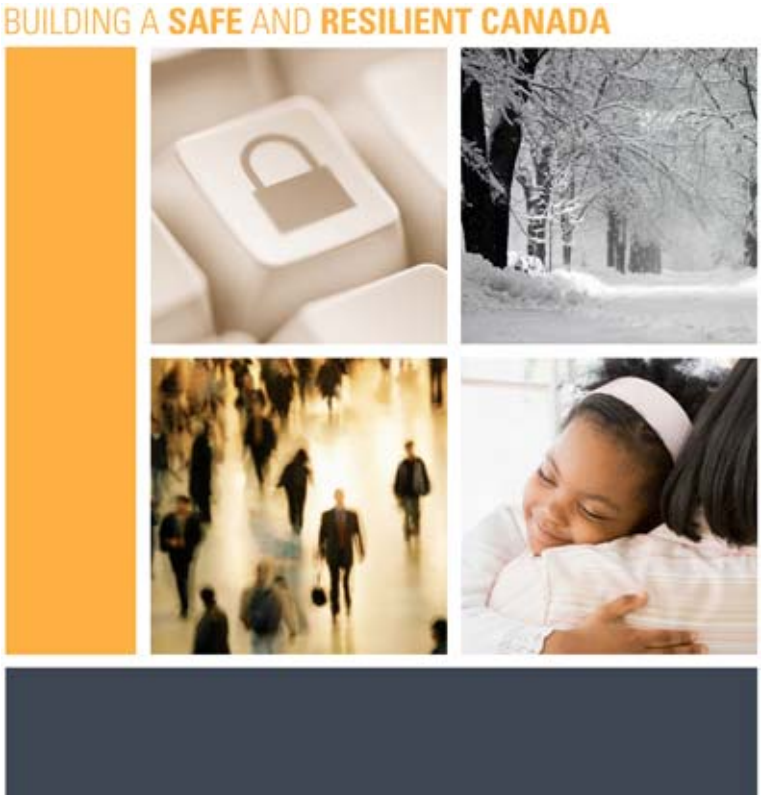
Public Safety Canada | Sécurité publique Canada



Public Safety Canada Social Media Sites:

New Fora for Criminal, Communication, and Investigation Opportunities

AUGUST 2011
RDIMS #434480

Canada

Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities

By

Dr. Richard Frank
Simon Fraser University

Connie Cheng

and

Vito Pun

prepared for

Research and National Coordination
Organized Crime Division
Law Enforcement and Policy Branch
Public Safety Canada

The views expressed herein are those of the authors and do not necessarily reflect those of the Department of Public Safety Canada.

Report No. 021, 2011

Cat. No.: PS14-5/2011E-PDF
ISBN No.: 978-1-100-19190-4

Contents

Executive Summary

Over the last two decades, rapid advances in communication technologies have significantly enhanced efficiency and information sharing. The spread of online discussion fora and most recently, social networking websites such as Facebook and Twitter, has helped rekindle and maintain connections between friends and acquaintances, facilitated the building of various online communities that share common interests, and created a new space for entrepreneurship and business transactions. Social media tools help to link people with common interests, and facilitate a wide variety of activities in the legitimate sector; it follows that such popular communication and business tools may also facilitate work in the illegitimate sector, perhaps even the work of criminal organizations. The current research complements and builds on existing empirical information regarding the use of social media by criminal organizations and law enforcement by way of literature review and interviews with law enforcement officials and social media experts.

All law enforcement respondents and social media experts indicated that law enforcement personnel and organizations have, and continue to, employ social media to connect to the communities that they serve. The goals of law enforcement use of social media as identified by respondents were to connect to and interact with the community, and to proactively monitor the community for disruptive events and activities. Respondents reflected on the challenges they faced when conducting such investigations online. These included the ability to find the correct person among the large number of online social media users, the procedural difficulties associated with acquiring private information from social media data owners, and the time consuming nature of following forensically sound procedures when collecting online evidence, particularly when it is done in such a way as to not leave behind traces of police activities.

One recurring recommendation from respondents, which also appears in the literature, is that police officers need more basic training on using computers and the Internet for open source intelligence gathering. Respondents suggest that it is important that law enforcement personnel have access to different computers, websites, and software so that they can be more fluent with them and utilize a variety of tools. Respondents indicated that law enforcement personnel need to accept that police officers will want to use online social media sites for personal reasons. But, they warned that separating police work from personal work is a mandatory requirement. They expressed concern that many police officers do not understand the danger of posting photos and personal information on online social media sites (OSMS), even if they have strict privacy settings. Some respondents suggested that a set of principles be created and followed regarding how police should and can obtain evidence and what they should (not) do to a crime scene where a computer is involved. Respondents suggested that such a guideline would allow law enforcement personnel to be more effective and consistent in gathering evidence from computers. Moreover, such a guideline may help minimize trails left by law enforcement personnel during investigation.

Most respondents agreed that persons suspected of organized crime involvement do not tend to display their illicit activities on their social media profiles, but instead use social media to keep connected to their networks. The intersections between the demographic characteristics of persons who use social media and those of persons involved with organized crime may be useful for targeting investigation and communication efforts. This comparison illustrates that, in general,

persons involved in organized crime tend to be late-onset offenders, older than those who frequent social media sites, and may perhaps be less likely to use social media. Exceptionally, the two blog sites described in this report, Blogger and Wordpress, were shown to have an older cohort of users. It is possible that members of criminal organizations, like the older general public, may be more attracted to blog sites than to Twitter, FaceBook, or MySpace, and as such may be users or consumers of such social media. Unlike the typical social media user, women involved in criminal organizations tend to be non-Caucasian, with disadvantaged socio-economic backgrounds (Beare 2010). As such, it is possible that female organized crime offenders are even less likely than their male counterparts to use social media sites.

Introduction

Over the last two decades, rapid advances in communication technologies have significantly enhanced efficiency and information sharing. The spread of online discussion fora and most recently, social networking websites such as Facebook and Twitter, have helped rekindle and maintain connections between friends and acquaintances, facilitated the building of various online communities that share common interests, and created a new space for entrepreneurship and business transactions. Social media tools help to link people with common interests, and facilitate a wide variety of activities in the legitimate sector; it follows that such popular communication and business tools may also facilitate work in the illegitimate sector, perhaps even the work of criminal organizations.

As the proliferation of social media use is a relatively new and emerging trend, there is currently a paucity of Canadian research on the utilization of social media in the commission of offences, including those perpetrated by criminal organizations. The most recent Criminal Intelligence Service Canada (CISC) report (2010) indicates that criminal organizations use technology "to communicate securely, conceal their activities, target victims, and locate skilled labour and valuable goods, such as large caches of stolen personal and commercial data." Further, the same report notes that "Some organized criminal networks are exclusively virtual with illicit activities and communications occurring entirely online." The report did not discuss which online tools facilitate these communications.

