Online Harassment and Digital Stalking

Thaier Hamid, Ph.D
University of Bedfordshire, UK

Carsten Maple
University of Bedfordshire, UK

ABSTRACT

Cyberstalking is generally considered to be harassment that originates online; however it is also recognised that other forms of pre-existing stalking can transfer into online environments. Cellular phones are now owned by the vast majority of adults (91% in 2010/2011) in the United Kingdom. It is believed that this number will approach, and probably reach, 95% within the near future. The World Wide Web and Internet are great places to study, work or even play, but there is an unpleasant side to cyberspace. Cyberspace reflects the real world and some people tend not to remember that. Cyberstalking and harassment affect a large number of people (especially women). It should not be assumed that just because an individual owns the technology and has an Internet account that person is ethical. There are just as many stalkers in cyberspace as anywhere else; it is just that their methods have changed. In some cases, this harassment may become an organised operation, where stalkers attack with intimidating messages of hate and indecencies. In this paper we study the different aspects of the technologies used in stalking and some methodologies to reduce the impact in relation to our own safety and security.

Keywords Cyberstalking, Technology, Internet, Social Network, Facebook.

1. INTRODUCTION

We can define cyberstalking as the use of Information and Communication Technology (ICT) devices such as networked Personal Computers (PCs) but it can extend to portable devices such as laptops, PDAs (Personal Data Assistants), mobile phones and more generally devices linked to the Internet, or any other electronic means (global positioning systems (GPS), cameras, voice recorders etc) to stalk someone. Belsey [1] defines cyberstalking as "Cyberstalking involves the use of ICT to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others". To identify cyberstalking we need to consider the following features: repetition, suffering, hatred, planning, obsession, harassment and threats. However, many people do not take cyberstalking very seriously; in terms of reporting, usually cannot consider anyone as a victim of cyberstalking if they have not said No to the stalker and reported the incident. Technology is developing with unrestricted opportunities for people. The Internet provides instant answers to questions, fast information and unrestricted avenues for exploration. Social networking links with contacts is now easier than ever through mobile devices, PDAs and computers. Nevertheless, without proper instruction on how to navigate real life situations, technology can take individuals down a dark track. Individuals who have been cyberstalked can quickly become depressed or could turn to suicide. Cyberstalkers might use email, message boards, social networks, discussion forums, chat rooms, GPS technology, video games, listening devices, hidden cameras and more to target their victims. Addressing the American Psychological Association's Annual Convention, Elizabeth Carll [2] said: "Increasingly, stalkers use modern technology to monitor and torment their victims, and one in four victims report some form of cyberstalking, such as threatening emails or instant messaging". The majority of cyberstalkers are men and the majority of victims are women. According to WHOA [3], in 2011 74% of cyberstalking victims were females and only 26% were male as shown in figure-1, 40% of the stalkers are males and only 33.5% are females. The remainder are unknown or basically they prefer not mention their gender.

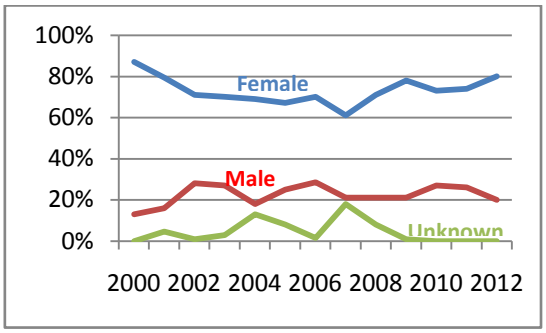

Figure-1: Number of stalkers (out of total case study of 3393) from 2000-2011

14,748 people were murdered nationally in 2010 [4] and, in the course of a one-year period, 3.4 million people aged 18 or older in the United States were stalked [5].

It is essential that technologies users understand how the technology might put them at risks and the actions they need to take to decrease those risks. Online information such as personal information, financial information, internet usage, details of friends and family, daily activities, work activities and location and much more is called a digital footprint. Anyone who leaves a unique identifier online as a digital footprint, that could be found and used by a stalker, puts themselves at risk and, therefore, we should give some thought as to what is shared and distributed on the cyber media. Social engineering is a method used to trick the victim or others into revealing information that could be used to harass or degrade the victim. The attackers use the information collected about the victim in order to gain respect and trust and to later publish additional false information to damage the victims' reputations. Social engineering is used to describe a not technical kind of attack which depends mainly on human collaboration and involves misleading other people into violating regular security measures. For example, instead of trying to find a vulnerability to crack the password, a social engineer may call an employee and pretend to be an IT technical support individual, trying to deceive the employee into disclosing his/her password. Spyware is a type of software that collects information from computing devices

without a user's agreement. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits and other personal information which is useful to stalkers. The data is often passed on to online stalkers or hackers. This paper reviews the most commonly used technologies - mobile phones and PDAs, geo-location, social networks and spyware and their risks.

