research method could have been adapted accordingly. This would have ensured that the research conducted by this study would have reflected similar material to that which is actually being viewed in reality.

Having said this, putting such a study into practice is much more problematic than it sounds. Taking into account what Sutton (2008) said regarding the online behaviour of young people (see p. 12, above), and the limited resources available to this researcher, in this case such research would have been an impossible task. Due to the anonymity of many of the viewers of such information, it is rendered unrealistic to expect this research to be able to contact any of the people who choose to view this information online. Some of those who disclose the information themselves could have been contacted, yet apart from the ethical considerations this would bring into question, it would add little to our knowledge about the behaviour of those who read the information which is available.

One important area where this research failed to adequately add a contribution to knowledge was the extent of the damage that such information may be having on the rest of society. Certain questions were addressed during the research process which aimed to gain an idea of this such as how many times a video had been viewed and whether any feedback left on information from other users suggested that it may be being used for illegal purposes in the "real" world. This would only be possible after conducting research on a far broader scale than was achievable on this occasion. Had more resources such as time been available to the researcher then this would be a way in which a more holistic picture of social reality could be gained. What this research did show however, is that it is certainly an issue which requires further study. Every tutorial video researched on this occasion had been viewed thousands of times by Internet users around the world which is a worrying quantity to say the least. The research also uncovered many occasions where criminal use of the information was explicitly admitted. Perhaps a good way of progressing in research would be to monitor the whereabouts or origin of the people who are viewing this information, this could be correlated with burglary statistics (e.g. do more people view the information who are from an area in which burglary is particularly rife such as Bristol, Nottingham or London?). Obviously the practicalities of this are farfetched but this would be a more effective measure of the effect that the availability of this kind of information is having on surrounding communities and on society as a whole. From this research alone, it remains impossible to draw cause and effect between the number of views or "hits" a website receives and the prevalence of burglary in the offline world.

The Internet as the source of the problem.

Anonymity, which was discussed earlier within the review of literature chapter of this research, is the characteristic which creates the most problems for law enforcement and is one of the main reasons for such information being freely available globally in its current state. It has often been argued that anonymous communications facilitate illegal conduct and allows perpetrators to evade the consequences of their actions (Ellison and Akdeniz, 1998 in Jewkes, 2002). The prohibition of these anonymous communications has been called for by many which would alleviate a lot of the associated problems. However, the problem that such a move currently faces is that it is halted by the argument that restricting anonymity, which is valuable for free speech, is unconstitutional (Jewkes, 2002). It therefore seems unlikely that such an achievement will ever be made for as long as this argument is respected as being of paramount importance. What needs to be considered by those who oppose such a move is the amount of damage that such anonymous communications have the potential to cause, and most importantly whether the value of free speech is to be considered more valuable than this.

What also needs to be considered is the social responsibility of search engines and portals such as Google, Yahoo and YouTube. Sources such as these currently provide easy global access via un-moderated links to all sorts of harmful content. Sutton (2007) said of this issue that 'more research is needed in this area in order to make policy recommendations for the information industry and for non-profit organizations, particularly regarding the possible impact of the

"advertising effect" (Bjorgo, 1993)' (Sutton, 2007, p. 35). Although here the authors Sutton and Bjorgo were discussing the issue of white racialist web presence, the "advertising effect" mentioned could also be attributed to the issue of this research which the ease of access, that is currently being granted by search engines to web users all around the world, is almost entirely to blame for.

Conclusions

Despite the issues previously mentioned in the recommendations chapter concerning the areas that this particular research failed to cover or was unable to answer, this study provided many insights which highlighted areas of concern for public safety which require attention before they become even more destructive to society. Until now this, and other similar harms, have been seen as an online issue. The truth is however, that this is an issue which causes crime in the offline world, it has offline consequences and causes offline victims. Therefore issues such as this are an essential aspect of social governance and until this is realised and action is taken, information sharing of this kind will continue to prevail.

The first issue which this study has discovered is the lack of research that has directly addressed the issue of the Internet as a source of knowledge for general offending techniques. As discovered during the review of the relevant literature, there exist only a handful of issues of this genre which have been directly addressed in a positive way by law enforcement. Three of the main examples which have been tackled, or are at least in the process of being addressed, are terrorism, anorexia websites and websites which are perceived to encourage suicide. Since the infamous terrorist attacks on New York and London in 2001 and 2005, the presence of terrorist groups online has been directly addressed and legislation such as the Terrorism Act 2006 was drafted in with the purpose of preventing the illicit spreading of information and ideologies online. Viewing harmful material became an offence under this legislation and as a result we saw previously accessible bomb-making sites removed from the Internet from the public eye. Although action such as this is certainly not watertight by any means, it serves the purpose of harm reduction. A similar move with regards to burglary techniques is what is ultimately required yet it seems as if this is an unlikely aspiration without a nationwide rapid increase in the burglary rate coupled with research which is able to prove a direct link between this and the availability of this online information.