The current research complements and builds upon existing empirical information regarding the use of social media by criminal organizations by way of literature review and interviews with law enforcement officials and social media experts. This report simultaneously addresses uses of social media by law enforcement organizations. Indeed, the purpose of the current report is threefold:

1. to provide empirical evidence on how organized criminal groups are using or could be using social media tools;
2. to showcase how the law enforcement community is using or could be using social media to investigate organized crime and to undertake other police work; and
3. to provide recommendations for law enforcement professionals and policy makers on potential ways of mobilizing social media for Canadian law enforcement or crime prevention purposes.

To that end, this report describes the types of social media tools and some examples of popular social media sites. Within this discussion, descriptions of the demographic composition of the users on selected social media sites are provided. The purpose of this information is to build a foundation for a discussion of criminal, communication, and investigation opportunities available via social media sites. Following a description of the interview methodology, a discussion surrounding the use and possible uses of social media by law enforcement, as well as by criminal groups is provided. Conclusions are offered along with some thoughts on future research directions.

Description of Social Media Tools

There is a wide variety of social media tools currently available on the Internet. These social media tools can be categorized into microblogs, blogs, web-forums, social bookmarking sites, social networking sites, media sharing sites, and virtual content sites. These types of sites are described in brief below.

- **Blogs**: A short-form for web-log, these websites facilitate the sharing of regular entries detailing information about individuals' own lives, as well as commentaries on specific topics or events. Entries made on blogs can contain photos, audio or video.
- **Microblogs**: These services, such as Twitter, allow users to blog, but only using limited amounts of content, such as short sentences or links to other places. People can then respond to the posts of others, or re-post something if they so wish.
- **Web-forums**: An online version of a discussion room, but where the conversation can be viewed for a period of time. Web-forums categorize each discussion into a "thread", a chronological discussion on a topic where each person can reply to any previous posts. The forum is organized into a hierarchy of sub-forums, which usually contain a specific topic(s).
- **Social bookmarking sites**: These sites do not facilitate the trade in files or other forms of media, but in references (or "bookmarks") to resources (i.e., links to media, files, or web pages). Each bookmark can be categorized under a number of topics. The social aspect of this type is the user's ability to vote about the quality of a bookmark or comment on it.
- **Social networking sites**: An online site whereon social relationships between users with similar interests or friends can be established and shared. Each user may have a profile on which they can put content about themselves and in this sense keep their network of friends updated on their activities. The most popular social networking site is Facebook.
- **Media sharing sites**: These sites typically allow for the sharing of audio, video, photos and text with others. After sharing media with others, users are invited to comment, respond and react (perhaps by sharing another piece of media). The most popular example of this type of service is YouTube.com.
- **Wiki Sites**: Wiki sites can look like any other web page, with the difference being that these sites are created, edited and maintained by a collection of users who volunteer their time. The most popular example of this type of site is Wikipedia.
- **Virtual World Content Sites**: These sites are not websites *per se*, but online communities that can interact via a computer-simulated virtual environment and users represented by avatars. A popular example of this is Second Life.

The above listed categories are not mutually exclusive. For example, FaceBook could be considered a social network site, a status-update service and a media-sharing site, while it also incorporates social bookmarking tools and applications that could be considered virtual world content. This paper focuses on blogs, social networking sites, microblogs and media sharing sites. In order to understand how police and criminal organizations are or could be using social media, it is first important to understand the popular social media tools and the demographic characteristics of its users. By understanding the demographics of social media and its users, more insight could be drawn concerning potential victim demographics and potential methods organized criminals

can use to achieve their goals. As such, several popular social media tools that are popular among Internet users were chosen for this report. These social media tools are described below.

Twitter

The Twitter service, available at www.twitter.com, was launched in 2006 and has since become the de-facto standard in microblogging. Users can post text-based messages known as "tweets", each containing up to 140 characters. Currently, it is estimated that 190 million users generate 65 million tweets a day on Twitter. The service can be used to share images, audio, or video but only if it is from a third party supported website (such as YouTube or Twitpic). Users can access Twitter to view new tweets or send out their own tweets via SMS, instant messaging, or applications on smart-phones. Cheng and Evans (2009) looked at the links between the users of Twitter and concluded that only 5% of Twitter users had more than 100 people following their tweets, 5% of all users generated approximately 75% of the tweet traffic on Twitter, while of all accounts, 20% were inactive.

Blogger

Blogger is a blog publishing service launched in 1999 which allows users to post time-stamped entries, such as text, photos or videos. Widely used as a mainstream medium to express opinions and linkage to other materials on the Web, weblogs have become a very popular method of communication (McIntosh 2003). Blogger was created by Pyra Labs, which was bought by Google in 2003. In the US, approximately 53 million users access weblogs on Blogger every month. In an analysis of 100 million random blogs done by Jasra (2010), the country with the largest number of blogs was the US (29.22%), whereas 3.93% of blogs originated from Canada (the US population is roughly 10 times the size of the Canadian population, so this web-presence is comparable).

WordPress

WordPress, unlike many blog hosting companies, offers an open source[1] content management system (CMS) to its users. The CMS, an application for managing and creating content for a website, provides templates and also allows users with basic coding knowledge to freely create new designs or adopt the templates; therefore, users may freely customize their own web pages or blogs.

Facebook

Facebook is the most popular social media network around the globe today. It has a global audience of 600 million users (CheckFacebook.com 2011). Even though Canada only accounts

[1] Open source is a term describing a development and production philosophy where the source material is publicly available for further modification and distribution.

for 2.82% of Facebook's population, this represents 16 million users on Facebook in Canada, 53.8% of whom are female (CheckFacebook.com 2011; Litwinka 2010). Whereas other social media sites may target specific demographic groups, Facebook seems to appeal to a variety of age groups in Canada, with the largest population of users being between the ages of 18 and 34 (53%) (Litwinka 2010). There is a significant population of 606,000 (3.6%) of Canadians over the age of 65 on Facebook and over 1.4 million teens between the ages of 14 and 17.

MySpace

MySpace, owned by News Corporation, became the largest social network in North America in June 2006, but lost that crown to Facebook in April 2008 (Techtree 2008). The site is primarily aimed at youth and provides the opportunity to relate to brands, bands, meet other friends and other entertainment media. Probably due to these redesigns, the demographics of MySpace have changed since its inception. The site has reportedly given up competition with Facebook (Ostrow 2010) and has now morphed itself into a service focused on music and young people (Oreskovic 2010). Many of its users come from North America, most from the US. More recently, however, an estimate of MySpace traffic in Canada indicated that there are only 830,000 users are accessing MySpace per month (Google, Inc. 2011). As of March 2010, MySpace.com received 28.6 million visitors per month.

Flickr

Flickr is an image-hosting online community that has captured a great deal of attention from image enthusiasts, photographers, and technologists. It allows each user to upload photos into their own photo-albums and then manage the albums and the photos contained in them. Friends can then view the photo-albums and comment on the contents. There has been a decline of web traffic since 2008 whereas other social networks, such as Facebook, continue to grow.