2. RISK ASSESSMENT

The Risk is defined to be a function of the probability (likelihood) and the severity (impact) of the probable breaches on the systems. The risk in IT systems could be exposed from Internet, Network, Servers and Local Host.

Risk = Likelihood of an adverse event x Impact of the adverse event.

Since 1980 the above method has been fundamentally challenged. Specialists accept the main elements in the function but disagree on the production of likelihood and impact on calculating the risk, as the risk should be evaluated in terms of maximum impact on an adverse event.

$$W_i = f(I, L)$$

Risk assessment could be implemented to measure system reliability and to benchmark different security solutions. A measureable risk assessment is the main tool used to determine if the additional budget should be allocated to allow more secure features.

The objective of risk assessment is to measure the likelihood of exploitability and its consequences, by measuring the probability that manifest threats in terms of access required, attack complexity and weighting the impact of the occurrence with the potential damage that may be effected.

In cyberstalking, the likelihood is a feature of stalking as the stalkers need to repeat the aggressive behaviour by an individual or group that is intended to harm others; the impact could be experienced psychological and behavioural effects such as depression, isolation, anxiety and extreme caution of their surroundings.

A risk matrix shown in Figure 2, linking the two vectors of likelihood and impact, is a graphical description of different risks in a relative way. The matrix uses four levels of weights to classify the ranks of different types of risks.

Figure-2: Risk assessment matrix

1- Level 1 (100): A vulnerability that will allow an intruder to immediately gain privileged access (eg Administrator, root) to the system; for example Buffer overflow from a local or remote system.

2- Level 2 (70): Vulnerabilities that allow local or remote users to increase their privileges on a system or access confidential information such as company financial records or user passwords are usually considered moderate risks.

3- Level 3 (50): Vulnerabilities like a Denial-of-Service attack. Generally, these do not compromise the system beyond a Denial-of-Service. This type of condition is often inherent in running a particular service.

4- Level 4 (10): Vulnerabilities that provide information (information about the target is gathered) to an intruder that might lead to further compromise attempts.

3. MOBILE PHONES

Smart phones are now considered as key technology to exchange information and to communicate between people. The regular cell phones users are considered very old fashioned because they do not give individuals access to the Internet, Facebook and Twitter. Smart phones enable users to post instant messages that can be seen by all friends and followers of the account holder on the social network. With the majority of social networking sites used today with smart phones, the normal users usually accept a request from a friend or follower, without realising the risk of their actions. So instead of using your cell phone to send a text message to one or more, your message is immediately seen by potentially hundreds or thousands of people. Mobile phone ownership has increased worldwide in the last decade. In the United Kingdom in 1998/1999 27% of households owned a mobile phone, rising to the vast majority of adults (91%) in 2010/2011 (National Statistics [UK], 2011). The vast increase in this communication technology usage indicates that we should start demonstrably to detect the various impacts it has made on people's activities and interactions. Mobile phone technology has improved the overall level of communications within a social circle but it can also permit stalkers and strangers to connect to you without your knowledge. We believe that the media should be used to educate people about the risks associated with using mobile phone technology, as will be recommended for schools containing elements of increasing awareness of using technology concerns. It is well known that the existence of GPS in mobile phones can track your movements, but many people are not aware of the availability of application software that can be installed on all kinds of mobile phones that can monitor your location, conversations and any sort of personal information existing on your mobile such as photos and videos. If someone remotely controls and activates your mobile phone, you will not be aware of his/her actions; they might be looking at your photos or observing your conversations at your location. Your phone could be used, for example, to operate the camera next to you while you are watching television and someone can access your phone and see what you are viewing. It is predicted that the coming years will see huge amounts of wireless data through mobile devices. There are three most commonly used location technologies: standalone, satellite-based and terrestrial-radio-based [5]. As examples, a typical satellite-based technology is GPS; and a typical terrestrial radio-based technology is the "C" configuration of the Long Range Navigation (LORAN-C) system. Many researchers focus on the control of mobile phones remotely to explore the current location, by capturing pictures automatically and uploading

them to a web server. They can also be used to retrieve and send the GPS latitude/longitude to the database of a web server and control of electrical device interfaced with mobile phone via DTMF detection circuit.

