
# 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**

ÐÒÅÐÁÒÅÄ £ÏÒ

2ÅÓÅÁÒÃÈ ÁÎÄ . ÁÔÉÏÎÁÌ #Ï ÏÒÄÉÎÁÔÉÏÎ
/ ÒÇÁÎÉÚÅÄ #ÒÉÍÅ $ÉÖÉÓÉÏÎ
,Á× %Î£ÏÒÅÍÅÎÔÁÎÄ 0ÏÌÉÃÙ "ÒÁÎÈ
0ÕÂÌÉÃ 3Á£ÅÔÙ #ÁÎÁÄÁ

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

2ÅÐÏÒÔ . Ï πςρ ςππρ

´ (ÅÒ - ÁÊÅÓÔÙ ÔÈÅ 1ÕÅÅÎ É Î 2ÉÇÈÔ Ï£ #ÁÎÁÄÁ ςππρ
#ÁÔ . Ï 03ρτζυ ςππρρ%Ζ0$&
)3" . . Ï ωχψΖρΖρππΖρωρωπΖτ

# 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

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.

## 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.

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 Ap

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

## 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 s

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.

## 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.

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

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, Dutc-19.25 -1mm

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). Bear

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

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 servi

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.