YouTube

When the site launched in 2005, it introduced the ability for average Internet users to upload and share videos with each other, and has since facilitated the embedding of videos onto other websites. Through YouTube, Internet users everywhere can view and share videos with each other. Registered users can create "channels", to which other users can subscribe in order to get notifications of newly uploaded videos. Each video can be restricted so only specific people with direct links to the videos can view them. The site and the videos on it are accessible via multiple devices such as computers and smartphones (Google, Inc.(b) 2011). It is currently the largest video sharing site on the Internet, with 2 billion videos watched and hundreds of thousands of videos being uploaded daily (Youtube.com 2011) by its 123 million monthly visitors. After watching a video, other users can comment on and rate each video, or respond via other videos that they upload.

The Overall Demographic Landscape of Social Media

The demographic summaries of each social media brand are based on statistics created by Quantcast.com.[2] Demographic statistics for each social media site were only available from the United States. In terms of unique monthly visitors, Facebook dominated the rankings list, second only to Google. Of the social media sites discussed in this report, Facebook also had the most number of visitors, at 134 million people per month.

Different age cohorts are attracted to different social media brands; MySpace has a much younger population (71% are between 13 and 34 years old), than Wordpress (69% between ages of 18 and 49), or Blogger (72% between ages of 18 and 49). This could indicate that the younger demographic group tends to favour MySpace, whereas the blog-based sites are utilized by older users. The bulk of the people visiting these sites are between the ages of 18 and 34, the age group that was largest for every social media site included in this analysis. With respect to sex differences, all social media sites are relatively evenly split between male and female users (50% and 50%).

According to Quantcast.com, the vast majority of users of social media, at least 65% in all cases, are Caucasian. Hispanic and African American persons were the second and third most represented user groups, respectively. It is expected that the distribution of users within Canada would be different based on differences in the demographic composition of Canada.

Quantcast.com measures the expected income of the visitor through statistical inference. In all cases the visitor likely earns more than $60,000 per year; more than 50% of the visitors to all social media sites were in this expected income range. This income range is not representative of the average Canadian: the average family earns $91,500 per year and the average unattached person earns $37,800 per year (Gerlsbeck 2009).

Persons with different educational backgrounds were attracted to different social media sites. MySpace had the highest proportion of users without a college degree. MySpace users are also younger than the average user, which may have impacted on this statistic. WordPress and Blogger were the only two sites where the population-segment with a college degree outweighed those without a college degree.

---

[2] Quantcast.com creates demographics statistics by tracking what the user does on each website (for example download an MP3, respond to an ad, play online game) and how they move from one website to another. From this, they build a "Visit Graph" which "analyzes the dynamic relationship between Internet media audiences and their interactions with a comprehensive set of digital media assets, which includes websites, blogs, video, widgets and advertising campaigns" (Quantcast 2008). The main goal behind this type of demographic calculation is to understand the visitor to the site better, and serve them advertisement that they will find relevant. According to Technology Review (2010), Quantcast measures and analyzes the audience statistics with the use of complex machine learning techniques. As of 2008, they were using more than 1 trillion observations to build their models (Quantcast 2008). By 2010, they had statistics from information 1 billion Internet users Technology Review (2010). Quantcast was ranked the third most innovative company on the web in 2010 (Fast Company 2010). Although several other companies exist which offer similar services, the same company (Quantcast) was used for all demographic information in order to maintain the integrity of the demographic comparisons.

Overall, the different demographic details presented by Quantcast.com are consistent: MySpace tends to have a younger and less educated audience, whereas blog sites tend to have a more educated, older audience. The other included sites were fairly evenly distributed across the remaining identified demographic variables considered for the purposes of this report.

Methodology

In order to address the project objectives, a literature review and a series of interviews with law enforcement officials and social media experts were undertaken. Different interview guides were customized for the different groups. The interview guide for both groups included questions related to the following themes:

- advantages and challenges related to the utilization of social media for law enforcement investigation purposes;
- how social media is being employed to facilitate criminal activity by criminal organizations;
- best practices for law enforcement professionals regarding the use of social media tools for investigative and other purposes; and
- recommendations for law enforcement professionals and policy makers on potential ways of mobilizing social media for Canadian law enforcement or crime prevention purposes.

The convenience and snowball sample started with three known experts in the law enforcement community, and resulted in interviews with a total of 11 respondents. Each respondent had a background that made them well-suited to discuss the stated interview themes. Ten interviews were conducted (one interview was attended by two respondents), completed between February 15 and March 1, 2011.

The law enforcement sample included four police officers who specialize in computer-related crimes and investigations conducted via the Internet. One respondent was from the United Kingdom, and the remaining three respondents were from municipal, provincial, and federal Canadian police forces. In addition, three respondents were instructors who specialize in the realm of open source intelligence investigations (investigations using publicly available information on the Internet). The law enforcement sample also included respondents working in the private sphere: one interview was with a private investigator who specializes in open source intelligence investigations, and another interview was with a person who is involved with computer-based security, including investigating and protecting against cybercrime.

The social media expert sample was small, and consisted of a civilian who works full-time "mentoring" police officers on their use of social media and a vice president of a Canadian social media service.

Use and Possible Uses of Social Media by Law Enforcement

The use of online social media sites (OSMS) has grown at a very fast pace over the past few years, and although many studies show how the general public uses these services (Marsico 2010; Cheng 2009), there is only a small literature on how these services can be used to commit and fight crime. Yet, common investigative practices have been adopted by law enforcement officers around the world. For example, the Police Services of Northern Ireland have used Facebook as a tool to conduct local surveys to learn more from its citizens (Alderson 2011). In Canada, the Royal Mounted Canadian Police (RCMP), and police departments in Victoria, Vancouver, and Toronto all have Facebook pages.

Several themes emerged from interviews with respondents regarding potential uses of social media for committing crime, investigating crime, and communicating with the public. Those themes were categorized into the following broader themes: connecting with communities, information gathering, investigative challenges, and recommendations from respondents.

Connecting with Communities

All respondents agreed that law enforcement officers have, and continue to, employ social media to connect with the communities they serve. This finding may reflect bias of the sample.

Respondents were asked whether their department or organization had a goal or goals it was aiming to achieve through its use of social media. The organizational goals articulated by respondents were similar. Respondents cited connecting and interacting with the community, and proactively monitoring the community for disruptive events. One respondent indicated that a rave (a type of party that typically involves dancing, music, and can involve drug use e.g., ecstasy, methamphetamine, and other stimulants) was monitored and controlled through intelligence from Facebook.

Next, respondents were asked to describe how they or their team work(s) with social media for engaging with the public. As noted, the Toronto Police Service (TPS) is active on Facebook; it is also active on Twitter and YouTube (Masterman 2010). One respondent suggested that OSMS enabled the TPS to have more contact with people that do not access traditional methods of community engagement. Further, this respondent suggested that OSMS allow the police to engage with younger and different people than they traditionally have access to. At the same time, it was also suggested that information posted on the OSMS may facilitate the reporting of crime by young people who are looking for something positive to do.

