A Review of Using Online Social Networks for Investigative Activities

Adnan Abdalla and Sule Yildirim Yayilgan

Gjovik University College
Po. Box. 191, 2802 Gjøvik, Norway
adnanbodo@gmail.com, suley@hig.no

Abstract. In this paper, we will describe the use of online social networks (OSNs) for law enforcement. With the increased growth of use of OSNs, the use of OSNs for law enforcement has also shown a parallel growth. Such a trend can easily be seen in the increase of reported number of criminal cases being solved by police officers of various countries. It is of interest to find out how OSNs are actually used by law enforcers to anticipate a crime, how they are being used by law enforcers to solve a crime committed, how they are used by criminals to commit a crime and what possible further needs law enforces have in using OSNs for predicting and solving crimes.

In order to be able to answer these questions, we have done an extensive review of the literature and existing available crimes. This led us to understand the nature of using OSNs for law enforcement. Further, we have contacted a questionnaire with the top level law enforcers in Turkey in order to find answers to the given questions above.

Keywords: Online Social Networks, Law Enforcement, Framework, Investigation, Digital Forensics, Evidence, Analysis, Tool, Digital Crimes, Activity.

1 Introduction

During the last few years, the activity of online social networks (OSNs) has increased excessively throughout all layers of society and nations. According Alexa traffic data, Facebook has now a total of 1.155 billion monthly active users. In Africa and Latin America, Facebook has 346 million users, Asia 339 million, Europe 272 million, and US and Canada 198 million users [1]. The excessive use of OSNs activities makes them an attractive arena to perform digital crimes (e.g. harassment, grooming, and child pornography) and classical crimes (e.g. Burglary, Kidnap, sex trafficking) [2] [3].

In contrast, widespread use of OSNs and their applications on diversity of digital devices (e.g. PC, pad, smartphone, etc.) attracted law enforcement agencies (LEAs) for help to solve and prevent any crimes linked and non-linked to OSNs, from evidence collection, to criminal identification and location [4][5].

G. Meiselwitz (Ed.): SCSM 2014, LNCS 8531, pp. 3–12, 2014.

Examining the activities of users on OSNs will provide a useful source for law enforcement investigators (LEIs) to find any missing information about particular person during digital investigation process. Nevertheless the law enforcement professionals (LEPs) are facing significant problems since there is no consistent, systematic, and legal framework built specifically for investigation on OSNs [6].

Based on reviewed existing literature of digital forensics investigation models for OSNs, most of these models have similar approaches which are focusing on internet investigations, but none of these have the nuance related to the investigatory process on OSNs.

In this paper we outline the current use of OSNs for investigative activities which describe the current system and framework for conducting investigation. In addition to that, the outline also categorizes crimes been employed by criminals which are involved directly and indirectly with OSNs.

Based on recent developed models of digital forensics investigation for OSNs, we propose an improvement for existing frameworks which describes the integration of analysis of user's behaviors in OSNs. Finally we will present a result of online study conducted among LEPs of various ages, geographies and experience levels in Turkey to understand the use of OSNs in law enforcement and current resources and processes used when utilizing OSNs in investigations.

2 Crimes Involving OSNs

OSN is a resource of information that can be employed by criminals to commit different types of crimes [7] [8]. The propagation of criminal activity on social networking sites is hard to define. This excessive use of social network activities makes them an attractive arena for different types of cybercrimes (e.g. malware distribution, fraud, harassment, grooming etc.). In addition to cybercrime as a specific activity, the social networks also serve as an informational valuable source for criminals in more traditional crimes (Assault, burglary, domestic violence, kidnapping). Because of this aggressive pattern of usage of social networking platform, we are being exposed to some bigger issues such as terrorism and organized crimes. We have divided crimes that involved OSNs into classical and digital crimes. These crimes are described in the following sections.

2.1 Classical Crimes

OSN is a place for criminals to perform their classical crimes. For instance, Facebook users can update their status by posting their current location, for how long they are away from home and what are they doing, which gives potential thieves enough time to take their chance to burgle into their property. There are numerous cases like this that appeared in the media [8].