4. A SOCIAL NETWORK SYSTEM

Personal disclosure used to be something that was intimate and private. Social networks like Facebook have changed that view of social relationships. As of September 2012 [update], Facebook has over one billion active users [6], more than half of them using Facebook on a mobile device (Facebook Statistics, 2012).

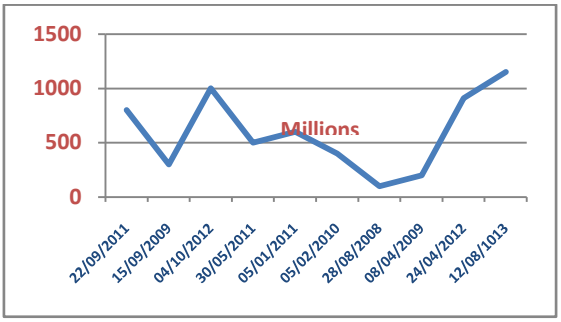

Figure-3: Number Of Facebook Users (Millions) From 2009-2012

Advancement in broadband technology has parabolically increased accessibility to the Internet. It is now cheaper, easier and more convenient for people to communicate globally. In the past four years, social networking websites like Facebook have grown with exponential popularity. Facebook defines itself as: a social utility that helps people communicate more efficiently with their friends, family and co-workers. The company develops technologies that facilitate the sharing of information through the social graph, the digital mapping of people's real-world social connections. Anyone can sign up to Facebook and interact with people they know in a trusted environment. A social network system (SNS) allows groups of friends to be accessed and engaged with from one's mobile phone. Foursquare [8] is the latest social networking tool to generate online buzz. The story has become very familiar in recent years: a bright young person develops an internet app that connects people and allows them instantly to communicate with each other and within months a million or more people around the planet are using it. Investors queue up expressing an interest and speculation begins about how much Google, Yahoo!, Apple or Microsoft are willing to offer to snap it up. (To date, the speculative figure in the media has reached $100m.) Twitter, Facebook, MySpace and Bebo have all come before it, but Foursquare promises something new. After a decade of false dawns for the industry, it leads the way in a wave of new "geolocative" social networking tools. Unofficially, at least, 2010 has been labelled by many within the technology world as the "year of location". In addition to offering the communal connectivity of Twitter and Facebook, Foursquare also uses your Smartphone's global positioning system (GPS) to broadcast your precise location to your "friends" and, should you wish, to the wider world. Users are encouraged to "check in" on their phone whenever they arrive at a point of interest – a shop, a cafe, a museum, a nightclub, an office – so that fellow users know where they are. A great way supposedly to see if any of your friends are round and about. Glance down at your phone and see the names of all the other users around you within a mile or so and, crucially, exactly where they are and which fellow users they are with. Foursquare is now being widely touted as the app which will, after years of anticipation and prediction, mark the beginning of "life as a game" computing. Whatever you do, wherever you go, you will be scoring points, earning "medals", and are in, at the very least, social competition with other users around you. What the ultimate prize is, no one is yet quite sure, but some companies have been quick to realize the potential of this technology with Starbucks, Debenhams and others offering loyal customers who frequently check in to their stores rewards such as a free cup of coffee. Imagine a supermarket loyalty reward card synced with Twitter! Privacy advocates fear that Foursquare, along with other geolocation apps such as Gowalla and Google Latitude, are vulnerable to "data scraping"; namely, the sophisticated trawling and monitoring of user activity in an effort to build a rich database of personal information. The big worry, say critics, is who might get to make use of this information. Pick your paranoia. Someone with criminal intent, such as a burglar, identity thief or stalker? Governments, the security services or police? Terrorists? Or a corporation looking to target its products at you with incredible precision? Compounding the threat is that "friends" are much more readily accumulated in the online world of social networking compared to who we might choose to accept as friends in our "real life". Accept a friend request in Foursquare without due care and you are potentially opening up your personal record to a complete stranger. "The issue with location-based information is that it exposes another layer of personal information that, frankly, we haven't had to think much about: our exact physical location at anytime, anywhere," explained the creators of PleaseRobMe.com, a website set up to expose how vulnerable Twitter users can be when displaying location-based messages, earlier this year. "If you're comfortable being a human homing beacon, that's fine, we just want you to be fully aware of what that means and the potential risks it might involve." Nearby Friends: New Cyber-Stalking App for Tracking Facebook Places Check-Ins Nearby Friends is a Facebook application-2010 which taps into the recently launched Facebook Places check-in service to locate all your Facebook friends plotted on a Google Maps interface. The app, a simple tool that places Facebook profile photos as a pin on the map, doesn't limit itself to where your friends are right now, it actually displays their entire Facebook check-in history, as lines traversing the map. With the app installed, you can actually track a friend's movements, easily identifying their favourite hangouts, daily treks, their workplace and more.