To draw a parallel from information available on police use of social media, the Police Service of Northern Ireland also created a trial Facebook page, and conducted a study to understand public opinion about the police agency after the page was launched. Of those who participated in the study, 85% thought that the Facebook page provided a platform for citizens to participate and get involved in making the neighbourhood a safer place; 83% thought it increased the appreciation for police activity; 82% thought that the information provided on the site facilitated crime prevention; 75% stated that the police service improved after the page was launched; and 70% stated that their confidence in local police had increased. Interestingly, increasing public confidence in law enforcement can decrease fear of crime (Skogan 2009), but also increase crime awareness as well. Using OSMS, police can now instantly deliver local crime appeals and prevention advice.

When asked to describe how they or their team work(s) with social media for engaging with the public, two respondents stated that police engagement with social media can help in the delivery of emergency instruction, traffic updates, special event promotion and asking for aid in the search of missing people. A law enforcement respondent from the UK stated that they regularly use Facebook and Twitter to interact with the community in other ways, such as setting up a book of condolences for lost officers and performing consultations with the public (which were not well attended when done through offline consultations, but were a huge success when done online).

In general, respondents agreed that the more interaction law enforcement can gain with the community, the better that relationship will be. By providing more opportunities for citizens to interact with the police, such as uploading the newest information on a profile page that members regularly visit, respondents suggested that citizens may be more likely to come for help, as well as provide useful tips for crime-solving. According to respondents, the only way to benefit from OSMS is to educate the police and the public about the use of these services so they are used to their potential.

Information Gathering

Respondents were asked to speak to how they or their team work(s) with social media over the course of an investigation, particularly for investigations of organized crime, and to provide a concrete example of how an investigation was assisted by the use of social media tools. Two respondents did not agree to speak about specific strategies for investigation, citing security concerns. Of the rest, five indicated that they had used social media during investigations into organized crime and all had experience in intelligence gathering for non-organized crime related offending.

All respondents from the law enforcement sample indicated that they now often begin investigations by opening up a web-browser and gathering online information. While both online and offline investigations have their places, a lot of information can be gathered from public sources, an activity called Open Source Intelligence (OSINT) gathering. Describing OSINT, one respondent stated:

> OSINT is about searching for information accessible to the public, but finding the information that the public does not know how to obtain, and analyzing it in a fashion the public doesn't know how to analyze.

Taken together, the respondents painted the following picture of a typical OSINT gathering exercise. First, an individual, or group of individuals (referred to simply as a suspect hereon) is identified. The suspect's profile is sought on multiple OSMS in the hopes that the suspect is available on at least one. The suspect's network of friends, co-workers, collaborators and relatives is built based on his linkages to other individuals or organizations (including gangs) on OSMS. At the same time, information specific to the suspect is collected, such as phone numbers, aliases, age, city, and nearest intersection or addresses frequented. This information can be derived from GPS-coordinates embedded in photos, for example. Some individuals make this information private on the OSMS sites they frequent. Police officers and private investigators can

attempt to befriend such individuals using fake accounts in order to try to infiltrate the network of the suspect. Fake accounts can be long-term efforts, with the goal of gaining enough connections with the suspect to earn their trust. Once sufficient information about the suspect is collected, the individual, or members of the network, can be charged by law enforcement.

Once an investigator has established a connection between themselves and the suspect, this connection might not actually lead anywhere since, according to two respondents, suspects do not tend to use OSMS to discuss crime, but will join OSMS for the same purposes that the general public will: to keep up with friends and family. Thus, in order to gain some useful information, sometimes the focus of the online aspect of an investigation can be on the network of the suspect, including as girlfriends, family members, and close acquaintances. One story shared by an OSINT instructor illustrates the value of monitoring the network of a suspect: a Mexican drug cartel's leader was found and arrested because his location was determined due to the police monitoring his girlfriend's Facebook account when she used it to keep in touch with her friends and family.

It is clear from the interview responses that intelligence can be gathered from unexpected resources. For example, one respondent mentioned they will look for a suspect's presence on genealogy sites[3] because, according to his experience, offenders tend to have relatives who are also offenders. Further, some sites allow users to identify their hobbies, which can lead investigators to, for example, clubs and associations the suspect attends. Knowing a suspect frequents a specific location can lead to linkages with friends of the suspect, or allow law enforcement personnel to find the suspect at the club.

Respondents noted that intelligence can be unintentionally shared by the suspect on OSMS. For example, one respondent pointed out that modern phones have GPS built in, and if a suspect posts a tweet, the message will have the location embedded into it, allowing law enforcement personnel to track the suspect. Also, as previously noted, according to one of the respondents the metadata contained in images posted to OSMS can be used to establish a location via GPS coordinates. Images can also be used to quickly find the same person in other images using face-recognition software (such as that built into the free Picasa software by Google).

Although all respondents expressed that OSINT gathering is an integral part of the investigations, respondents from the law enforcement sample indicated that sometimes their investigations were limited by the policies of their organizations. One respondent stated that their organization fully supports investigations through OSMS, and encourages staff to use OSMS for both private and work related use (subject to controls on time and appropriateness) because their specific goal is to ingrain OSINT into their business and daily activities. Another respondent indicated that their organization had the same goal in theory, but that restrictions on the equipment available for work use tempered their ability to use OSMS to the extent of their abilities. An unavailable tool in some organizations, for example, is Mozilla Firefox (an Internet browser) which was mentioned by four respondents as the browser of choice for OSINT gathering due to available plug-ins that can significantly reduce the effort of the investigator.

[3] Genealogy websites allow the user to construct family trees depicting their ancestry, lineage and history.

Challenges Regarding the Use of Social Media for Investigative Purposes

Respondents were asked to discuss some of the challenges related to engaging with communities using OSMS. According to one respondent, some police inappropriately use social media as a broadcast medium. Social media are *social mediums*: the purpose or benefit of social media is not to broadcast messages from, for example, law enforcement authorities to the community, but rather to facilitate interaction and community building between people and organizations. In addition, although law enforcement personnel may initiate discussions via social media, respondents suggested that community involvement will vary.

Respondents identified a number of very significant challenges hindering the OSINT process. First, according to all respondents, most law enforcement officials lack: basic knowledge of computers needed in order to ask the right questions; skills in Internet-based investigations; and awareness of the amount of personal detail they leave behind during a digital investigation. According to the respondents who instructed OSINT classes, police do not tend to have an IT background and are not as fluent in social media as they could be. Most respondents agreed that technology is changing at a fast pace, and that police need to take advantage of the newest technology, as more illegitimate opportunities will present themselves on these fora. Although officers may receive training to adapt to the latest telecommunications and IT, their learned skill set will diminish over time if not used. Moreover, respondents highlighted that it is difficult for investigators to stay in touch with changing technologies, as well as retention schedules, legal processes, and their other regular police duties.