A survey was conducted by Friedland UK's Home Security Week on 2011 among fifty convicted burglars. According to the survey, 78% of burglars stated that they believed OSNs like Facebook, Twitter, and FourSquare are fruitful tools for burglars targeting specific assets, while 74% stated that Google Street View was an important role in home burglaries [9].

2.2 Digital Crimes

OSN involves numerous illegal activities including; unauthorized or illegal access, interception by technical means of transmissions of digital devices to, from, or within digital devices. Types of digital crimes where digital evidence has been located: Social engineering, Cyber-Identity Theft, Cyber-Threats, Scams, Cyber-stalking, Online credit card fraud, Cyber-Harassment and more [10]. The majority of digital crimes on OSNs are cyber based, and social engineering can be used as one of technique for these crimes [11]. From statistics and real cases studied, we divided the crimes into digital and classical as shown in figure 1. All types of crimes which have been discussed above are widespread crimes in OSNs such as, Facebook and Twitter that provide a powerful communication tool for potential criminals to initiate their communication and to connect them to others anywhere at any time. While criminals are finding ways to cover and shield their posts from people, in the same way the criminal investigator works hard to discover any evidence related to criminals.

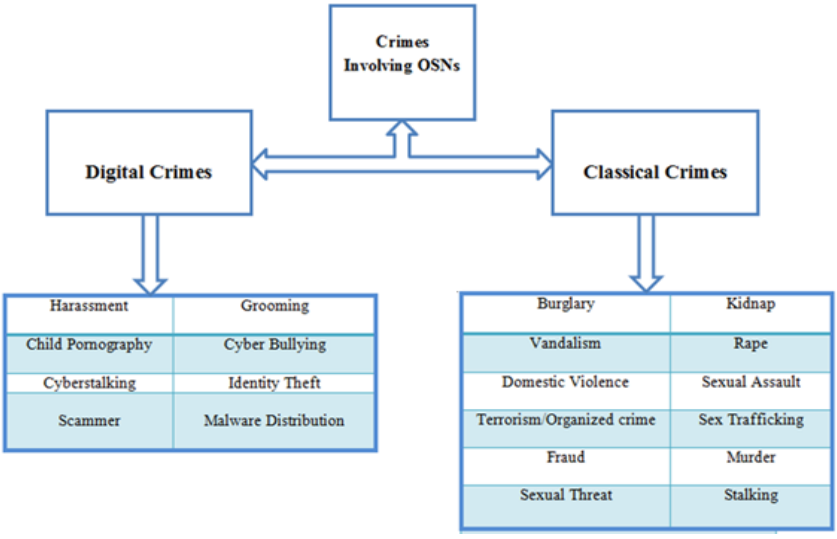

Fig. 1. Current crimes been involved by OSNs

3 Analysis of Online Social Networks

Social network analysis as a method is not something new, but a method that has emerged from social science, used by researchers to examine group structures and communication flows within a chart network by focusing on the relationships between entities. This type of analysis approach can provide efficient filtering of network information, quick identification of potential key individuals or groups for better prioritization of (often limited) resources and the ability to look beyond the network structure into its dynamics to identify characteristics that may not be immediately

apparent. This type of monitoring and analysis of groups and individuals of particular interest, which are generated from social networking data, can help forensics examiners to answer possible questions in their investigation.

3.1 Existing Digital Forensics Tools for OSNs Analysis

The confidential nature of work by LEAs and companies of OSNs was one of obstacles and barriers for our research to have structured interview with officers from National criminal investigation service. There is need to know how law enforcement officers deal with incidents that involved OSNs, and whether there are any standard instruments or computer programs utilized for extracting and analysis of public and private information of OSNs users.