5. ACCOUNT TAKEOVERS

Account takeover is one of the more prevalent forms of identity theft. It occurs when a stalker obtains an individual's personal information (account number and social security number usually suffice) and changes the official mailing address with that individual's financial institution (FI). Once accomplished, the fraudster has established a window of opportunity in which transactions are conducted without the victim's knowledge. An account takeover can happen when a stalker or computer criminal poses as a genuine customer, gains control of an account and then makes unauthorised transactions. Any account could be taken over by fraudsters, including bank, credit card, email and other service providers. Be careful of scams. Online banking accounts are usually taken over as a result of phishing, spyware or malware scams. This is a form of internet crime or computer crime. Where a fraud has been committed, the main reason is weak

passwords. Our passwords allow us to access accounts, information and devices. It is what keeps our data private, safe and secure. All our online activity: our email, Google or iPhone mobile account, e-shopping, social networks, banking and taxes all require passwords. Because we have so many online accounts and couldn't possibly remember a different password for each one, we use the same password and username for all of them. But that means if an abuser can access one account they usually can access multiple accounts. The other problem is we choose passwords we can remember. They are usually a piece of personal information such as favourite football team, name of our children/dogs, hometown etc. Studies show that a significant percentage of people use the same 50 common passwords such as passw0rd, qwerty, letmein or 123456. Because stalkers know their victims well and will be determined, they often succeed in guessing a victim's password(s). There is free software called "password managers" that can make it easy to use multiple, secure passwords. When a stalker compromises your customer account, the perpetrator can use the victim's account to send themselves abusive messages in order to incriminate the victim. They can damage or destroy relationships by accessing a victim's e-mail account to send family, friends, work colleagues or clients abusive messages, or messages telling them never to contact the victim. Solving the problem becomes complicated. When was the account breached? Which account activities were fraudulent—and which were not? How do you manage all of the consequences? Account takeover is becoming progressively noticeable and is a growing point of security, exposing businesses and individuals. Dipping exposure is best accomplished through methods such as:

1. Prevent losses due from transactions using stolen credentials

2. Lock out malware that steals credentials while customers are on your site

3. Reduce challenges to legitimate customers while finding the suspicious ones

4. Offer trusted customers visible security with client-side malware screening

5. Add global network intelligence to fraud prevention, without sharing personally identifiable information

6. COMPUTER SPYWARE

Spyware is one type of malicious software (malware) that gathers information from a computing system without your permission. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits and other personal information. The data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute crimes or identity theft. Spyware can monitor almost any activity or data related to your computing environment. This is not limited to files on your hard drives but can also include temporary data such as screen shots, keystrokes and data packets on connected networks. When spyware is running on a computer system, there is almost no data outside the reach of a malicious programmer. Commonly targeted data includes

1. internet activity
2. email and contact information
3. Windows Protected Store data
4. clipboard contents
5. keystrokes
6. screenshots
7. network traffic

To help stop the spread of spyware and other malware, it is essential to be alert to suspicious activity on your computer and to learn safe computing practices. While some spyware is deployed by exploiting flaws in operating systems or applications, much of it still relies on social engineering to trick you into running or installing malware. You must exercise caution when downloading anything from public web sites, newsgroups, and instant messaging sessions or when opening email attachments, even from senders you know. Identity is often difficult to verify on the internet. Frequently, attackers and their malware impersonate associates of the target user to coax them into installing the malicious code. A common example of this is when malware infects a system and then automatically emails itself to everyone in the infected person's address book. When such an email is received, the recipient is more likely to open the contents because the sender is a familiar, trusted source.