Among officers who possess the necessary skills, another challenge present in online investigations was underscored by respondents: ensuring that a specific profile actually belongs to the suspect in question. Most respondents expressed difficulty of finding the correct profile for a suspect. For example, an informal search of a common name on Facebook can easily yield more than 200 matches. Without more details on the suspect, an exhaustive search based on name only is extremely time consuming, or even futile, unless the name happened to be extremely unusual. Names can also be obfuscated due to misspellings, nick names, different languages, aliases or other factors. Thus, the search has to be complimented by using as much specific information as possible, including phone numbers, street names, nearest intersections and/or nearest subway stations. According to the respondents who described this process, once the suspect has been identified on a single OSMS, new information can be learned which can then be utilized for further investigative purposes and to create a more detailed picture of the suspect and their network.

Another challenge noted by respondents concerns the strict privacy sharing policies of some OSMS. Respondents noted that popular sites like Twitter and Facebook are willing to provide access to the information of an account holder only when a search warrant is supplied. Facebook even has a guide for law enforcement personnel on how to request user information. Moreover, since most OSMS reside outside of Canada, mutual legal assistance treaty applications must be prepared to access legal information on targeted accounts for use in court. Respondents indicated that it can take as long as six months to receive requested information due to the processes

involved between two countries. Further, respondents note that evidence collection from these services is a challenge. All evidence must be captured according to forensic standards: website content must be generated into a static PDF document, and screen shots must be captured in case of a discrepancy between the actual content layout and the PDF. All of this requires resources, time, and effort to properly process. One of the OSINT instructor respondents notes that it is very important for police to understand the legislation associated with information gathering in order to present relevant evidence in court.

As an exception to the rule, there are some social media sites that choose to aid in investigations by responding quickly to requests from law enforcement, even without a warrant, such as the Canadian social network site of one respondent. As stated by the respondent, "the police must have a reason for asking" so they usually will comply without a warrant.

Finally, one respondent was concerned that the use of OSMS can pose a danger to police officers. This concern is supported in the empirical literature: Weimann has found that offenders are continuously monitoring online services to gather information on law enforcement (2010). Police officers are advised to keep personal and business separate by discouraging officers to use OSMS for personal use, particularly on their phones (due to GPS capabilities). Police are strongly advised to not post pictures, especially recent pictures, and to ensure that friends do not post information about them. According to one respondent, if an officer's information can be easily found online, they may not be able to get an undercover job, and their credibility as a police officer may be attacked in court.

Recommendations from Respondents

Respondents were asked to share their recommendations for law enforcement use of social media services. One of the recurring recommendations, which also appears in the literature, is that police officers need more basic training on using computers and the Internet for OSINT. This suggestion was shared by practically all respondents. Having general, up-to-date knowledge of how to effectively use the Internet aids in the investigation of possible suspects, according to one respondent. Four respondents agreed that a set of principles should be created and followed regarding how law enforcement personnel should and can obtain evidence and what they should (not) do to a crime scene where a computer is involved. Respondents suggested that such a guideline would allow law enforcement personnel to be more effective and consistent in gathering evidence from computers. Moreover, such a guideline may help minimize trails left by law enforcement personnel during investigation.

Respondents suggest that it is important that law enforcement personnel have access to different computers, websites, and software so that they can be more fluent with them and utilize a variety of tools. The respondents who instruct OSINT courses indicated that most of the courses they are teaching are tailored towards this need, but the courses only last a few days. They recommended that all law enforcement personnel attend these courses periodically. Indeed, that is what seems to be happening. All of the instructor respondents noted that their courses are all wait-listed with people from all jurisdictions and positions trying to attend. Respondents indicated there may be a problem on the supply side, and suggest that a prudent course of action may be to increase the availability of these courses to meet the increasing demand.

Most of the law enforcement sample mentioned that law enforcement personnel need to accept that officers will want to use OSMS for personal reasons. They warned that separating police work from personal work is a mandatory requirement. They expressed concern that many police officers do not understand the danger of posting photos and personal information on OSMS, even if they have strict privacy settings. Participating in OSMS can eliminate their future chances of undercover work, as well as endanger themselves, their relatives and friends. Individuals can gather information on police officers through the same means law enforcement personnel employ to gather information on suspects. Respondents suggest that policies be drafted that carefully detail the activities law enforcement personnel can and cannot engage in online in order to eliminate the shades of grey when it comes to participating on OSMS.

Use and Possible Uses of Social Media by Criminal Organizations

There is considerable debate in the academic literature surrounding organized crime about what constitutes a criminal organization. A wide variety of terms have been applied to describe groups that participate in organized crime activities, including "Mafia, outlaw motorcycle gangs, triads, car theft rings, criminal gangs, hate crime groups, youth gangs, urban gangs, rural gangs, ethnic gangs, girl gangs, drug trafficking gangs, aboriginal gangs, terrorist cells and delinquent youth groups" (Wortley 2010, 5). These labels are based on demographic characteristics of the group, as well as their particular criminal activities. For example, gangs are differentiated from criminal organizations in some literature, with the former often characterized as younger and/or less organized. Definitions of organized crime tend to vary, reflecting local circumstances and needs (Wortley 2010, 5). Recent literature based on social network analysis suggests that criminal organizations are rather flexible, loosely structured, and comprised of many small networks (Morseilli, Gabor and Kiedrowski 2010, 9), contrary to their depiction in popular media. A criminal organization is defined by the *Canadian Criminal Code* as meaning

> a group, however organized that is composed of three or more persons in or outside Canada and has as one of its main purposes or main activities the facilitation or commission of one or more serious offences that if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any of the persons who constitute the group.

For the purposes of this report, a broad definition of criminal organization has been adopted, including loosely based criminal networks.

People involved in organized crime have been described as "self-organizing and emergent in settings where there are ample vulnerable opportunities to seize and interact across a variety of cross-border, cross-market, and cross-industry settings" (Morselli, Turcotte, and Tenti, 2010, pp.10). According to Routine Activities Theory, opportunities for crime will occur where a victim meets with a motivated offender in space and time without a capable guardian present (Felson and Clarke 1998). Both trusting victims and a lack of capable guardians are present in the space of online social media services. As stated by one respondent, "Among all categories of crime,

cybercrime is the most popular because the risks are very low and the potential gains are very high."

Respondents were asked how criminal organizations are and could use OSMS. For the purposes of analysis, their responses were divided by theme: connecting and (not) recruiting via social media, coordinating criminal activities via social media, and victimization via social media. The interview responses were paired with information from academic literature and from the news media to provide a clearer picture of the topics discussed by respondents.