We observed that LEIs have used different software or tools for different types of social networks to collect and analyze "publicly available" information. Based on our research we found that LEIs have been using different tools for different types of OSNs (e.g. Facebook, Twitter, LinkedIn, MySpace, and others) and different programs for different types of investigation to gather publicly available information. We propose that (figure 2), investigation types can be categorized into private investigation (e.g. burglary, kidnap, rape, murder, sexual assault), national investigation (e.g. domestic violence), and global investigation (e.g. terrorism attack/organized crimes).

Fig. 2. Types of investigations in OSNs

One of the major challenges for LEIs is how to gather and analyze public information from OSNs by utilizing different tools with different features within short period of time. LEIs stated that there are more valuable information that can be collected from OSNs than traditional investigation process such as interview with family members and acquaintances of the person of interest.

Examining the activities of OSNs users can help the investigators to extract direct feeling of person whenever he/she shares it in OSNs. For instance a person's post photos of holiday trip in somewhere with someone, can give a direct impression of happiness that he/she is having in specific time of posting the photo, or post

comments about incident happened expressing the sadness that he/she feeling it. Visualization and geographically presenting user's activities over time were dominant feature in most of tools been utilized. To enhance validity and accuracy of data collection of these tools, we have a need for a framework that visualizes the emotions of people based on their activities on OSNs by analyzing activities such as comments, tweet posts and other. A framework can correlate detected user's behavior on OSNs and compare it to Real-time incident. The framework must geographically estimate the expressions of feelings in ordinary and slang language. Mapping the mood over time can help the investigators to analyze the reactions of people for any incident can help in guiding national and private policy on the best way to counter major incidents.

3.2 Proposed Framework for the Forensic Analysis of User Interaction with OSN

We propose our improvement based on existing literature on framework for forensic analysis of user interaction with OSN as shown in figure 3. The investigation is initiated by acquiring data in two different approaches. Gathering evidence from public domains which are created by individuals where they made their pieces of information publicly available to anyone with internet access. In the second approach law enforcement has to legally request OSNs provider to obtain restricted data of user's information which they made their data private and not accessible for anyone with internet access.

Continuing the investigation process the forensic investigators have to run a search through large amount of different types of users' activities where data that can be collected and utilized as evidence (e.g., photos, comments, videos, link, posts in news, tagged photos and others). Nonetheless due to time consuming and huge amount of data that have to be examined, filtering the data is applied to identify temporal and geographical analysis of user activities, such as what, when, and where the user posted or commented, uploaded, tagged photos, or any updated statutes over time. Identifying the temporal analysis by highlighting peaks of activities (e.g., posting photos of visited places) over time and at particular point of time with geographical changes can help the forensics examiners to answer the needs by comparing temporal and spatial changes of users activities with real-time incidents. Analyzing accurate expression of user feelings in real time (e.g. just fine, bored, bored, tired, happy, hungry, confused, embarrassed, guilty, smart, hurt, annoyed, mad, sad, upset, angry, scared, disgust, surprise, and shame) and geographically and tracking how they develop these feelings over time, will give great advantage to forensics examiners to see real-time record of how and what people were feeling and if there is a relation between these expressions with real-time incidents that happened in a criminal case. Analyzing individuals' emotions can be achieved by developing a program with visualization features applied which help forensics investigators to determine the direction of investigation of mass amount that represents someone's virtual community.