Although to label terrorism as a moral panic is somewhat controversial, the realistic threat it posed to society was perceived to be far greater than it was likely to be during the aftermath of the notorious attacks on the Western world, albeit justifiably. It is far easier to describe anorexia and suicide websites as being at the heart of a moral panic. The current state we are in with these two issues is that the media have created a deviancy amplification spiral (Cohen, 1980). By affording a handful of cases far more coverage than they would ordinarily receive, this has created the impression that the issue presents far more of an imminent threat to society than it perhaps does in reality. Public fear fuels public pressure on policy makers and we are currently on the verge of seeing the outlawing of the existence of such websites on the Internet as a result. During the conduction of research, only one newspaper article (The Evening Standard, 2006) was discovered that expressed concern for the possible implications of the availability of burglary tutorials online. The article expresses similar concerns to those of this study, discusses the possible implications and provides examples of when the techniques have been explicitly used for illegal purposes. Despite the publication of this article in 2006, it contributed very little both in increasing awareness and on the behalf of YouTube. Hopefully, more research such as this study and more coverage in the media will highlight the need for affirmative action on the behalf of those responsible for change, and policy will eventually be made which confronts this issue along with the many other similar dangers and offending opportunities the Internet presents, before they

cause more harm than they already are. Although moral panics have so far been presented as a relatively negative thing as it creates disillusion, they are not. The alarming truth is that they are the most effective way of grabbing the attention of policy makers and law enforcement and for this reason, a moral panic needs to be created if progress is to be made.

To discuss the issue on a far broader scale, it seems unlikely that we will ever have an international law that binds all Internet users due to the different moral values and cultural beliefs that exist around the world. The fact is that no one set of morals, values or codes can be considered to be the "correct" set, which is why it is the personal belief of this author that no one nation has the right to exert and enforce theirs upon another. Due to the global reach of the Internet, the international access that is made possible and the varying moral values around the world, it is unlikely that we will see information sharing such as this eradicated globally. Successful governance of the Internet will require a UN-style level of command and control yet without compliance from every single nation around the world the entire concept would be compromised as people would always be able to exploit the loopholes that certain jurisdictions possess in their law.

It may be a far bigger issue than at first perceived which can concern the whole of the media. Information can adversely be divulged in many different forms by the media which can range from saying how a burglar achieved a burglary in an article in a newspaper, to the Discovery series "It Takes a Thief" which demonstrates to viewers how to break into peoples homes. For this reason, the responsibility does not lie entirely upon the shoulders of the Internet as we must consider the messages which are being portrayed by all areas of the mass media. However, what makes the Internet the most prolific of this diverse range of threats are the unique characteristics that it possesses, and the sheer range of the possibilities that it affords people the ability to achieve. Areas of the media such as newspapers and television can to a certain extent be regulated by authorities, yet in its current state, due to its borderless nature and the anonymity users can achieve, the Internet remains a place in which harmful information sharing can flourish and is controlled almost entirely by whoever wishes to control it.

References

BJORGO, T. (1993) *'The Role of the Media in Racist Violence'.* Taken here from SUTTON, M. (2007) (in press) *'Finding the Far Right Online: An Exploratory Study of White Racialist Websites'.* In POYNTING, S., & WILSON, J. (ed.) *'Sticks and Stones: Writings and Drawings on Hatred'.* Sydney: Sydney Institute of Criminology and Federation Press.
BRYMAN, A. (2004) *'Social Research Methods' (2nd Edition).* New York: Oxford University Press.
CAVADINO, M. & DIGNAN, J. (2002) *'The Penal system: An Introduction' (3rd Edition).* London: Sage.
COHEN, S. (1980) *'Folk Devils and Moral Panics' (2nd Edition).* Oxford: Martin Robertson.
COHEN, L., E., & FELSON, M. (1979) *'Social Inequality and Predatory Criminal Victimisation: An Exposition and Test of a Formal Theory.'* American Sociological Review, 44: 588-608.
DENNING, D. E. (1999) '*Information Welfare and Security*.' Boston: Addison Welsey.
ELLISON, L. & AKDENIZ, Y. (1998) *'Cyber-stalking: The Regulation of Harassment on the Internet'.* Criminal Law Review 29 (special edition, December): 29-48. Taken here from
JEWKES, Y. (2002) *'Dot.cons; Crime, Deviance and Identity on the Internet'.* Cullompton: Willan.
FRANKO A., K. (2007) *'Beyond 'the Desert of the Real': Crime Control in a Virtual(ised) Reality'.* Taken here from JEWKES, Y. (ed.) (2007) *'Crime Online'.* Cullompton: Willan.
GRABOSKY, P., & SMITH, R. (2001) *'Telecommunications Fraud in the Digital Age: The Convergence of Technologies'.* In WALL, S., D. (ed.) (2001) '*Crime and the Internet.'* London: Routledge.
HOPKINS-BURKE, R. (2005) *'An Introduction to Criminological Theory' (2nd Edition).* Cullompton: Willan.
JEWKES, Y. (2002) *'Dot.cons; Crime, Deviance and Identity on the Internet'.* Cullompton: Willan.
JEWKES, Y. (2007) *'Crime Online'.* Cullompton: Willan.
LEVY, S. (1984) *'Hackers: Heroes of the Computer Revolution'.* Taken here from NEWMAN, G., R., & CLARKE, R., V. (2003) *'Superhighway Robbery: Preventing E-Commerce Crime'.* Cullompton: Willan.
OFFICE OF PUBLIC SECTOR INFORMATION, (2006) *'Terrorism Act 2006'* (Internet). Available from http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_2#pt1-pb3-l1g11. Accessed 22/03/2008.
PEASE, K. (2001) *'Crime Futures and Foresight: Challenging Criminal Behaviour in the Information Age'.* In WALL, D. (ed.) (2001) *'Crime and the Internet'.* London: Routledge.
SUTTON, M. (2007) (in press) *'Finding the Far Right Online: An Exploratory Study of White Racialist Websites'.* In POYNTING, S., & WILSON, J. (ed.) *'Sticks and Stones: Writings and Drawings on Hatred'.* Sydney: Sydney Institute of Criminology and Federation Press.
SUTTON, M. (2008) *'Viruses, Virus Writers and Hactivism'.* Presentation for BA Criminology High Tech Crime module. Nottingham Trent University. 7th February 2008.
THE EVENING STANDARD (29/11/2006). *'Anger at YouTube Videos That Show How to Break into Houses'.* www.thisislondon.co.uk *(Internet).* Available from http://www.thisislondon.co.uk/news/article-23376335details/Anger+at+YouTube+videos+that+show+how+to+break+into+houses/article.d. Accessed 21/11/2007.
WALL, D., S. (2001) *'Cybercrimes and the Internet'.* In WALL, D., S. (ed.) *'Crime and the Internet'.* London: Routledge.