Connecting and (Not) Recruiting via Social Media

Online social media sites (OSMS) create opportunities for people to interact with other people and organizations all over the world. Many people involved with organized crime recognize the "risk of having their real identity tied to their online personas" and as such are reluctant to use OSMS as communication tools (Weimann 2010, 48). One respondent indicated that many well-known criminal groups, such as the Hells Angels, can easily be found online because they use OSMS. This statement is supported by research done by Morselli and Décary-Hétu (2010), which found the presence of well-known criminal groups such as the Crips, Hells Angels and Latin Kings on major OSMS based on using keyword searches of Twitter, Facebook and MySpace. A respondent who is a cyber-security investigator indicated that members of the Hell's Angels do not discuss crimes online. The respondent indicated that the Hells Angels use OSMS to promote their organization by supporting the outlaw biker subculture; the group does not publicize involvement in illegal activities on OSMS. Although details could not be released, a respondent from the law enforcement sample alleged some prominent members of street gangs do use OSMS. They use it to socialize, and very rarely expose or discuss details related to criminal activities. These findings also concur with previous research done in the area of "cyberbanging" (Morselli and Décary-Hétu 2010).

Unlike previous research (Morselli and Décary-Hétu 2010), two respondents from the current study indicated that gang members use OSMS for such activities as intimidation of other gangs and individuals, committing fraud, and gang recruitment. Either by recruitment or gang subculture promotion, some respondents agreed that OSMS could be used by criminal organizations to more effectively recruit and grow their operations by reaching out to a wider audience.

Recruiting via social media is more evident in the context of terrorism. For example there were over 100 propaganda videos uploaded by a Liberation Tigers of Tamil Eelam, a YouTube user in 2009, and the most recent videos were even dubbed in English or with English subtitles. Research shows that videos containing terrorist-promoting material are spreading far, which may contribute towards the growing of their support base beyond the Middle East and North Africa (Weimann 2010).

Coordinating Criminal Activities via Social Media

There is evidence to suggest that OSMS had long been used for the purposes of planning and organizing criminal activities. A report released by United State Army's 304th Military Intelligence Battalion mentioned that OSMS, such as Twitter, could become "an effective coordination tool for terrorists" to launch attacks (Weimann 2010, 48). The instantaneous update capabilities allow people involved in terrorism to organize more precise attacks by facilitating real-time updates. Weimann (2010) indicated that 90% of the terrorist activities carried out on the Internet are organized through social networking tools. In addition, one respondent indicated that in Mexico YouTube is a powerful advertisement tool for glamorization of organized criminal offending and for delivering threatening message to law enforcement and drug cartels.

Although not discussed by the respondents, there is evidence of virtual criminal network activity on Web forums and on Internet Relay Chat (IRC) channels (see, for example, Smyth 2011).

Victimization via Social Media

Of all the reports of cybercrime sent to the FBI's Internet Crime Complaint Center[4] (Internet Crime Complaint Centre 2010), the most common type of complaint is fraud: 8 of the top 10 types of crime reported to the Internet Crime Complaint Centre were a type of fraud. Of all fraud victims, 70% were victimized through online activities (Internet Crime Complaint Centre 2010). Traditionally fraud was committed by individuals working alone (Kapardis and Krambia-Kapardis 2004). This has changed significantly, with much fraud committed through spamming, phishing and scams. For example, a very common example of a contemporary scam is the "Nigerian 419 advance fee fraud scam letter" (Buchanan and Grant 2001).

The following is one example of such a scam. Large sums of money are supposedly available for inheritance, but need to be relocated to another country and require advance-fees in order for them to be moved. The victim who assists with the transaction would share in the inheritance. Processing fees, which the victim is asked to pay for, delay the transaction and further fees follow. Some details were shared by one law enforcement respondent who investigated such a scam. The investigation showed that a 419-scam email was sent out from West Africa which targeted people from all over the world. Anyone who responded to the email was transferred to co-offenders in Canada for further communication. Any fees that were sent by the victim were sent into China. Any money that was received was transferred from China to Canada, then to the United Kingdom and finally to Africa. These scams are usually perpetrated by Nigerian Crime Enterprises (NCEs). These criminal organizations are not hierarchally structured (Buchanan and Grant 2001). Like many contemporary criminal organizations, NCEs do not exhibit a clear line of authority or communication, but are created and connected according to convenience, skill set and profitability. The members of this scam met on an Internet forum where participants are ranked by their colleagues based on previous experience.

[4] Although run by the FBI, it accepts complains from anywhere in the world.

Another common type of fraud identified by the Internet Crime Complaint Centre was online dating fraud, also called the 'sweetheart swindle'. With this type of fraud, scammers will find a victim on a popular dating site, approach them and start a romance. The eventual goal is to trick the victim into believing that there are mutual strong feelings between them, possibly over long periods of time, before trying to get money from them in the form of gifts or loans. This type of fraud takes advantage of romantic feelings, rather than the promise of financial gain, to defraud funds ($3,000 on average) from the victim (Rege 2009). While some of these scams are perpetrated by individuals, some are operated in a fashion similar to the Nigerian 419 scams. The network tends to be flexible and hires members as needed. Certain people would be responsible for setting up fake profiles on online dating service sites. To initiate the contact with potential victims, other members (called 'communicators') would work in cyber-cafes overnight so they could extract thousands of American email addresses and send each a fraudulent email written by members (called 'executors') of the same organized crime group who could speak foreign languages in order to compose proper letters/emails or speak on the phone. 'Money movers' handled the money, while 'crossovers' supplied the criminal organization with legitimate governmental/financial/commercial material, such as official letterheads, in order to make the scam look official. According to Rege (2009), this scam network received seven replies each day, with each having a 70% chance of generating money.

Some professional burglars monitor Facebook accounts to search for potential victims who are on vacation, so they can identify opportunities for burglary. For example, a woman was burgled after one of her friends saw her Facebook status stating she would be at a concert that night and broke in; the burglar was caught after someone on Facebook recognized the burglar in the video footage of the robbery (Indiana News 2010).

Creating a better profile, and gaining the trust of targeted victims is much easier than before the advent of OSMS because of the enormous amount of personal information and photos shared, according to two of the respondents. This finding corresponds with the empirical literature (Timm and Perez 2010). People are able to utilize this information to convince victims that they are their acquaintance and to extract information from them for financial gain. The case of Bryan Rutberg can well illustrate how cyber criminals exploit the information from OSMS for the purposes of scamming.

Rutberg's Facebook account was hijacked and the scammer posted the status "BRYAN IS IN URGENT NEED OF HELP!!" (Timm and Perez 2010). Following the status, the scammer sent out emails to Rutberg's Facebook circle of friends stating that Rutberg was robbed while he was in U.K., and he needed money to get home (Timm and Perez 2010). Several of Bryan's friends suffered financial loss due to this incident because they believed the story and sent money. A similar incident also happened to at least two different people – Paul Emile d'Entremont and Scherrman, (CBC News 2011; Daily mail reporter 2008). In the case of Paul Emile d'Entremont, the scammer found out her husband's name through a Facebook connection and used his name to gain d'Entremont's trust. Scherrman's scammer went further to have someone pose as an immigration official with an English accent, and called Scherrman to send more money in order to release her friend from detention.