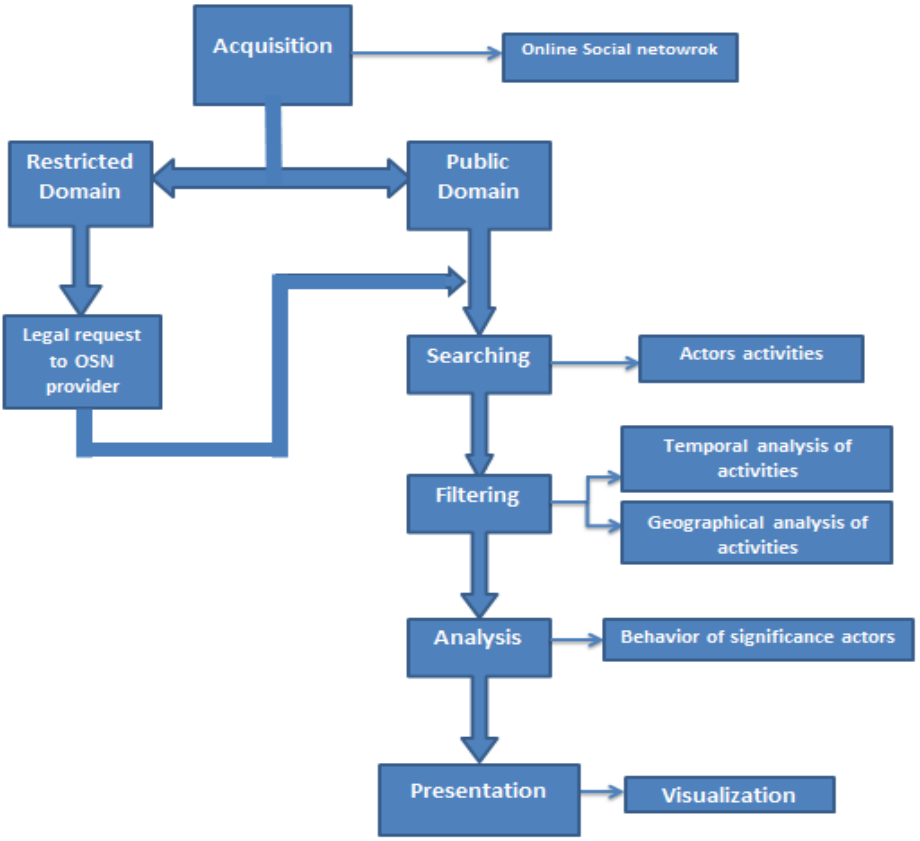

Fig. 3. Proposed framework for the forensic analysis of user interaction with OSN

4 Questionnaire

We designed the questionnaire in a way that lead us to answer to the main objectives for discovering related facts to highlight and understand the use of OSN for law enforcement, specifically with regards to criminal intelligence and investigative process.

We distributed questionnaire among law enforcement agencies in Turkey. Fortunately we received response from some law enforcement with different designation and possessing high experience ranging between 10 to 19 years. The participants were having various positions from deputy chief of police, leadership, special police units (SPU) officer, war crimes investigator and police officer. Majority of their ages were in the range of 40-49 and 30-39 years. In addition, the participants were representing from different provinces and highly populated areas such as Istanbul, Antalya and Bursa. Therefore, we believe the numbers of participants from these law enforcement agencies are sufficient to allow us in drawing statistical analysis.

Questionnaire contains fifteenth questions which focus on the scope of research work. Questionnaire starts with brief explanation about the purpose of the study and informing that the identity of participants will be kept hidden. The participants will be asked to provide (if they feel it comfortable) information about their age, region, position/ responsibility in the organization and years of experience if they have.

5 Analysis and Result

We have analyzed the collected data by utilizing proper and different features of Questback and Excel for the purpose of getting clear results that everyone can understand. We have analyzed data for each question separately, with summary of each one and we have used comparison feature for question itself in order to find interesting results of data collection. We have presented the results by using different types of graphs.

5.1 Main Findings from questionnaire

Among law enforcement users, OSN is widely used for non-investigative activities with 57 % versus 43% for investigative activities. Background investigations for job candidates are top non-investigative activity done via OSN, followed by In-service training. A top investigative activity of OSN is for crime investigation, followed by listening/monitoring for potential criminal activity. Lack of OSNs skills and training is a primary reason of often non-use in investigative activities. In addition OSNs is a new scope work especially for new graduated law enforcement officers.

Identifying persons of interest, identifying criminal activity and identifying/ monitoring person of interest's whereabouts are top investigative activities done through OSN as shown in figure 4. Utilizing OSNs for investigative activities has not used obtained information from OSNs as probable cause for search warrants in Turkey. Currently, OSN is utilized by law enforcement in Turkey just as resource to obtain information that can be only used for intelligence investigations, but cannot be used as evidence in the court of law to get legal search warrant.