7. GEOLOCATION

The combination of GPS services and information technology is increasing with the use of geolocation occurring as a default action in many personal property based devices' functionality, for example mobile phones and cameras. The camera in suitably enabled phones takes the picture and embeds GPS co-ordinates of the location into the metadata of the resulting image file. Furthermore, there are now online services such as foursquare that are directed at the geolocation or geocaching community. In addition to this bespoke service, other social online services such Flickr and Twitter are providing a means of geolocation users. This enablement of technology has significant and considerable effects on personal security and also extends into corporate security. One of the recent innovations enabled in these phones is the use of GPS services to tag the location of the device, or where a digital photograph was taken, referred to as geolocation. The phones also compute location as an on-going feature that is used to report location on social networking applications when interacting with services.

Many of these services not only use GPS but also wireless access points and mobile telephony towers. As an example, the first generation iPhone used Skyhook [3] to provide locational service by this vector. Later devices are now using combinations of positional services to get even finer resolution of location. We study the geolocation from an aspect of personal privacy and security as well as enterprise implications. Geolocation in images involves the insertion of location data, specifically latitude and longitude format, into an image file. Insertion of location data can be performed as a manual operation or automatically, by a location aware image capture device (commonly a camera or mobile phone) at the time of creation. The Exchangeable Image File format (EXIF) is a published industry specification for the image file format used by digital cameras. The location data is typically stored within the EXIF records for the image using the EXIF Global Positioning System sub-IFD that uses the TIFF Private Tag 0x882. The EXIF can also contain information that uniquely identifies the device that has taken the image. Graphics tools such as ExifTool are able to extract this extended device and locational data; likewise digital forensics tools are able to

locate this data in images involving the insertion of location data, specifically latitude and longitude format, into an image file. Geolocation in social applications is achieved in much the same manner as that of images; individual files and objects within a social media construct are tagged with geolocation data. The geolocation data is harvested from media at the time of upload or provided by the client application at the time of submission. There are a number of social media services that have enabled geolocation features; we will be examining two of the most widely known services in the social media arena: Twitter and Flickr. Twitter is a micro-blogging service that allows its users to post 140 character status updates. These status updates are then available to the user's friends or the broader internet; this is dependent on the user's privacy settings. The ability to tag posts with geolocation information was added in November. These technologies bring together the intersection of cyberspace and real space, real object and real people. Already GPS style technologies can be used for a variety of reasons for the good, including the safe tracking and monitoring of the vulnerable ie young children or the elderly. This combination of technologies delivers true cyberstalking capability to stalkers from the anonymity of cyberspace. An example of the use of this for criminality is the site called pleaserobme.com [9] that aggregated Facebook users holiday entries and indicated whether a specific person was home or not. The use of geolocation tags allows for even more conclusive answers to home owners' possible locations ie you upload photos of your holiday to your favourite online photo repository indicating you are presently in another country.

8. CYBERSTALKING PREVENTION

In the case of a cyberstalking event, it is highly recommended that the victim saves all of the communication evidence, without altering or modifying, for future reference. If your Email software comes with Email filtering, the victim should warn the stalker to stop and then block him/her. If the stalking continues, using a different email address, the victim should consider contact the Internet Services Provider (ISP) and report the incident to law firm and cyberstalking helpline. If the online material appears to present a legitimate imminent threat of violence and danger to others, contact law enforcement, and initiate a protective response from the police.

The following are general rules for cyberstalking protection:

Assess what online information exists about you using internet search engines like Google; change your e-mail and passwords frequently for key online accounts and keep them safe; review all privacy and security settings in the computing device; avoid public forums; limit what you share especially personal information, photos, videos and educate friends, family and work colleagues; gather evidence; report to police; seek help and support from the charities.

The protection and prevention of cyberstalking does not only include personal measures, rules and regulations. The solutions to a cyberstalking problem could be represented as a technological solution, for example parental control settings in most operating systems or alternatively special parental control software, which help parents to filter Emails and chat rooms, block unwanted messages and messages received from unknown sources, web filtering may also be provided to restrict access to some harmful web sites. Anonymous remailers and browsers further reduce the likelihood of potential stalkers being able to identify victims. Some stalkers acting as hackers to exploit operating systems and software applications vulnerabilities; can install spyware and other monitoring software to follow the victim. Network Security Planning Architecture (Net SPA) and other attack graphs and vulnerabilities scanners can fix these problems by applying special patches which no longer allow attackers to access other computers. Some stalkers, with high technical skills, use IP Scanners programs which are widely available on the Internet, to scan a range of IP addresses for open ports or back doors to exploit and get access to the victim's computers for monitoring and tracking. There are many technical fixes developed to alleviate these problems, for example using NAT and PAT, mapping public IP addresses to a range of private ones. There are many other techniques available today to make the Internet users more secure.