Web Addresses

FINAL THOUGHTS, INVENTGEEK.COM (01/06/2006) *'The Quick Vibrating Lockpick'* (Internet). Available from http://www.inventgeek.com/Projects/lockpick/page4.aspx. Accessed 03/01/2008.
INVENTGEEK.COM (01/06/2006) *'The Quick Vibrating Lockpick'* (Internet). Available from http://www.inventgeek.com/Projects/lockpick/Overview.aspx. Accessed 03/01/2008.
LOCKPICKSHOP.COM *'Lockpickshop.com: The Best Priced USA Made Lockpicks'* (Internet). Available from http://www.lockpickshop.com/. Accessed 03/01/2008.
MAKEZINE.COM (11/01/2006) *'How To: Make a Quick Low Cost Vibrating Lockpick'* (Internet). Available from http://blog.makezine.com/archive/2006/01/make_a_quick_low_cost_vibratin.html. Accessed 03/01/2008.
PROJECT OVERVIEW, INVENTGEEK.COM (01/06/2006) *'The Quick Vibrating Lockpick'* (Internet). Available from http://www.inventgeek.com/Projects/lockpick/overview.aspx. Accessed 03/01/2008.
PRODUCT FEEDBACK, UKBUMPKEYS.COM/LOCKPICKS (2008) (Internet). Available from http://ukbumpkeys.com/BMWinnergroovepick.html. Accessed 03/01/2008.
TOPSECRETMAGIC.CO.UK/LOCKPICKS *'Lock Picks and Escape Tools'* (Internet). Available from http://www.topsecretmagic.co.uk/lockpicks.html. Accessed 03/01/2008.
UKBUMPKEYS.COM/LOCKPICKS *'Uk BumpKeys'* (Internet). Available from www.ukbumpkeys.com/lockpicks. Accessed 03/01/2008.
UKBUMPKEYS.COM/LOCKPICKS *'BMW Inner Groove Kit'* (Internet). Available from http://ukbumpkeys.com/BMWinnergroovepick.html. Accessed 03/01/2008.
YOUTUBE VIDEO (04/09/2006) *'How to Pick Locks (The Beginners Guide)'* (Internet). Available from http://www.youtube.com/watch?v=LkuUGOsAETw. Accessed 03/01/2008.
YOUTUBE VIDEO (15/10/2006) *'Miles Shows us How to Break into a House!'* (Internet). Available from http://www.youtube.com/watch?v=TNXaxIlXqKw&feature=related. Accessed 03/01/2008.
YOUTUBE VIDEO (27/10/2006) *'20 Seconds Real Cylinder Lock Picking'* (Internet). Available from http://www.youtube.com/watch?v=_J2CLVmIMoI. Accessed 03/01/2008.
YOUTUBE VIDEO (20/03/2007) *'Lock Picking a Padlock'* (Internet). Available from http://www.youtube.com/watch?v=U24MQAK-Sxs. Accessed 03/01/2008.
YOUTUBE VIDEO (14/08/2007) *'New Lock Picking Kit'* (Internet). Available from http://www.youtube.com/watch?v=VPW_vnAHxZg. Accessed 03/01/2008.
YOUTUBE VIDEO (14/08/2007) *'Learn How to Pick Combination Master Lock'* (Internet). Available from http://www.youtube.com/watch?v=CM1Mtj3aCUs. Accessed 03/01/2008.
YOUTUBE VIDEO (14/08/2007) *'Paperclip Door Lock Picking'* (Internet). Available from http://www.youtube.com/watch?v=D-zWo8IT9kg. Accessed 03/01/2008.