The other results that we obtained from the questionnaire are as follows:

- Law enforcement professionals are mostly self-taught and depend on their knowledge from use of OSNs for personal purposes, and corporation with colleagues with experience.
- There is not significant statistics for any formal training seminar or conference that was dedicated to the use OSNs in law enforcements.
- Communal OSNs, such as Facebook are most used in OSNs, followed by YouTube and Twitter. Myspace, LinkedIn, and blogs are less used.
- Top frequent crimes been encountered by law enforcement professionals during their work are, assault, burglary, child abuse, harassment, hate crime, and murder.
- There is infrequent of use of OSNs for investigative activities, approximately half of law enforcement using it less often, and half using it 2-3 times in a month- However the level of usage has grown somewhat compared to the previous year.

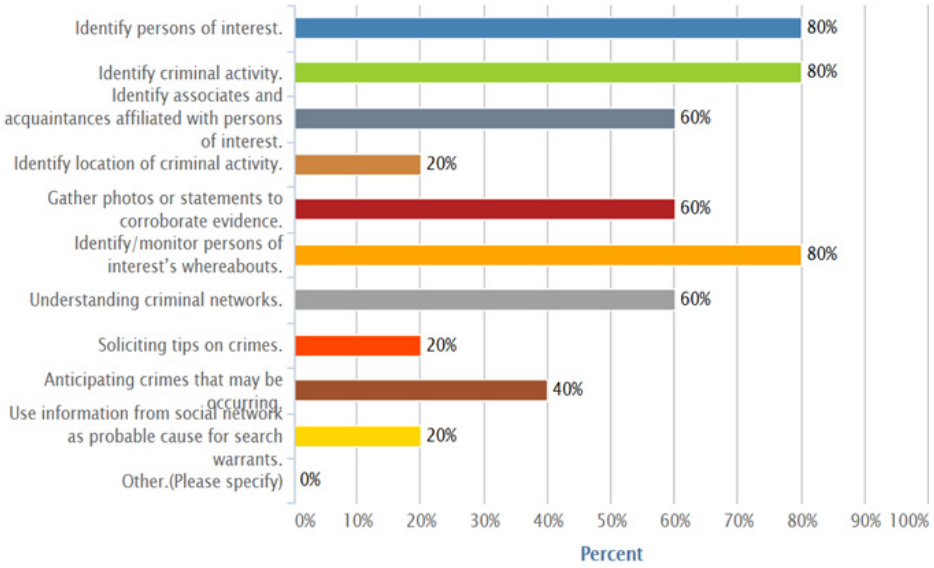

Fig. 4. Types of Investigative Activities Done via OSNs

Forensic Investigation in OSN. Establishing a relationship with the person of interest by creating a fake account is a most used approach among law enforcement to obtain user information from OSNs, followed by request to access into victim's or person of interest account from OSN provider, and request access into associates and acquaintance's affiliated account with person of interest. Photos/videos, location, groups, name are most collected data from OSN by forensics examiner, followed by linked websites, userID, list of friends, status updates, network, and chat.

More than two-third of law enforcement are not using any tools for analyzing OSN activities. Law enforcement believed that visualization is very useful feature to determine the direction of investigation and narrow down the scope of work.

Law enforcement stated that they are following these steps (Identification, Searching, Filtering, and Capturing) in OSN investigations process.

Non-users OSN in Investigations. The main reasons for not using OSN in investigations purpose are the following:

- 33% of law enforcement do not have enough knowledge to use in investigations.
- 33% lack of support from law enforcement leadership.
- 17% Unable to access during working hours.
- 17% Agency policy

Beliefs in OSNs Use

- The value of OSN in investigation will increase in future, and can significantly help to solve crimes more quickly.