In addition, the application and newsfeed sharing built into OSMS can be used to spread unwanted malware, allowing phishing attacks to happen faster than ever (Timm and Perez 2010). According to one respondent, the only challenge facing people who want to use social media for illicit purposes is to create something that would appeal to what people want, or to create material people would sympathize with. In fact, a group of Brazilian identity thieves who used banker Trojans to steal information for identity theft and financial gain used Twitter as a platform to create a botnet[5] (Timm and Perez 2010). The perpetrators posted commands as status updates and sent them to all the subscribers, making them the bots in the botnet. Similarly, a group created a new type of botnet – the Puppetnet, using the Facebook Application Program Interface (API) (Timm and Perez 2010). The attackers created an application that, once the viewer clicks a link in the application, it would launch an attack from the viewer's browser to the targeted computer.

As for spreading malicious software, the Samy worm was able to infect more than 1,000,000 user profiles on MySpace within 24 hours (Timm and Perez 2010). It started with Samy's profile which contained a malicious code that could alter the visiting user's profile. Once a user viewed Samy's profile, the code would force the viewer to add Samy as "friend" and posted a tag stated "but most of all, Samy is my hero" (Timm and Perez 2010). The code spread as users viewed the infected pages, spurred there by "recommendations from their friends", who were victims themselves. Facebook also suffered from a similar malware attack in 2009 (Timm and Perez 2010). A vulnerability in the Facebook API allowed malicious code to collect users' personal information without the user knowing it.

Discussion

There is a dearth of research on the demographic characteristics of persons involved with organized crime (Van Koppen 2010). According to research by Motiuk, convicted offenders affiliated with gangs in the Canadian context are mainly male (98%), non-Aboriginal (95%) and range from age 19 to 64 years. The average age for gang affiliated convicted offenders in this dataset at the time of study was 36 years old. The majority had a prior criminal record as an adult (85%), with more than two-thirds having served prior provincial terms, and approximately 25% having served prior federal terms (Motiuk and Vuong 2005). Due to the lack of studies on the demographics of persons involved with organized crime in Canada, Dutch organized crime group demographics are also studied to shed light on demographics of organized criminal offending.

Van Koppen et al. concluded that the average age of persons involved in organized crime was 38 years at the time when the offence occurred, and indicated that 70% were between the ages of 30 and 50 years. The sample only included one juvenile offender. Van Koppen et al.'s research suggests that persons involved in organized crime are generally experienced offenders, as on average, many of the older offenders had committed their first offense approximately 26 years ago. The sample of offenders stayed criminally active for an average of 12 years before being convicted of an offence. Indeed, the majority of the sample was comprised of adult onset

[5] A botnet is a network of computers infected with malicious software that is controlled, often without the knowledge of the computer owner, to perpetrate acts (e.g., spamming).

offenders – offenders who do not start committing crimes until they have reached adulthood and whose criminal activities peak at age 40. Their primary activities were illegal trafficking of various products, including drugs, humans, automobiles and firearms.

With respect to the sex of gang affiliated convicted offenders, the vast majority (98%) were men (Motiuk and Vuong 2005). Beare (2010) provides an overview of women involved with organized crime in Canada. According to her research, women who are convicted of organized crime-related offences have typical female offender demographics: they are non-Caucasian, with disadvantaged socio-economic backgrounds and have extensive histories of being victims of abuse. Although Beare suggests there is an increasing amount of women who are taking leadership roles in organized crime, women represent only a minority of the population of offenders who are convicted.

The intersections between the demographic characteristics of persons who use social media and those of persons involved with organized crime may be useful for targeting investigation and communication efforts. This comparison illustrates that, in general, persons involved in organized crime tend to be later-onset offenders, older than those who frequent social media sites. Such offenders may perhaps be less likely to use social media. For example, as demonstrated, the largest age group of online social media users is between the ages of 18 and 34, whereas 70% of members of organized crime groups in the Netherlands were between 30 and 50 years old (Van Koppen 2010). Within the Canadian context, recall that Motiuk and Vuong (2005) found that the average age of gang affiliated offenders was 36. This, again, is dissimilar to the typical online social media user, who tends to be below the age of 35. Exceptionally, the two blog sites described in this report, Blogger and Wordpress, were shown to have an older cohort of users. It is possible that members of criminal organizations, like the older general public, are more attracted to blog sites than to Twitter, FaceBook, or MySpace, and as such may be users or consumers of such social media.

On the other hand, street gang members, as described by Morselli and Décary-Hétu (2010), who tend to be aged between 18 and 24 years, fall into the typical age of social media users. Morselli and Décary-Hétu investigated media claims that street gangs and criminal organizations use social media sites. The authors found that street gangs are not directly using social media for recruitment. Results of a key word search of over 50 gang names on Twitter, FaceBook, and MySpace showed that "gang presence on social networking sites is linked primarily to promote a general gang or street culture through individual displays. In most cases, the sites are designed and managed by members and associates who emphasize their allegiance to reported groups, such as the MS-13, Crips, Bloods, or Latin Kings." The use of Internet-based social networks to "showcase illegal exploits, make threats, and honor [sic] killed or jailed members" has been described by Gutierrez (2006) as cyber or net banging. Morselli and Décary-Hétu suppose that "cyberbanging" sites allow gangs to "create a new convergence setting for street gang members to interact with a wider number of people who would probably never have been exposed to their lifestyles and exploits through physical interactions… [and] have made street gangs a more accessible phenomenon to a larger portion of the population." Interestingly, the authors found that unlike the street gangs monitored in this research, the Hells Angels Outlaw Motorcycle Club did not use social networking sites to profile criminal or violent acts, despite having a prolific web presence.

Finally, unlike the typical social media user, women involved in criminal organizations tend to be non-Caucasian, with disadvantaged socio-economic backgrounds (Beare 2010). As such, it is possible that female organized crime offenders are even less likely than their male counterparts to use social media sites.

Conclusion

Online social media sites can allow for the rekindling of past friendships and for active engagement in discussions about common interests. OSMS allow people to share their hobbies, interests, favourite places to hang-out, likes, dislikes, photos, who their friends are, their current location, and other very personal information. Social media sites have created a large space for connecting and sharing information. People share a great deal of information with their online communities, both intentionally and without their explicit understanding. This information can be used by different actors in different ways. This report investigated, by conducting interviews with law enforcement officials and social media experts and through literature review, how online social media sites (OSMS) are and could be used by criminal organizations and by the law enforcement community.

Just like the average social media user, people involved with organized crime use OSMS. Similar to previous research, this study suggests that organized crime groups use OSMS to engage in "cyberbanging," that is, the glorification or promotion of gang subculture. Unlike previous research, two respondents from the current study indicated that organized crime groups use have used social media sites as a means to intimidate other gangs or individuals, to commit fraud, and for general gang recruitment.