The fact that, an offensive phone call or message, e-mail or other technological media is received at work on a personal level, does not justify the message or prevent it being a crime. Aggressive messages sent within the workplace can still constitute criminal offences. In addition, they may justify a claim for constructive dismissal and compensation under employment law.

Cyber harassment legislations are reasonably new, but that does not mean that crimes committed through the network are not punishable under legislation drafted for that purpose. In the UK, The Protection of Freedoms Act 2012 created two new offences of stalking by inserting new sections 2A and 4A into the PHA 1997. The two offences are in force from 25 November 2012 and provide further options for prosecutors to consider when selecting charges [10] when considering cyber harassment as a crime.

Although there are existing laws that prohibit cyberstalking or harassment in many countries, representatives on occasion consider that such laws are insufficient because the legislative responses are the most difficult and take a very long time for the cases to be finalised.

9. CONCLUSION

We studied different technologies used in cyberstalking; in conclusion we will summarise the countermeasures the individual should take to deal with different aspects and impacts of this technology. The password should protect all of your accounts - use complex passwords, do not use the same password for all accounts. We must always use anti-virus and anti-spyware software and keep security software regularly updated. Use advanced security settings and be suspicious of unsolicited contact, unusual contact or content. Never give out details unless you are absolutely sure of integrity and monitor your account activity.

Be cautious of using geo-location services on your mobile phone. Use encryption software to store data.

There are enormous uncertainties in the risk assessment of the security system because probability and statistics were used to evaluate the security of different cybersecurity systems. We suggest the use of information entropy to represent the average uncertainty of information systems and entropy weight method since the weight of the object index is usually used to measure the importance of the feature index. Integrating information entropy with risk assessments will help to identify whether the victim is high, medium or low risk in order to take the appropriate measures. The protection and prevention of cyberstalking does not only include personal measures, rules and regulations; the solution to a cyberstalking problem could be represented as technological solutions, for example parental control settings in most

operating systems or alternatively special parental control software, which help parents to filter Emails and chat rooms, block unwanted messages and messages received from unknown sources, web filtering may also be provided to restrict access to some harmful web sites.

10. REFERENCES

[1] Belsey, B. (2005). Cyberbullying: An emerging threat to the "always on" generation. Retrieved January 16, 2007 from http://www.cyberbullying.ca/pdf/feature_dec2005.pdf E. W. Dijkstra. A Discipline of Programming. Prentice Hall, Upper Saddle River, NJ, USA, 1976.

[2] Stern, Susannah R. 2004. "Studying Adolescents Online: A Consideration of Ethical Issues." Pp. 274-287 in Readings in Virtual Research Ethics: Issues and Controversies, edited by Elizabeth A. Buchanan. Hershey, PA: Information Science. B. Schneier. Attack trees: Modelling security threats. Dr. Dobb's Journal, December 1999.

[3] 2011 Cyberstalking Statistics, 1997-2012 WHOA from http://www.haltabuse.org/about/about.shtml visited on 05/12/2012.

[4] Federal Bureau of Investigation, "Crime in the United States, 2010," (Washington, DC: GPO, 2011), Table 1, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl01.xls (accessed 05/12/2012).

[5] Y. Zhao, "Mobile Phone Location Determination and Its Impact on Intelligent Transportation Systems," IEEE Transactions on Intelligent Transportation Systems, vol. 1, no. 1, pp. 55-64, Mar. 2000.

[6] "Facebook, 1 billion active people fact sheet". https://s3.amazonaws.com/OneBillionFB/Facebook+1+Billion+Stats.docx. Retrieved 05/12/2012.

[7] Japan Electronics and Information Technology Industries Association, Exchangeable image file format for digital still cameras: Exif Version 2.2, 2002.

[8] November 20, 2012. Olanoff, Drew. "Foursquare Adds "Recently Opened" Feature To Its Explore Section For iOS, To Promote New Businesses." http://techcrunch.com/2012/11/20/foursquare-adds-recently-opened-section-to-its-ios-app-to-promote-new-businesses/.

[9] Please Rob me website, raising awareness about over-sharing, http://pleaserobme.com/ (accessed 06/12/2012).

[10]http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/ Visited on 13/06/13.