- Law enforcement professionals have no worries about the ethics of creating fake profile account as an investigative method.
- Law enforcement believes that information obtained through OSN is credible.
- More than one-third of law enforcement said that they are comfortable to use OSNs, but are not able to use it to its fullest effort due to a lack of proper training. Within age interval 30-39, the law enforcement professionals are more comfortable to use OSNs, but less comfortable to use within the age interval 40-49.

6 Conclusions

The use of OSN in law enforcement agencies has entirely changed in their traditional techniques and procedures in which law enforcement professionals using it in criminal intelligence and investigative activity.

Law enforcement greatly benefited from OSNs and resources as a fruitful tool to prevent, mitigate, respond, and investigate criminal activity. The outline of our work described how criminals committed crimes by using these sites for illegal purposes, and we categorized the crimes that are involving OSNs. Forensics investigators were following two approaches in obtaining data from OSNs; collecting publicly available information of user's subscribers and cooperation with social network provider in order to obtain restricted data of any particular user. There should be transparency in sharing personal information between law enforcement of social networks companies and law enforcement authorizes.

Current approaches in which forensic examiners analyze user interaction vary depending on the types of investigation, such as private (e.g., murder, rape, kidnap crimes), national (e.g., local violence) and global (e.g., organized crime).

Majority of forensic examiners develop their own tools and software that can automatically identify, search, filter, and capture relevant information for investigation. We believe that developing a program that visualizes accurate expression of users feeling and geographically tracking how they develop these feeling in real time and possibility to compare it to time of incidents that happened, can help forensics investigators to identify and predict criminals plans for any actions that represents someone's virtual community. In connection to main findings in questionnaire we discover that primary reason for collecting information from OSNs is just only for investigations intelligence. Law enforcement did not use this information as evidence against the suspects in the court of law in Turkey. In addition to that there is a need for modification in legal jurisdictions in Turkey that can help the law enforcement agencies to use collected information from OSNs as evidence in the court of law.

To the end, OSN will increase in its popularity and usefulness for coming years, especially towards criminal intelligence and investigative activities. Therefore, to ensure that information which is being collected from OSN is vital and legal, there should be a policy on use of OSN for law enforcement and focus and articulating the importance of privacy and how to protect individual's privacy, group's privacy, civil rights, and civil liberties.

References

1. World Map of Social Networks, http://vincos.it/world-map-of-social-networks/
2. Huber, M., Mulazzani, M., Leithner, S.S., Wondracek, G., Weippl, E.: Social Snapshot: Digital Forensics for Online Social Networks. In: 27th Annual Computer Security Applications Conference, pp. 113–122. ACM Digital Library, New York (2011)
3. A Digital Forensic Investigation Model for Online Social Networking, http://www.cms.livjm.ac.uk/pgnet2010/MakeCD/Papers/2010042.pdf
4. Assault Fugitive Who Was Found Via Facebook Is Back In NY, http://newyorkcriminallawyersblog.com/2010/03/assault-criminal-who-was-found-via-facebook-is-back-in-ny.html
5. Facebook status update provides alibi, http://edition.cnn.com/2009/CRIME/11/12/facebook.alibi/
6. A Digital Forensic Investigation Model and Tool for Online Social Networks, http://www.cms.livjm.ac.uk/pgnet2011/Proceedings/Papers/m1569453211-mohd_zainudin.pdf
7. Facebook Sex Trafficking: Social Network Used To Kidnap Indonesian Girls, http://www.huffingtonpost.com/2012/10/29/facebook-sex-trafficking-_n_2036627.html
8. Facebook Sex Trafficking: Social Network Used to Kidnap Indonesian Girls, http://www.sileo.com/facebook-status-update-leads-to-robbery/
9. Burglars Use Social Media to Plan crimes, http://www.blog.littlesafe.co.uk/?p=969
10. Criminal Use of Social Media (2013), http://www.nw3c.org/docs/whitepapers/criminal-use-of-social-media.pdf?sfvrsn=10
11. Digital Crime, http://www.dcrime.com/dcrime.pdf