Online social media sites can be used to coordinate criminal activities among networks of people who have never met each other offline, to identify criminal opportunities and to defraud people out of money through a variety of mechanisms. Information can be collected about the networks victims, people suspected of criminal activity, and about police officers who share information online.

Interviews show that law enforcement personnel routinely utilize OSMS with the goal of gathering intelligence to construct a profile of the suspect(s) in a crime. OSMS is a wonderful tool for achieving this because according to almost all respondents people tend to put too much trust and material into OSMS. Construction of the suspect(s) profile is only one activity for law enforcement. Law enforcement personnel also effectively use OSMS to stay in contact with the community that they serve and look for activities within the community that they should be aware of, such as upcoming disruptive events. Respondents also indicated that social media can help in the delivery of emergency instruction, traffic updates, special event promotion and asking for aid in the search of missing people. Social media can be used to interact with the community in other ways, such as setting up a book of condolences for lost officers and performing consultations with the public. In general, respondents agreed that the more interaction law enforcement can have with the community, the better that interaction will be.

It was agreed on by most respondents that law enforcement personnel must incorporate OSMS into their daily activities for both investigative and communication purposes. While some allow for this, respondents recommend widespread adoption of these techniques, suggesting that the next generation of suspects are more likely to have been exposed to OSMS and be more likely to make use of them for both criminal and personal purposes.

This study is subject to a number of limitations. Only 10 interviews were conducted with 11 interviewees, most of whom work in the Canadian context. This paper focused on blogs, social networking sites, microblogs and media sharing sites. This focus necessarily limits the scope of the research. Finally, some respondents were reluctant to speak about the activities of organized crime groups. Future research could be undertaken with involving interviews with people convicted of cybercrime in order to provide additional information on this emerging area of criminal and communicative opportunity.

References

Alderson, M. "Facebook: a Useful Tool for Police?" Connectedcops. 25 January 2011. Web. 3 February 2011. <http://connectedcops.net/?p=3637>.

Buchanan, Jim, and Grant, Alex J. "Investigating and Prosecuting Nigerian Fraud." *United States Attorney's Bulletin.* November 2001.

CBC News. "Beware Facebook scams: police." CBC. 6 January 2011. Web. February 8, 2011. <http://www.cbc.ca/canada/nova-scotia/story/2011/01/06/ns-facebook-scam.html#socialcomments>.

CheckFacebook.com. "Facebook Statistics and Breakdowns." CheckFacebook.com. n.d. Web. 26 January 2011. <http://www.checkfacebook.com/>.

Cheng, Alex, and Evans, Mark. "Inside Twitter – An In-Depth Look Inside the Twitter World." Sysomos: a Marketwire Company. June 2009. Web. <http://sysomos.com/insidetwitter/>.

Daily Mail Reporter. "Facebook hijacked by cyber criminals in scam to con 'friends' out of cash." Associated Newspapers Ltd. 11 November 2008. Web. 8 February 2011. <http://www.dailymail.co.uk/sciencetech/article-1084669/Facebook-hijacked-cyber-criminals-scam-friends-cash.html>.

Felson, Marcus, and Clarke, Ronald V. *Opportunity Makes the Thief: Practical Theory for Crime Prevention, Police Research Series, Paper 98*. Edited by Barry Webb. London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 1998.

Gerlsbeck, Rob, "The All-Canadian Wealth Test," *MoneySense Magazine*, October 2009.

Google, Inc.(a) "Site Profile: domain: myspace.com." Google, Inc. n.d. Web. 26 January 2011. <https://www.google.com/adplanner/planning/spite_profile#siteDetails?identifier=myspace.com&geo=CA&trait_type=1&lp=true>.

Google, Inc.(b) "About YouTube." Google, Inc. n.d. Web. 5 February 2011. <http://www.youtube.com/t/about_youtube.>

Internet Crime Complaint Centre. *2010 Internet Crime Report.* US: National White Collar Crime Center. 2011. Web. 11 March 2011. <http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf>.

Indiana News. "Woman's Facebook 'Friend' Suspected In Burglary." McGraw-Hill Broadcasting Company. 6 August 2010. Web. 10 March 2011. <http://www.theindychannel.com/news/24537182/detail.html>.

Jasra, Manoj. “Blogger Demographic Study by Sysomos.” Web Analytics World. 5 June 2010. Web. 6 February 2011. < http://www.webanalyticsworld.net/2010/06/blogger-demographic-study-by-sysomos.html>.

Kapardis, Andreas, and Krambia-Kapardis, Maria. “Enhancing fraud prevention and detection by profiling fraud offenders,” *Criminal Behaviour and Mental Health* 14, 3 (March 2006): 189-201.

Marsico, Edward M., Jr. “Social Networking Websites: Are MySpace and Facebook the fingerprints of the twenty-first century?” *Widener Law Journal* 19, 3 (2010): 967-976.

Masterman, Kevin. “Employing social media in the fight against crime.” *Gazette* 72, 2: 38. Royal Canadian Mounted Police, 2010.

McIntosh, Neil. “Google buys Blogger web service.” The Guardian. 18 February 2003. Web. 6 February 2011. <http://www.guardian.co.uk/business/2003/feb/18/digitalmedia.citynews>.

Morselli, Carlo, and Décary-Hétu, David. *Crime Facilitation Purposes of Social Networking Sites: A Review and Analysis of the “Cyberbanging” Phenomenon*. Ottawa: Public Safety Canada, 2010.

Motiuk, Laurence, and Vuong, Ben. *Federal Offenders with Criminal organization Offences: A Profile.* Ottawa: Correctional Services Canada, 2005. Web. 14 March 2011. <http://www.csc-scc.gc.ca/text/rsrch/briefs/b38/b38-eng.pdf>.

Oreskovic, Alexei. “MySpace launching new version of website.” Reuters. 27 October 2010. Web. 31 October 2010. <http://www.reuters.com/article/2010/10/27/us-myspace-idUSTRE69Q11M20101027>.

Ostrow, Adam. “You can now login to Myspace with Facebook.” Mashable, Inc. 18 November 2010. Web. <http://mashable.com/2010/11/18/you-can-now-login-to-myspace-with-facebook/>.

Quantcast. Information retrieved from: http://www.quantcast.com/. n.d. Web. 1 February 2011. <http://www.quantcast.com/>

Quantcast. *Quantcast Methodology Overview*. 2008. Web. 1 February 2011. <www.quantcast.com/white-papers/quantcast-methodology.pdf>.

Rege, Aunshul. “What’s Love Got to Do with It? Exploring Online Dating Scams and Identity,” *International Journal of Cyber Criminology* 3, 2 (2009): 494–512.

Smyth, Sara and Carleton, Rebecca. *Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources*. Ottawa: Public Safety Canada, 2011.

Timm, Carl, and Perez, Richard. *Seven deadliest social network attacks.* Rockland, Massachusetts: Syngress, 2010.

Weimann, Gabriel. "Terror on Facebook, Twitter, and Youtube," *The Brown Journal of World Affairs* 16, 2 (2010): 45-54.